LA RÉSISTANCE ESTHÉTIQUE À L'ASSEMBLAGE DE SURVEILLANCE DE SÉCURITÉ : L'ART NUMÉRIQUE COMME PARTICIPATION CITOYENNE

SIMON HOGUE

Thèse
en
science politique
présentée aux Facultés de l'Université d'Ottawa
conformément aux exigences partielles du
diplôme de Doctorat en philosophie

École d'études politiques
Faculté des sciences sociales
Université d'Ottawa

Remerciements

Une thèse ne s'écrit jamais seule[1].

Mes sincères remerciements à David Grondin pour ses questions incisives qui savaient cibler de façon systématique les failles et les angles morts de ma réflexion, pour la confiance qu'il a portée envers mon travail et pour la liberté de création qu'il m'a autorisée. En espérant que la fin de la thèse ne marque pas la fin de notre collaboration.

Des remerciements vont également à Miguel de Larrinaga et Emily Wills, ainsi qu'à Nisha Shah et Daniel Trottier pour leurs précieuses observations, critiques et suggestions qui auront su pousser mon analyse au-delà de ses apparentes limites. Le succès des projets à venir vous sera en partie redevable.

Remerciements à Marie-Joëlle Robichaud, modèle de persévérance, de rigueur et de réussite ; remerciements à Marc-Olivier Castagner, compagnon de route depuis le tout début, à qui je dois beaucoup plus que j'ai su lui rendre : votre amitié a été essentielle à l'aboutissement de ce projet. Vous avez su mettre une chaleur humaine à la froideur de ce travail monastique.

Le soutien aveugle de mes parents, Claire Brisebois et Gaston Hogue, et beau-parent, Ginette Morasse et Louis Lapointe, doit être louangé. Toujours, vous avez fait montre d'une présence rassurante, d'un appui indéfectible et d'un respect véritable envers mon choix irrationnel de retourner aux études et de me lancer dans l'interminable parcours doctoral.

Mes remerciements les plus intimes et les plus chers vont à ma conjointe Noémie Morasse Lapointe qui est demeurée à mes côtés contre vent et marée depuis les premiers balbutiements de cette folle aventure; ainsi qu'à Adrien, Daphné et Laurent qui sont venus nous rejoindre en cours de route. Sans vous, cette thèse aurait été impossible ; une mer sans étoiles.

[1] Je reconnais la participation financière du Fonds de recherche du Québec – Société et culture.

Résumé

La thèse explore la surveillance algorithmique des communications mondiales à travers l'art numérique. Elle examine les projets artistiques à la lumière du moment post-Snowden qui met en évidence l'étroite relation entre la surveillance d'État et la lutte au terrorisme, l'économie numérique, et le droit à la vie privée. Plus spécifiquement, la thèse pose la question de la résistance esthétique à la surveillance déployée par les dispositifs de sécurité occidentaux et à la sécurisation du quotidien. Animée par une réflexion sur le public et la circulation de l'art, la thèse s'intéresse à une communauté d'artistes circulant principalement autour de New York et Berlin. Ces artistes se réapproprient les médias et les artefacts de la culture numérique et explorent la relation technologie-culture-pouvoir pour comprendre et contester les structures de pouvoir associées à ces pratiques de surveillance. L'art numérique propose une cartographie alternative du pouvoir qui éclaire et politise les structures de pouvoir rendues invisibles par le secret d'État et la banalisation des technologies. Il conteste en outre la subjectivité numérique néolibérale et les pratiques de catégorisation sociale pour repenser une collectivité politique égalitaire.

La thèse démontre la pertinence de l'art comme avenue de résistance à la surveillance, et propose une nouvelle méthode pour analyser l'art en Relations internationales. Mettant en évidence la complicité volontaire et involontaire des entreprises numériques aux efforts antiterroristes, l'incapacité du droit à la vie privée à protéger les individus contre la surveillance algorithmique des communications mondiales, la liberté d'interprétation des données que s'attribuent les dispositifs de sécurité occidentaux, et l'impératif de visibilité qui accompagne la participation numérique, la thèse montre les limites que cette surveillance impose à la résistance. De là, la thèse suggère à travers les œuvres analysées une avenue de contestation à la fois technologique et collective permettant la mise en place d'une collectivité radicalement égalitaire qui brouille les processus de catégorisation sociale et constitue un espace de dissensus face à la société profilée et sécurisée de la surveillance algorithmique.

Table des matières

Table des illustrations

1 Introduction : Participation numérique : de la complicité à la résistance, l'art comme forme de contestation de la surveillance algorithmique

I don't want to live in a society that does these sort of things.
Edward Snowden[1]

2013 a-t-elle été l'année du retour vers le futur ? En quelques semaines de l'été 2013, en une série de révélations orchestrées avec la collaboration des journalistes Laura Poitras, Glenn Greenwald et Ewan MacAskill, Edward Snowden, ancien employé de Booz Allen Hamilton contractant privé à la National Security Agency (NSA), a jeté une bombe sur le monde de la surveillance : l'appareil de renseignement américain, en collaboration avec ses pairs occidentaux, particulièrement le Government Communications Headquarters (GCHQ) britannique, pratique une surveillance de masse des communications mondiales (Greenwald 2013a; MacAskill & Dance 2013).

Ces révélations ont galvanisé les critiques de la surveillance étatique et les défenseurs du droit à la vie privée. Regroupés sous le titre Writers Against Mass Surveillance, plus de 500 auteurs internationaux se sont insurgés dans une lettre ouverte contre la surveillance de masse rappelant les risques qu'elle faisait peser pour la démocratie. « The basic pillar of democracy is the inviolable integrity of the individual, » écrivent-ils.

> This fundamental human right has been rendered null and void through abuse of technological developments by states and corporations for mass surveillance purposes. A person under surveillance is no longer free; a society under surveillance is no longer a democracy. To maintain any validity, our democratic rights must apply in virtual as in real space (Writers Against Mass Surveillance 2013).

Certains, dans la tradition politico-juridique américaine, ont choisi de contester les pratiques de surveillance devant les tribunaux (ACLU 2015b). D'autres ont préféré y opposer l'ironie. PRISM, programme phare de la NSA, a été disqualifié pour dopage dans la course aux prix Big Brother[2] remis pour souligner les « government agencies, private companies and individuals who have

[1] (Snowden, Poitras & Greenwald 2013)
[2] Créés en 1998 par l'organisation britannique Privacy International, les prix Big Brother sont remis par des associations nationales d'organisations issues de la société civile.

excelled in the violation of our privacy » (Big Brother Awards Privacy International 2017; Privacy France 2018). Edward Snowden s'est quant à lui vu décerner un prix spécial Julia et Winston pour son courage exceptionnel dans la dénonciation de la surveillance (Digitalcourage 2018).

La tentation de comparer la surveillance menée par la NSA à celle de l'iconique Big Brother est vive — quoique l'on puisse souhaiter au protagoniste Snowden une fin moins tragique que celle qui attend les héros de *1984*. Comme dans le roman de George Orwell, la surveillance de la NSA est omniprésente, un instrument du maintien d'un ordre social inégalitaire inscrit dans un dispositif sécuritaire en apparence sans complexe. À l'image de cette Londres du bloc Océania où les caméras de surveillance vidéo, qui meublent les moindres recoins de l'espace public et privé, s'assurent de capter chaque geste et sentiment de ses habitants, la NSA collecte, dans les mots du lanceur d'alerte, « everything about everyone » (Snowden cité par Appelbaum & Poitras 2013). Scrutant les détails quotidiens de millions de personnes, la NSA traque toute information susceptible de mener à l'interception de terroriste, au risque de surveiller au passage des innocents. « [Surveillance] is no longer based on the traditional practice of targeted taps based on some individual suspicion of wrongdoing, » explique Snowden. « It covers phone calls, emails, texts, search history, what you buy, who your friends are, where you go, who you love » (Associated Press 2014).

Figure 1.1 : Un monde sous surveillance.
Image tirée du film 1984 (1956) (source : Stonebridge 2015)

À l'instar de cette novlangue qui réécrit le monde orwellien, la NSA joue également de rhétorique pour camoufler la portée de leurs pratiques : des données ne sont surveillées que si elles ont été soumises à l'œil humain, ne sont collectées que si elles sont analysées ; les données de citoyens américains sont collectées de façon fortuite (« incidental ») et non sciemment (« not wittingly ») (EFF 2012; Contorno 2014). Sans égard à la richesse de l'information qui peut en être soutirée, la collecte de métadonnées n'est pas une forme de surveillance, suggère-t-on, puisqu'elle écarte le contenu des communications (Feinstein 2013). Pourtant, il suffit de s'attarder quelques instants au projet du parlementaire allemand Malte Spitz qui a cartographié ses déplacements à l'aide de ses métadonnées téléphoniques pour réaliser la précision de ces informations (Biermann 2011). Dans le climat de guerre permanente contre le terroriste invisible qui définit les premières décennies du siècle, la surveillance de la NSA serait nécessaire pour assurer la paix : la sécurité vaut bien le sacrifice d'un peu de liberté, semble-t-on indiquer.

La comparaison entre la présente situation et le monde de *1984* a toutefois ses limites. Contrairement aux apparences, qui sont d'ailleurs renforcées par l'accent médiatique et critique sur la NSA, la surveillance de la NSA n'est pas centralisée. Ou plutôt, la NSA n'est qu'un acteur parmi plusieurs autres d'un vaste assemblage de surveillance numérique, pour reprendre les mots de Kevin D. Haggerty et Richard V. Ericson (Haggerty & Ericson 2000). « [S]urveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole, » écrivent-ils.

> It is this tendency which allows us to speak of surveillance as an assemblage, with such combinations providing for exponential increases in the degree of surveillance capacity. Rather than exemplifying Orwell's totalitarian state-centred Oceana, this assemblage operates across both state and extra-state institutions (Haggerty & Ericson 2000, 610).

Cette intégration entre institutions étatiques et économiques ne signifie pas pour autant la consolidation de la surveillance sous une seule autorité, mais une plus grande fluidité, interaction et interchangeabilité des informations d'une vers l'autre[3] (Bauman & Lyon 2013).

[3] Ainsi, le gouvernement américain a mis en place des Fusion Centers pour assurer la fluidité des informations entre les organisations nationales (Monahan & Palmer 2009). Des entreprises privées comme Axciom et Oracle se spécialisent dans l'agrégation d'information provenant d'émetteurs privés et publics (Christl 2017; Raley 2013). L'État achète des données privées ou délègue à des compagnies financières ou aériennes une partie de ses pouvoirs régaliens (Amoore & de Goede 2005).

La surveillance de masse de la NSA, faut-il le rappeler, est dépendante de l'économie et des infrastructures numériques. Comme le suggère le Groupe de révision du renseignement et des technologies de communication mis sur pied par le président Obama en réponse à la sortie de Snowden, si la surveillance numérique apparaît aujourd'hui comme une source privilégiée d'information, c'est parce que le réseau de communication qui sillonne le monde est global. Ce même réseau est utilisé tant par les acteurs civils et étatiques que par les forces obscures qui menacent l'ordre social. Cette condition structurelle permet à la NSA de se greffer à la toile de fibres optiques mondiale pour mener ses opérations de surveillance des signaux et des systèmes électroniques (Clarke et coll. 2013, 179-87). L'agence s'approprie alors les données produites par l'utilisation des technologies numériques qu'elle filtre et analyse. « [T]his kind of [mass] surveillance … means that the NSA and similar agencies watch for cookies and log-in information, » analyse David Lyon.

> They thus use data derived from the use of devices such as cell phones or geo-locating social media. What users unknowingly disclose on those platforms—such as Facebook or Twitter—or when using their phones, is usable data for "national security" and policing purposes. … The NSA thus depends on codes, the algorithms, plus the witting or unwitting cooperation of both telephone and internet corporations in order to do surveillance. Individual users may play a part, too, but their role is hardly one of conscious actors in the drama. This already goes beyond what many once imagined was direct and specifically targeted relationships by state agencies of individuals, to mass surveillance, dependent on a close liaison with corporate bodies and on the self-recording devices used in everyday communications and transactions (Lyon 2014, 2–3).

Figure 1.2 : Surveillance contemporaine
Un centre de données de Facebook, à Luleå en Suède, photo : David Levene (source : Harding 2015)

Le partage d'une même technologie numérique entre les institutions économiques et sécuritaires est à la base de l'étroite collaboration mise au jour par Snowden. Cette technologie marque également une rupture avec la surveillance vidéo représentée dans *1984*. La surveillance algorithmique introduit une hybridation du corps, pour reprendre à nouveau Haggerty et Ericson, où la chair se double d'un fantôme numérique. « First [the human body] is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a 'data double' of pure virtuality » suggèrent-ils (Haggerty & Ericson 2000, 611). Cette virtualité n'est pas en opposition au monde réel. Le double numérique y a un effet tangible. Gilles Deleuze proposait dix ans plus tôt le passage du gouvernement des individus vers celui des « dividuels » (Deleuze 1990). Ces fragments d'information prélevés à partir des déplacements et autres transactions de chacun sont recomposés pour former une personnalité et agrégés dans des bases de données à partir desquelles il sera possible d'établir des comparaisons, des tendances de population afin d'en contrôler la mobilité et d'en maximiser la profitabilité. C'est l'ère de la société de contrôle. « Today … we are witnessing the formation and coalescence of a new type of body, a form of becoming which transcends human corporeality and reduces flesh to pure information, » écrivent Haggerty et Ericson.

> … Data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent. … And while such doubles ostensibly refer back to particular individuals, they transcend a purely representational idiom. Rather than being accurate or inaccurate portrayals of real individuals, they are a form of pragmatics: differentiated according to how useful they are in allowing institutions to make discriminations among populations (Haggerty & Ericson 2000, 613–614).

Méconnu de l'individu auquel il est associé, le double numérique voyage d'une institution à l'autre déterminant les services auxquels un individu a droit. Mais si le double numérique marque la fin — si jamais elle fut — de l'unicité de l'identité individuelle, il n'est pas lui-même unique. Les données qui circulent donnent naissance à une pluralité de doubles numériques selon les besoins des institutions. Comme le remarquent les auteurs, les données et doubles ont avant tout une fonction utilitaire. Les informations sont traitées dans une logique d'action. « What holds [government agencies, private corporations and, albeit unwittingly, ordinary users] together, » écrit Lyon,

> … is the software, the algorithms, the codes that allow users' data to be systematically extracted or disclosed, analyzed, and turned into what the data collectors and others, such as the NSA, hope will be actionable data. In other words, it is the (big) data practices that different kinds of operations have in common. As Snowden himself said in a 10 June 2013 video, the "… NSA targets the communications of everyone…" then " … filters, analyzes, measures them and stores them for periods of time simply because it's the easiest, most efficient and most valuable way of achieving these ends" (Lyon 2014, 3).

Dans cette logique d'opérationnalisation du savoir, rappelle Louise Amoore, les données sont extirpées de leur contexte réel, séparées de leur contexte de surveillance, et inscrites dans une nouvelle structure de signification (Amoore 2011). Ainsi, comme le propose l'auteure, l'intérêt de la NSA pour le réseau social Facebook d'un individu n'est pas biographique, mais sécuritaire : il doit permettre de calculer les probabilités que cet individu devienne un terroriste susceptible de mener à terme ses viles intentions (voir aussi de Goede 2014; de Goede 2008a).

La surveillance numérique dépasse le cadre individuel rompant avec l'image de l'armée d'agents de bureau et d'espions infiltrés. À l'instar d'autres facettes de la société contemporaine, la surveillance numérique est automatisée : produite par une lecture technologique des humains ; les données, conçues pour une analyse algorithmique. La machine découpe, assemble et établit les inférences. L'humain, cible de la surveillance, se retrouve en marge du cycle d'intelligibilité et soumis à une surveillance s'étendant dans une multiplicité de contextes et de lieux. La surveillance numérique participe à un exercice de catégorisation des individus, accéléré et raffiné par la rapidité,

la précision et l'abondance des informations disponibles (Monahan 2010, 9-10). Plutôt que de chercher à discipliner les individus comme le proposait le panoptisme foucaldien, la surveillance numérique adopte un modèle de contrôle qui, à l'image de la fluidité des données, module les services et autorisations en fonction des catégories auxquelles appartiennent les individus. Polices d'assurance, autorisations de crédit, emplois, soutiens sociaux et visas deviennent tous déterminés par cette catégorisation. Ce processus de striation sociale privilégie ou marginalise certains groupes de la population de façon d'autant plus précise que la surveillance est pointue.

Snowden a ainsi révélé l'existence d'une vaste entreprise de surveillance algorithmique des communications mondiales par les dispositifs de sécurité occidentaux. Celle-ci se couple à d'autres pratiques de contrôle déjà en place érigées au nom de la sécurité nationale telles que la surveillance aéroportuaire et des passagers (Adey 2006; Salter 2004; Adey 2009), la surveillance de la mobilité internationale (Amoore 2006b; Fuller 2003; Pallister-Wilkins 2016; Cowen 2010), la surveillance des flux financiers (de Goede 2012; Amicelle 2011; de Goede 2008a), la biométrie (Bellanova & Fuster 2013; Hristova 2014; Aas 2006), la surveillance urbaine (Lippert & Walby 2013; Crang & Graham 2007; Monahan & Mokos 2013), ou la surveillance aérienne et par drones (Chamayou 2013; J. Weber 2016; Bishop 2012). En s'affairant à rendre visible le risque à la sécurité nationale pour mieux le contrôler ou l'abattre, ces pratiques de surveillance soulèvent ensemble l'enjeu de la visualisation de l'objet de sécurité (MacDonald, Hughes & Dodds 2010; Ericson 2006). Qui constitue un risque à la sécurité nationale ? Quels lieux de passage et quelles pratiques permettent de capturer des informations sur le risque afin de l'identifier et de l'intercepter ? La surveillance des communications mondiales, si elle diffère dans ses modalités, s'insère aussi dans cet objectif de visualisation. Elle se distingue toutefois par la portée de sa pénétration en s'insérant au cœur même du quotidien et de l'intimité de ces cibles. Les téléphones intelligents et les médias sociaux génèrent d'importantes quantités de données offrant de nombreuses informations personnelles sur l'utilisateur, ses goûts, intentions et relations sociales. Or, ces données demeurent rarement en circuit fermé. Elles circulent le long des infrastructures Internet qui composent l'architecture principale des communications mondiales et sont entreposées dans les serveurs des entreprises numériques. De ce fait, elles deviennent les cibles potentielles de la surveillance des dispositifs de sécurité qui transforment des données en apparence anodine en autant de sources d'information de sécurité.

Constatant l'omniprésence des pratiques et technologies de surveillance, la circulation des données, et la vitesse et la précision des données collectées, Haggerty et Ericson suggèrent que « the surveillant assemblage marks the progressive 'disappearance of disappearance'—a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions » (Haggerty & Ericson 2000, 619). Nonobstant l'intention derrière la surveillance — Lyon rappelle par exemple que l'expansion de la surveillance est associée à l'État-providence et, à travers lui, au soutien des personnes défavorisées et quelle peut ainsi être bénéfique (Lyon 2001; Lyon 2003) —, Snowden rappelle la possibilité de voir les données générées par toute institution être appropriées par la NSA. Si les motivations qui animent la lutte au terrorisme du dispositif de sécurité peuvent être louables, les effets de la surveillance et de l'inclusion des mégadonnées dans un cadre d'analyse sécuritaire n'en sont pas moindres : elles sécurisent la vie quotidienne occidentale, assurant le contrôle d'une population de consommateurs économiquement profitables et sécuritairement dociles. Ainsi, Lyon conclut-il des révélations Snowden que

> the expanding securitization of daily life prompts the use of extended surveillance… The quest of "national security" breeds Big Data, particularly through efforts to preempt security breaches by a form of anticipatory surveillance described, somewhat vaguely, by the Department of Homeland Security as "connecting the dots" (Lyon 2014, 4).

Est-ce donc dire que nous sommes condamnés au contrôle ou à être complice du dispositif de sécurité américain ? La pénétration des technologies numériques dans le quotidien, à la source de la surveillance de masse, confirme l'illusion de l'évasion vers un espace encore vierge tel que la mythique cabane dans la forêt. La cryptographie est tout aussi incapable d'assurer la protection contre l'assemblage de surveillance, offrant au mieux, aux dires de Snowden, un « breathing room » (Snowden cité par Poitras 2014). L'absence de sortie et l'ubiquité de la surveillance algorithmique ont ainsi poussé le Free Art and Technology (F.A.T.) Lab, groupe d'artistes activistes consacré à la défense de l'Internet comme espace public, à fermer boutique et à abandonner la lutte contre la surveillance. Ainsi, écrivent-ils dans un mot d'adieu :

> We, who believed the Internet could change society, that technology could take other paths than surveillance, centralization and consumerism. The battle is lost and the juggernaut of the security industry, power and capital has been unable to stop… There's no use banging our heads against the wall anymore. Either your head will explode or they will simply open the door and let you in. Either way, no house will come crumbling down (M. Eriksson & Roth 2015).

Cette vision dystopique de la surveillance mène au fatalisme, comme le remarque d'ailleurs le F.A.T. Lab même s'il s'en défend bien. Pour le F.A.T. Lab, fermer est libératoire. Il ne s'agit pas d'abandonner la lutte, explique-t-il, mais de la mettre en sursis, de la reporter à plus tard lorsque les conditions seront plus favorables à ce combat d'avant-garde que le reste du monde ne semble pas avoir encore compris. La faute reviendrait — encore une fois — aux petites gens.

Si la fuite semble vaine, la résistance, malgré ce que peut en croire le F.A.T. Lab, reste possible. Comme le suggère Haggerty et Ericson, l'assemblage de surveillance marque certes la fin de l'anonymat, mais l'expansion de la surveillance permet toutefois une inversion du regard : « [s]urveillance has … transformed hierarchies of observation, and allows for the scrutiny of the powerful by both institutions and the general population » (Haggerty & Ericson 2000, 617).

1.1 Questions de recherche : espace d'action et participation résistante à la surveillance algorithmique

La question du déterminisme numérique et de l'agentivité structure ma thèse. Réfléchir à l'agentivité dans le contexte de la surveillance algorithmique est d'autant plus criant qu'au-delà de son omniprésence, la participation est devenue, pour l'individu qui habite nos sociétés contemporaines, nécessaire pour assurer la prospérité individuelle et celle de la collectivité. « Across a broad range of social domains, our expectations to participate are matched with expectations that we will participate, » écrivent Barney et coll.

> Participation has become a measure of the quality of our social situations and interactions, and has come to stand in for virtues that, under other conditions, might have names like equality, justice, fairness, community, or freedom. Participation is normal; a lack of participation seems suspicious, strange, and disappointing… Participation has become a tremendously valuable social, political, and economic resource … a condition that is constitutive of the social itself (Barney et coll. 2016, ix-x).

S'il n'y a d'autre choix que de participer, peut-on imaginer une forme de participation qui soit néanmoins critique de la surveillance algorithmique sans pour autant retomber dans une dichotomie entre technofétichisme et technophobie ? Quel espace d'action existe-t-il face à la surveillance algorithmique ? C'est avec ces interrogations à l'esprit que je pose mes questions de recherche :

1) Comment l'art de surveillance, pensé comme une forme particulière de participation citoyenne numérique, peut-il constituer un espace de résistance à la surveillance algorithmique et à la sécurisation du quotidien ?

2) Comment l'art de surveillance s'insère-t-il dans le régime de visibilité de la surveillance algorithmique ?

3) Comment l'art de surveillance peut-il proposer une forme alternative de visibilité à l'ère numérique ?

En réponse à ces questions, je suggère que devant la complicité volontaire et involontaire des entreprises numériques aux efforts antiterroristes et l'incapacité du droit à la vie privée à protéger les individus contre la surveillance algorithmique des communications mondiales, l'art numérique propose une cartographie alternative du pouvoir qui éclaire et politise les structures de pouvoir rendues invisibles par le secret d'État et la banalisation des technologies. S'appropriant les technologies numériques, l'art numérique conteste en outre la subjectivité numérique néolibérale et les pratiques de catégorisation sociale pour repenser une collectivité politique égalitaire.

1.2 Orientations : art, critique de la notion de vie privée et régime de visibilité

« One of the enduring questions that the modern period asks of art is about its relationship to politics and specifically the politics of resistance, » écrit Vivienne Jabri. « Just how art comes to situate itself in relation to politics is itself subject to much controversy, both in the history of art and in philosophy » (Jabri 2006, 819). Dans les études critiques sur la sécurité et la surveillance, la pertinence politique de l'art semble toutefois faire l'unanimité (voir néanmoins Holden 2006). Tant dans l'une que dans l'autre, l'esthétique occupe une position de choix pour déstabiliser des structures de pouvoir omniprésentes, capillaires et subjectivantes (Bleiker 2000; Amoore & Hall 2010; McGrath & Sweeny 2010; de Goede 2005; Danchev & Lisle 2009). Symptôme de la mort du rêve révolutionnaire, reconnaissant avec Foucault l'illusion du grand Refus, l'art est l'expression de la multiplicité des lieux de résistance et offre la possibilité d'une contestation tacticienne. En soulevant des moments d'incertitude, l'art permet de contrer par la créativité la rationalité hégémonique (Bleiker 2009) et de donner libre cours à l'imagination d'un présent alternatif (Raley 2009). Ainsi, peut-on résumer à travers Louise Amoore la pertinence politique de

l'art telle qu'elle se comprend dans ces deux champs d'études : « [t]he aesthetic realm, … though not unproblematically or naturally politicizing, has a capacity to call us into question, to challenge our sense of invulnerability to the problems of the world, and to make us feel a certain discomfort » (Amoore 2006a, 270). J'emboîte ici le pas de ces littératures, en signalant toutefois que l'art n'est pas un espace social pur, autonome et critique. Comme le rappelle Bourdieu, le champ de l'art est traversé par ses propres relations de pouvoir qui déterminent les tendances, les têtes d'affiche et la diffusion de l'art (Bourdieu 1987). La critique artistique peut aussi faillir (G. Graham 2005, 183-199; Monahan 2015). Il ne s'agit donc pas de mettre un chèque en blanc entre les mains de l'artiste ou de prétendre au monopole de l'art sur la résistance, mais de s'intéresser, d'un point de vue tant théorique qu'empirique, à l'apport politique de l'esthétique.

Dans le contexte de la résistance à la surveillance algorithmique, l'art offre la possibilité de contourner les limites et de compléter l'activisme légal et la défense du droit à la vie privée qui occupent l'avant-scène. L'activisme légal tel qu'il se pratique par exemple par l'American Civil Liberty Union, l'Electronic Frontier Foundation, Privacy International, ou OpenMedia, s'il demeure pertinent, se trouve pris dans un fétichisme constitutionnel où le juste et le souhaitable — le cadre éthique au moins implicite de la résistance — se trouve coincés dans les limites du texte de loi et de son contexte culturel de production. Comme le rappelle David Lyon, le concept de vie privée est un produit culturel dont on ne peut présupposer une définition universelle (Lyon 2001, 20-22). En Occident, le concept de vie privée est associé à un espace protégé assurant l'autonomie et l'intégrité individuelles. Que l'on parle d'une « zone of immunity » comme l'historien Georges Duby (Duby cité par Lyon 2001, 20), d'un « breathing space to survive » comme le juge à la Cour suprême américaine William Brennan ou d'une « distance from others » comme le fait Anthony Giddens (Brennan et Giddens cités par Cheney-Lippold 2017a, 206-2011), l'espace de solitude assurerait à l'homme (blanc) un moment pour veiller à son bien-être spirituel, émotionnel et intellectuel nécessaire au développement et au bonheur individuel. En pratique, il faut reconnaître que cette autonomie de l'individu est largement demeurée le privilège d'hommes blancs[4].

Lyon identifie à terme trois lacunes au recours à la notion de vie privée pour contester la surveillance algorithmique.

[4] Lyon risque d'ailleurs l'hypothèse que le souci croissant pour la protection de la vie privée est conséquent au fait qu'avec la surveillance algorithmique, les hommes blancs voient leurs privilèges s'effacer (Lyon 2001, 22).

> First, privacy answers, consistently but paradoxically, to personal fears of invasion, violation and disturbance. Having successfully prised each of us from our neighbours so that we could be individuated social atoms, amenable to classification and sorting as disembodied abstractions, privacy responses echo just such individuation. Second, privacy is frequently conceived as a residual means of compensating for human errors and computer failures. The systems themselves are deemed safe when policies protect against surveillance slippage or data leakiness. Third, privacy policy and legislation is notoriously cumbersome and unresponsive to the rapid changes taking place in surveillance. … In each instance, privacy tends not to see surveillance as a social question or one that has to do with power. … Surveillance today is a means of social sorting and classifying populations and not just invading personal space or violating the privacy of individuals. … Technological developments and social processes interact to produce outcomes which … raise … questions of fairness, mutuality and appropriate resistance (Lyon 2001, 150–151).

Confirmation de l'individualisation de la société, aveuglement aux conséquences structurelles des technologies au-delà des brèches qui peuvent apparaître, incapacité à prendre acte des transformations rapides que la surveillance algorithmique encourt, les critiques de Lyon à l'endroit d'une perspective uniquement légale de la surveillance sont sévères. Reprenant l'esprit de cette dernière critique, John Cheney-Lippold remarque que les algorithmes remettent en question la notion même d'intégrité de l'individu alors que son identité est recomposée, à son insu, à partir de données produites par l'utilisation des technologies numériques (Cheney-Lippold 2017a). Le modèle économique de l'industrie numérique, qui fait des données d'utilisateurs le nouvel or noir, contredit également l'idée de la vie privée transformant l'intimité en un espace lucratif plutôt qu'un espace protégé du regard de l'autre (Cinnamon 2017).

Synthétisant les conséquences des récentes transformations des pratiques de surveillance algorithmique au contexte particulier de la sécurité, Marieke de Goede soulève trois limites que rencontre la notion de vie privée. Premièrement, la mobilité des données du monde commercial vers celui de la sécurité et la réinterprétation qui en est alors faite

> means that traditional privacy safeguards which revolve around conditions of movement, access, and (the duration of) storage of data are at least supplemented and perhaps superseded by novel questions concerning the nature of selection and specific data-analytics deployed within security practice (de Goede 2014, 102).

Deuxièmement, les efforts déployés pour anticiper et intercepter un attentat terroriste remettent en question les notions de suspicion et de présomption d'innocence. « Demanding privacy safeguards in this context may miss its target » (de Goede 2014, 102). Troisièmement, les dispositifs de sécurité cherchent avant toute chose à établir des connexions entre les données et à identifier celles générant des « 'nexus' of suspicion ». Ce n'est qu'alors que l'identité individuelle devient

pertinente. Mais afin d'établir ces connexions, il aura été nécessaire, au préalable, de filtrer des montagnes de données qui, si elles n'ont pas fait sonner l'alarme, auront néanmoins servi à établir des profils de normalité contre lesquels mesurer le risque. Ainsi, de Goede conclut-elle,

> understanding information as possessed, ceded, and protected by the individual, and understanding (informational) privacy as "the rights of a single subject" does not do justice to the way in which anticipatory knowledge constructs categories and draws connections (Rancière 2004: 302; Amoore 2013). … As long as privacy is thought of as tied to individual identities, it is of limited use in questioning the way that inferences are drawn, profiles are constituted, and suspicion is calibrated (de Goede 2014, 102–103).

Comme le propose Jonathan Cinnamon, la nécessité de penser la surveillance dans un contexte social plutôt qu'individuel semble faire consensus parmi les études de surveillance (Cinnamon 2017, 611). La perspective individualiste souffre d'un important angle mort : elle est incapable d'appréhender les conséquences sociales du régime de visibilité de la surveillance algorithmique.

La surveillance algorithmique des dispositifs de sécurité scrute sans cesse pour identifier et intercepter les risques potentiels à la stabilité de la nation. Pour ce faire, elle transforme chaque individu en objet de visibilité permanent. Ainsi, pourrait-on réinterpréter comme une directive de vie l'argument couramment énoncé selon lequel celui qui n'a rien à cacher n'a rien à craindre des pratiques de surveillance. Il faudrait plutôt lire : celui qui ne cache rien n'a rien à craindre. L'argument traditionnel veut démontrer que seules les personnes qui commettent des gestes répréhensibles doivent craindre la surveillance de sécurité. Cherchant à identifier et intercepter les terroristes et autres menaces à la sécurité nationale, elle ne vise ni ne s'embourbe de faits de vie de personnes « ordinaires ». À ce titre, l'intrusion dans la vie privée est minimale et nécessaire pour assurer la sécurité de l'État. En cette ère d'insécurité, il s'agirait de bien savoir équilibrer liberté et sécurité. Pourtant, comme le rappelle par exemple Torin Monahan, cette recherche d'équilibre masque les décisions politiques et les conséquences sociales des pratiques de surveillance. « Why are questions about surveillance and security always framed in terms of trade-offs? » demande-t-il.

> [O]nce the issues are presented in these terms, the only thing left to decide is whether the public is willing to make the necessary sacrifices to bring about greater national security. Absent are discussions about the politics behind surveillance and security systems, what one means by "security," what (or who) gets left out of the conversation, and the veracity of such assumptions about trade-offs to begin with. … Some of the obvious issues not discussed when talking about trade-offs are how surveillance contributes to spatial segregation and

> social inequality, how private high-tech industries are benefiting from the public revenue generated for these systems, and what the ramifications are of quantifying "security" (e.g., by the number of video cameras) for political purposes (Monahan 2006a, 1-2).

La surveillance algorithmique ne peut se limiter à une question d'équilibre, mais s'inscrit plus globalement dans un régime de visibilité qui accorde des droits et privilèges à certains et impose des contraintes à d'autres. Le régime de visibilité actuel crée un déséquilibre entre les institutions et pratiques de surveillance et les individus qui y sont soumis. « [C]ontemporary surveillance expands exponentially, » écrit Lyon,

> it renders ordinary everyday lives increasingly transparent to large organizations. The corollary, however, is that organizations engaged in surveillance are increasingly invisible to those whose data are garnered and used. This "paradox" is deepened by the advent of Big Data (Lyon 2014, 4).

Or, comme le rappelle Nicholas Mirzoeff, qui se positionne en héritier de Michel Foucault et Jacques Rancière, déterminer ce qui est visible de ce qui est invisible est plus qu'une question oculaire. « Despite its name, » écrit-il,

> this process is not composed simply of visual perceptions in the physical sense but is formed by a set of relations combining information, imagination, and insight into a rendition of physical and psychic space. … [V]isuality … [is] a discursive practice for rendering and regulating the real that has material effects (Mirzoeff 2011, 475).

Le régime de visibilité est politique distribuant les droits de présence dans une communauté. Dans ce contexte, la censure ou l'invisibilité ne sont pas contraires à la visibilité, mais constitutives de celle-ci, productrice de l'ordre social. Ainsi, pour Mirzoeff, l'invisibilité des populations tuées par les frappes de drones constitue un élément de la nécropolitique de sécurité américaine en Afghanistan (Mirzoeff 2011, 489), incarnant la relégation de ces individus au plus bas de l'échelle sociale. En même temps, l'invisibilité sous la forme du secret, comme dans le cas des pratiques de surveillance de sécurité, constitue un instrument du pouvoir. Le secret d'État, suggère ainsi Trevor Paglen, est un geste d'exception, une marque du pouvoir du souverain.

> "[S]tate secrecy is a form of executive power. It is the power to unilaterally and legitimately conceal events, actions, budgets, programs, and plans … a form of monarchical power that contemporary states have inherited from the kingdoms of yesteryear." This idea of secrecy as the sovereign's power to violate the law—an idea voiced by political theorist Carl Schmitt—is, in Paglen's view, continually at odds with the "normal" functioning of the democratic state, one that operates on the principles of "equal rights, transparent government, and informed consent" (Hu 2015, 135)

Les efforts déployés pour identifier et faire taire Snowden (Poitras 2014) et les demi-vérités des autorités entourant la nature des programmes de surveillance tendent à confirmer la nécessité et la légitimité du secret aux yeux des dispositifs de sécurité.

L'invisibilité de la surveillance algorithmique ne peut toutefois se réduire au seul fait du secret d'État. L'univers numérique sur lequel repose la surveillance algorithmique est, pour l'essentiel, invisible. « Dématérialisé », il se dérobe du regard. La miniaturisation des composantes, la délocalisation des services et la banalité de sa présence quotidienne font du numérique un fantôme contemporain, à la fois omniprésent et absent. En même temps, les effets de la surveillance sont pour plusieurs difficilement perceptibles. Peut-être surveille-t-on les informations de géolocalisation, de navigation Internet et les carnets d'adresses des utilisateurs. Cette surveillance est toutefois devenue si courante qu'elle apparaît insignifiante sinon pour tous, du moins pour un large segment des privilégiés[5]. Qui plus est, comprendre les tenants et aboutissants de la surveillance algorithmique peut s'avérer difficile pour un néophyte. Décoder les archives Snowden, par exemple, constitue un véritable travail de recherche. L'abondance des informations disséminées dans des centaines de notes légales et diapositives, la relative inaccessibilité des archives éparpillées dans plusieurs médias internationaux et la technicité du contenu constituent autant de barrières d'accès (voir cependant les compilations suivantes Canadian Journalists for Free Expression Politics of Surveillance Project 2018; Light 2016; La Fondation Courage 2018).

L'esthétique répond au régime de visibilité qui cache, sous le scellé du secret d'État et l'éther numérique, les pratiques de surveillance algorithmique des dispositifs de sécurité tout en imposant aux individus une obligation d'être visibles. En revendiquant un droit de regard, un droit de réécrire le régime de visibilité, l'esthétique offre une résistance à la surveillance qui n'est pas individualiste, mais sociale et politique.

[5] Deborah Lupton, partageant les conclusions de Bryce Peake, suggère notamment que les groupes sociaux les plus susceptibles d'être visés par la surveillance et pour lesquelles les conséquences sont les plus sévères partagent une plus grande conscience de l'existence de la surveillance. Dans ce contexte, la surveillance n'apparaît ni banale ni insignifiante (Lupton 2016, 141).

1.3 Étude de cas : art, technologie et surveillance, pour la revendication d'un droit de regard sur la surveillance algorithmique

Malgré l'hypervisibilité de la surveillance algorithmique provoquée par la rupture des révélations Snowden, il semble que les structures de pouvoir qui sont associées à ses pratiques demeurent obscures. Cette visualisation est pourtant nécessaire pour pouvoir comprendre son fonctionnement et ses effets, pour pouvoir évaluer la pertinence des pratiques de surveillance et les contester. L'universalité de la surveillance dite de masse et indiscriminée est trompeuse. S'il est vrai que tous sont soumis à la surveillance – il faut prendre aux mots cet officiel supérieur du renseignement américain qui déclare sous couvert de l'anonymat que pour la NSA « [e]verybody's a target; everybody with communication is a target » (cité dans Bamford 2012) — il n'en reste pas moins que chacun n'y est pas soumis de la même façon. La surveillance algorithmique pratiquée par les dispositifs de sécurité occidentaux est discriminatoire. Elle cible certains profils plutôt que d'autres, ceux jugés dangereux bien davantage que ceux qui n'apparaissent pas soulever de risque. Dans ce processus, la surveillance marginalise certains groupes, accentuant sur des populations souvent déjà précarisées le poids d'un système de contrôle.

Dans ma thèse, je tourne mon attention vers une communauté d'artistes issus de la culture numérique. Gravitant autour des pôles géographiques de New York et Berlin, des organismes Rhizome et Eyebeam, et du festival transmediale, ces artistes explorent les transformations sociales engendrées par les technologies numériques. Déjà intéressés par les questions liées à Internet, ces artistes ont réagi créativement aux révélations Snowden, abordant l'enjeu de la surveillance sous une multitude de sens au-delà de la notion de la vie privée : des infrastructures et de la matérialité de la surveillance (Burrington 2017; Wagenknecht 2015; Burrington and Whittaker 2016; Oliver 2015) à la reproduction de l'hétéronormativité (Blas 2014; Wagenknecht 2014), du savoir algorithmique (Bridle 2015g; van den Dorpel 2016; Grosser 2015) à la présence numérique (Cirio 2015; Roth 2015; Morone 2015). Contestant aussi l'appropriation des technologies numériques par les institutions économiques et sécuritaires, ces artistes ont investi ces technologies pour mieux les décortiquer et les redessiner, et pour proposer de nouvelles façons de concevoir leur place dans la société. Ces artistes explorent, à partir d'un matériel numérique, la relation technologie-culture-pouvoir, rendant certaines facettes plus opaques de la surveillance numérique visibles et proposant des avenues pour apparaître et brouiller la surveillance.

L'objectif de la thèse n'est pas de chercher à comprendre comment New York et Berlin, Rhizome et transmediale ou certains artistes ont su se positionner avantageusement afin de devenir des noyaux d'une communauté artistique. Je ne propose pas l'analyse d'un champ social artistique déjà constitué à l'image de la démarche bourdieusienne (Bourdieu 2002, 196-221). En m'intéressant à cette communauté d'artistes, au risque de lui imposer une unité qu'elle n'a pas réellement, je donne un corps, une entité sociologique, aux notions vagues d'art numérique ou d'art de surveillance. Qui est l'art numérique ? Quels matériaux composent cet art ? Quels thèmes sont abordés ? Où cet art est-il créé et exposé ? Quels sont les canaux de circulation ? Qui le voit ? Qui en parle ? En répondant à ces questions, il devient possible d'amener l'analyse de l'art au-delà de l'artiste ou de l'œuvre, montrant comment cet art s'insère dans un ensemble social qui lui assure une légitimité et un public (Warner 2002). La question de la thèse demeure toutefois celle de la participation résistante à la surveillance algorithmique et à la sécurisation du quotidien.

À travers la thèse, je défends l'idée qu'au côté de l'activisme légal mené en cour, du lobbying d'élus, du journalisme d'enquête, ou de l'hacktivisme, ces artistes investissent un autre registre de la résistance. Pour plusieurs, la surveillance algorithmique n'est pas intrinsèquement mauvaise, mais celle menée par les dispositifs de sécurité occidentaux est intrusive et met en danger la liberté d'expression et le respect des droits. Pour comprendre les structures de pouvoir associées à ces pratiques de surveillance, il est nécessaire, selon eux, de comprendre les technologies numériques et les diverses façons dont elles sont exploitées. L'exploration des technologies met en lumière la surveillance algorithmique et permet de reprendre le contrôle sur nos données. Ainsi, contestant le régime de visibilité de cette surveillance algorithmique, ils revendiquent un droit de regard sur l'assemblage de surveillance. En s'appliquant à collecter toutes les données, à surveiller toute présence numérique, la NSA et ses partenaires soumettent chacun à la possibilité de devenir un sujet d'intérêt de la sécurité. Or, la construction du sujet de sécurité à travers l'interconnectabilité des données et la mise en réseau montre la décentralisation du sujet qui ne peut plus être pensé en termes individuels. Dans ce contexte, la résistance à la surveillance algorithmique doit adopter une approche collective. Ici, la visibilité devient une tactique de mise en vulnérabilité qui permet de contextualiser et historiciser les structures de pouvoir de la surveillance algorithmique, de contester l'inévitabilité de son déploiement, et de s'attribuer le droit d'être visible sans être soumis à la surveillance algorithmique.

Dans ce vaste éventail d'artistes et d'art, je restreins mon attention aux œuvres s'intéressant explicitement aux pratiques de surveillance des dispositifs de sécurité. La surveillance algorithmique est largement répandue, menée par une multitude d'organismes. Même si plusieurs instruments, pratiques et stratégies sont partagés tant par les institutions économiques que par celles du monde de la sécurité, la surveillance de sécurité telle que menée par la NSA, se distingue par ses visées. Il ne s'agit plus, dans ce dernier cas, de fournir des services ou de produire les meilleurs outils de marketings, mais de déterminer le risque à la sécurité nationale, l'ennemi à intercepter et abattre. La surveillance de la NSA est investie des pouvoirs du souverain : le pouvoir d'établir l'exception et le droit de vie et de mort. La surveillance de la NSA est également partie prenante d'un processus de sécurisation de l'ensemble de la société, c'est-à-dire de soumission des diverses facettes de la société aux codes et aux impératifs de la sécurité. Si cette sécurisation vit en harmonie avec la société néolibérale, elle procède néanmoins d'une logique qui n'est pas marchande, mais qui relève plutôt du maintien de l'ordre social (Aradau and Van Munster 2008; Amoore 2013). Pour ces raisons, je m'intéresse aux œuvres qui traitent d'abord et avant tout de la surveillance de sécurité, même si en cour de route, la question de la surveillance économique refait inévitablement surface vu la proximité entre les deux mondes.

1.4 Structure de la thèse

Le cœur de la thèse se situe dans l'analyse d'interventions artistiques de contre-visibilité. Ces interventions sont regroupées sous trois thèmes : l'exploitation des infrastructures de communication mondiale, l'opérationnalisation du savoir de sécurité, et l'impératif de visibilité du sujet qui accompagne la participation numérique. Pour les deux premiers, l'art rend les structures du pouvoir visibles et conteste le secret et l'invisibilité des pratiques de surveillance algorithmique. Dans le dernier cas, l'art contourne la surveillance en proposant un mode de visibilité qui brouille les mécanismes de catégorisation et de ciblage des populations.

Avant d'explorer la résistance artistique, je retourne dans un premier temps aux littératures sur la sécurité, la sécurisation et la surveillance afin d'approfondir le rôle de la surveillance dans l'architecture contemporaine de sécurité et de contester la lecture manichéenne de la surveillance. Constatant l'impossibilité d'une sécurité absolue malgré l'extension du dispositif de sécurité et un glissement de l'idée de menace vers celle de risque, les études critiques de sécurité abordent la sécurité, dans la tradition foucaldienne, comme une technologie de gouvernement. Le dispositif de

sécurité assure le contrôle des circulations d'objets et de population et veille à intercepter les événements déstabilisateurs afin de maintenir l'ordre social nécessaire à la profitabilité économique. Pratique de catégorisation sociale et de contrôle des populations, la surveillance algorithmique s'insère dans ce dispositif de sécurité permettant un contrôle ciblé et en temps réel. Pourtant, plusieurs auteurs ont contesté l'interprétation à sens unique de la surveillance. La surveillance est une pratique culturelle qui met des technologies de visibilité en œuvre dans l'objectif de pouvoir contrôler les populations. Contrôler ne signifie pas pour autant la mise en place d'un régime totalitaire, mais il peut s'agir par exemple de l'octroi par l'État de services à des populations vulnérables. La surveillance peut promouvoir l'autodétermination des individus. Cette révision de la surveillance ouvre la porte à la réappropriation des technologies de surveillance qui viendrait contester son utilisation par les dispositifs de sécurité occidentaux.

Le chapitre 3 part de cette ouverture vers la résistance pour penser la contestation artistique de la surveillance algorithmique. Après avoir conceptualisé la politique de l'esthétique, je m'intéresse plus concrètement aux pratiques d'art résistant afin de donner une entité sociologique à l'art numérique ou de surveillance. L'esthétique a acquis, avec l'art moderne particulièrement, une dimension critique importante. Dans le chapitre, j'explore la façon dont les études critiques de sécurité et le tournant esthétique en Relations internationales définissent l'art et l'esthétique et lui attribue une pertinence politique. L'esthétique, proposent-ils, déstabilise les compréhensions traditionnelles du monde, créant un inconfort propice à la remise en cause des structures de pouvoir et à l'imagination d'alternatives. Également inspiré par Jacques Rancière, j'insiste sur la connexion entre l'esthétique et le régime de visibilité. L'art est à la fois un objet et une performance qui créent une rupture dans la distribution des parts et permet de revendiquer une présence à part entière dans le monde. Je présente également la méthodologie qui me permet de reconstituer une communauté d'artistes numériques et de sélectionner certaines œuvres au sein de celle-ci. Ces artistes et leurs œuvres circulent. Ils se regroupent néanmoins autour de quelques pôles d'attraction qui permettent de donner une consistance sociologique à ce groupe. Ils abordent aussi une pluralité d'enjeux liés à la culture numérique et la surveillance : de la matérialité de la surveillance à la reproduction de l'hétéronormativité, du savoir algorithmique à la présence numérique. Afin de restreindre le cadre de l'analyse et de l'ancrer dans la réflexion sur la résistance à la surveillance algorithmique et la sécurisation du quotidien, j'analyse uniquement des œuvres qui portent explicitement sur la

surveillance de sécurité, en particulier celle de la NSA, même si, en cour de route, la question de la surveillance économique revient de l'avant.

Les trois chapitres suivants approfondissent les œuvres de résistance artistique, abordant les thèmes des infrastructures de communication mondiale, l'opérationnalisation du savoir de sécurité, et l'impératif de visibilité qui accompagne la participation numérique. Dans les deux premiers cas, l'art revendique un droit de regard sur les pratiques de surveillance invisibles. Face au troisième thème, l'art s'approprie un espace de visibilité qui brouille les mécanismes de contrôle de la surveillance. Le chapitre 4 explore à travers les œuvres *Citizen Ex* de James Bridle, *IXmaps* d'Andrew Clement, et des photographies de Trevor Paglen l'exploitation des infrastructures de communication par la NSA et ses partenaires occidentaux. Ces œuvres montrent la nature politique des technologies numériques et la façon dont elles transforment la gouvernance mondiale. Parce qu'au fil de la navigation Internet, les données traversent des frontières internationales, elles deviennent sujettes à des cadres législatifs différents. Parce que les opérateurs de réseau et les fournisseurs de services américains occupent une position dominante dans l'univers numérique, les données numériques franchissent fréquemment les frontières américaines. Couplée aux opérations étrangères et aux partenariats stratégiques, la position centrale de la NSA lui confère un accès privilégié aux données mondiales. Plus que cela, la surveillance est un phénomène mondial. Dans ce contexte, penser les limites de la surveillance en termes juridiques est illusoire. Le droit à la vie privée consenti par les États à leurs ressortissants est rendu caduc aussitôt que les données quittent le pays, les agences de surveillance n'ayant pas de restriction à la surveillance d'étrangers. En ce sens, les infrastructures deviennent le lieu d'intervention du souverain. La mobilité des données normalise l'exception, permettant à la NSA et à ses partenaires de contourner les dispositions légales qui protègent les individus sans enfreindre le droit.

Le chapitre 5 se penche sur l'opérationnalisation du savoir de sécurité. Partant du constat que les dispositifs de sécurité occidentaux ont mis un mécanisme de surveillance en place qui leur permet de collecter une quantité astronomique de données, je me tourne vers l'œuvre *Secret Power* de Simon Denny pour réfléchir à leur utilisation. Denny interroge, dans une œuvre symbolique, la relation savoir-pouvoir à l'ère de la surveillance algorithmique. Explorant la cartographie de la NSA, Denny suggère que la surveillance transforme les notions de géopolitique et de souveraineté. Je poursuis son travail exploratoire en approfondissant la cartographie associée au programme TREASUREMAP de la NSA. Celui-ci inscrit dans sa représentation spatiale la logique

d'interconnectabilité qui domine la rationalité de sécurité dominante. Selon cette logique, le réel et le virtuel deviennent des mondes fongibles. Les données peuvent être associées et réassociées indéfiniment dans la mesure où ces interconnexions permettent d'établir des structures de suspicion et, de là, permettent d'intervenir pour intercepter les risques identifiés. Cette obsession pour l'interconnectabilité est performative, transformant le rapport au monde de la NSA. Elle insère le savoir de sécurité dans une logique paranoïaque et spéculative où l'opérationnalisation et la possibilité d'action priment sur l'exactitude. Les effets de ce savoir paranoïaque et spéculatif sont doubles. D'un côté, la volonté de cartographier et connecter la totalité de l'univers numérique indique que tout et tous deviennent des cibles potentielles de la surveillance de sécurité. De l'autre, les structures de suspicion scénarisées rappellent que l'attention de la surveillance n'est pas également distribuée. Elle scrute certains individus et groupes davantage que d'autres — dans le contexte de la lutte au terrorisme islamique les populations arabo-musulmanes — contribuant à leur marginalisation. Dans une perspective de résistance à la surveillance, la logique paranoïaque et spéculative du savoir de sécurité complique en définitive le contrôle sur la signification et l'interprétation de nos données.

Les chapitres 4 et 5 présentent des œuvres critiques de la surveillance algorithmique de la NSA. Les deux chapitres abordent des sujets distincts. Les méthodes de révélation sont également différentes. Alors que *Citizen Ex* et *IXmaps* utilisent les technologies numériques pour rendre le fonctionnement de la surveillance visible, s'appropriant le vocabulaire du réseau pour parler du réseau pour reprendre l'expression de Bridle (Bridle 2013), *Secret Power* décortique les artefacts culturels issus de la NSA pour en comprendre la culture. Toutes résistent néanmoins par la revendication d'un droit de regard sur l'invisible. Elles construisent ensemble une cartographie du pouvoir montrant les rouages de la surveillance des communications mondiales. Surtout, cette cartographie éclaire les limites et contraintes que cette surveillance impose à la résistance. Face à une surveillance qui se veut omniprésente et discriminatoire, la résistance doit s'approprier les technologies numériques afin que ces dernières ne se restreignent pas à des instruments de catégorisation et de contrôle social, mais permettent la constitution d'une nouvelle forme politique égalitaire. Contextualisant les pratiques de surveillance qui strient l'univers numérique, ces deux chapitres constituent aussi les pierres d'assise pour la dernière discussion où il est question de reprendre contrôle sur sa propre visibilité numérique afin de construire une collectivité politique marquée par l'égalité radicale.

Avec *Autonomy Cube*, Trevor Paglen et Jacob Appelbaum contestent l'impératif de visibilité auquel nous sommes soumis par la collectivisation de l'anonymat et la constitution d'une multitude, d'une collectivité ouverte à l'autre et modulable. J'explore dans le chapitre 6 ce projet à travers lequel les artistes veulent créer, en mobilisant la participation des institutions muséales, des havres contre la surveillance algorithmique. L'œuvre poursuit donc un premier objectif de révélation et un second, fonctionnel. Elle se veut une version institutionnelle de la réalité augmentée permettant de mettre en pratique, à travers le havre, un monde alternatif. Ce havre est, pour les artistes, nécessaire afin d'assurer la créativité, la liberté d'explorer, l'autonomie et la démocratie menacées par la surveillance. Pour ce faire, *Autonomy Cube* offre une connexion au réseau d'anonymisation Tor. Si Tor est généralement associée à la criminalité, aux cyberlibertariens et à la protection d'une vie privée individualisée, Paglen et Appelbaum insufflent une dimension sociale et politique au réseau. En interrompant l'association entre les données générées par les technologies numériques et l'utilisateur, Tor/*Autonomy Cube* permet une participation à l'univers numérique qui évite, pour un instant, la complicité avec les structures de pouvoir de la société de contrôle. Parce que l'œuvre n'est pas un bloqueur d'annonces, une hygiène numérique ou un exercice d'obscurcissement de l'identité réelle, l'œuvre contourne également le piège individualiste associé à la notion de vie privée. Pour rendre la navigation individuelle anonyme, Tor/*Autonomy Cube* crée une collectivité d'utilisateurs. L'image de cette collectivité hétéroclite remplace l'individu aux yeux de la surveillance. Ce faisant, elle brouille les mécanismes de catégorisation et de ciblage de la surveillance. En revanche, Tor/*Autonomy Cube* rend la participation au réseau visible. En ce sens, l'œuvre n'est pas uniquement un projet d'anonymisation ou d'invisibilité. Elle s'approprie un droit à apparaître sans être soumis à la surveillance algorithmique. La dimension sociale et politique de l'œuvre réside dans l'ambiguïté de cette visibilité : l'utilisateur est identifiable comme partie de la collectivité résistante, mais son identité est masquée par la collectivité. Tor/*Autonomy Cube* performe une visibilité politique qui revendique un monde numérique égalitaire et ouvert à l'autre.

Les révélations de Snowden présentent un dispositif de surveillance de sécurité bien établi et cohérent, tentaculaire et omniprésent. Son ubiquité, ses capacités technologiques, ses partenariats internationaux, ses accords commerciaux, le secret entourant ses procédures judiciaires et administratives, la légitimité de la lutte antiterroriste, et la complexité de son jargon érigent autour de lui une série de défense, autant de murailles ; le dispositif de surveillance deviendrait

intouchable. Pourtant, si l'on refuse cette cohérence, cette inévitabilité, qui lierait par défaut toutes les pièces de l'assemblage de surveillance, celui-ci devient chancelant : le résultat d'un alignement parfait, mais possiblement forcé et temporaire, d'étoiles. Plutôt qu'être une force, sa complexité devient alors une fragilité, autant de points de fracture potentiels. C'est cette fragilité, gardée secrète à coups de scellé de confidentialité ou dissimulée dans le paysage quotidien, qu'un nombre d'artistes permet d'éclairer et d'enfoncer pour mieux revendiquer un monde qui n'est pas monopolisé par la suspicion et la peur de l'autre.

2 Sécurisation, risque et surveillance : le gouvernement du quotidien

> *Il n'y a pas besoin de science-fiction pour concevoir un mécanisme de contrôle qui donne à chaque instant la position d'un élément en milieu ouvert, animal dans une réserve, homme dans une entreprise (collier électronique). Félix Guattari imaginait une ville où chacun pouvait quitter son appartement, sa rue, son quartier, grâce à sa carte électronique (dividuelle) qui faisait lever telle ou telle barrière ; mais aussi bien la carte pouvait être recrachée tel jour, ou entre telles heures ; ce qui compte n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle.*
>
> Gilles Deleuze[1]

Les pratiques de surveillance algorithmique[2] mises en lumière par Snowden ne sont pas entièrement nouvelles. La collecte massive de données de communication aux fins d'une surveillance mise au service de la sécurité nationale est une pratique issue des dernières décennies du vingtième siècle en forte croissance depuis les attentats terroristes du 11 septembre 2001. Dans leur analyse de l'utilisation des données dans l'évaluation du risque terroriste, Louise Amoore et Marieke de Goede écrivaient en 2008 :

> It is important to emphasise here that we are not arguing that the use of transactions data after 9/11 is unique or unprecedented—there is ample historical evidence of risk profiling via data prior to 9/11 (Haggerty and Ericson 2000; Andreas and Snyder 2000; Thrift and French 2002; Graham 2005). However, the specific representation of threat and danger after 9/11—terrorists who 'live among us'; 'home grown terrorists'; 'clean skins' and so on—has cleared the ground for the deployment of commercial data as a basis for (preemptive) security action. Although the risk practices involved in transactions data mining are far from new (we need only look to the history of insurance or credit scoring, for example), the scale and scope of their application to the sphere of security is distinctly novel, and entails practices of actionable visualisation that depart significantly from established uses of surveillance technologies in urban policing (Amoore & de Goede 2008b, 174).

[1] (Deleuze 1990)

[2] Je retiens le terme surveillance algorithmique plutôt que surveillance des données (« dataveillance ») ou surveillance de masse (« mass surveillance ») pour mettre en évidence l'importance du traitement de l'information collectée. Dans cette logique d'accumulation en masse de données numérique, il ne suffit pas d'amasser de l'information, mais de réussir à l'opérationnaliser, de la rendre utile à la réalisation d'un objectif quelconque. Comme le suggère Tung-Hui Hu: « [w]ith the mean North American user consuming over 45 GB of Internet data each month, the marvel of the cloud may be less its vastness than the software tools that manage, simplify, and make it intelligible: the indexers, the recommendation and visualization algorithms that offer users a sense of control over these data » (Hu 2015, 111).

La lutte au terrorisme, projetée à l'avant-scène depuis, a légitimé des pratiques de surveillance qui apparaissent et se généralisent au fur et à mesure que se popularisent les technologies de l'information. Au côté de pratiques conventionnelles de surveillance comme les opérations clandestines, les écoutes électroniques et la propagation de la vidéosurveillance, les années 1980 voient l'émergence de la surveillance électronique (S. Cohen 1985; Laudon 1986; Marx 1988; Gandy 1993). Cette forme de surveillance, technique de contrôle des populations qui procède par l'accumulation d'informations personnelles et la classification des individus en fonction de leur valeur économique ou sécuritaire, est rendue possible par la diffusion des technologies de l'information dans les sociétés occidentales. La numérisation de la vie contemporaine occidentale et les possibilités de traitement de données offertes par les ordinateurs font le lit de cette forme de surveillance qui s'insère de plus en plus dans le quotidien, lui-même de plus en plus dépendant des technologies de l'information :

> the mundane, ordinary, taken-for-granted world of getting money from a bank machine, making a phone call, applying for sickness benefits, driving a car, using a credit card, receiving junk mail, picking up books from the library, or crossing a border on trips abroad. In each case mentioned, computers record our transactions, check against other known details, ensure that we and not others are billed or paid, store bits of our biographies, or assess our financial, legal or national standing. Each time we do one of these things we actually or potentially leave a trace of our doings. Computers and their associated communications systems now mediate all these kinds of relationships; to participate in modern society is to be under electronic surveillance (Lyon 1994, 4).

Les traces numériques laissées par chaque utilisation de ces technologies de l'information, désormais parties intégrales de la vie quotidienne — Internet, ordinateurs, téléphones cellulaires, infonuagique, radio-identification (RFID), biométries, etc. se retrouvent et nous suivent littéralement partout, jusque dans nos poches et sur notre table de chevet —, alimentent cette forme de surveillance (Lyon 2001; Lyon 1994).

Toutefois, l'expansion des technologies ne peut à elle seule expliquer la surveillance de masse d'aujourd'hui, car la rationalité sécuritaire de la NSA est indissociable de la conception actuelle de la sécurité nationale américaine. L'interprétation qui a été faite des attentats terroristes du 11 septembre 2001, et les réponses qui leur ont été apportées ont marqué une expansion considérable du cadre d'analyse et de gestion sécuritaire du monde « civil ». Ce que Snowden révèle n'est pas contraire à cette dynamique. L'onde de choc Snowden n'est pas tant le résultat de la nouveauté de pratiques de surveillance, pour l'essentiel connues ou au moins en partie anticipées

par les milieux académiques et activistes. L'onde de choc provient de l'étendue de la surveillance, la capacité technologique à collecter et emmagasiner les données, et de la proximité du dispositif de sécurité avec l'économie numérique. Snowden montre en effet l'étroite collaboration des univers de sécurité et économique en un unique ruban de Möbius, pour reprendre l'image de Didier Bigo (Bigo 2016), le premier s'approvisionnant directement sur les serveurs des principales compagnies qui dominent les télécommunications (Gellman & Poitras 2013). Pour David Lyon, Snowden montre l'accélération de deux tendances existantes plutôt que de l'émergence de nouveaux phénomènes : la transparence croissante des individus face à des organisations elles-mêmes de plus en plus opaques et la sécurisation du quotidien (Lyon 2014, 4). Il révèle du même coup la dépendance de la communication moderne sur une infrastructure économique privée.

La surveillance de masse qui transforme chaque donnée de communication, chaque donnée numérique en objet de sécurité s'inscrit dans une sécurisation croissante de la vie quotidienne des sociétés occidentales. Adaptant la définition de la militarisation offerte par David Grondin, il est possible de définir la sécurisation de la vie quotidienne comme « un processus social large comprenant des microprocessus qui portent l'empreinte du fait [de sécurité] ou de la vision de la [sécurité nationale] en dehors des sphères stratégiques et [de sécurité] pour s'étendre de façon durable dans les sphères sociales et culturelles » (Grondin 2014, 458). La porosité de la frontière entre le civil et le champ de la sécurité s'affiche sous plusieurs formes : l'intégration dans les unités militaires américaines d'éléments civils, notamment des journalistes chargés d'assurer une couverture médiatique favorable à l'armée (Campbell 2003) et des universitaires ayant pour mission la conscientisation des soldats à la culture locale (Bell 2012, 227) ; la militarisation des forces policières dans la lutte antiterroriste (Horowitz 2003) ; l'utilisation d'armes militaires pour contrer les manifestations civiles (Weaver 2009) ; l'incursion du Pentagone dans l'univers des jeux vidéo et du cinéma (Hughes 2007; Shaw 2010; Der Derian 2009) ; la militarisation des espaces publics en premier lieu les points de passage que constituent les frontières, aéroports, gares et autres postes de péage autoroutiers (Zureik & Salter 2005; Salter 2008b; Packer 2006; Amoore 2013, 105-126) ; la fermeture des espaces à l'intérieur de camps d'internement où la norme législative est suspendue pour les indésirables (Agamben 1998; Fuller 2003; Hailey 2009) ou à l'intérieure de zone fortifiée qui affranchissent les mieux nanties d'un environnement jugé décadent (Duffield 2010b; Monahan 2010, 81-98). Ces manifestations de la sécurisation de la vie quotidienne en Occident, auxquelles s'ajoute la surveillance de masse de la NSA, illustrent deux tendances

complémentaires : la banalisation de l'exceptionnel où des pratiques généralement réservées au registre prioritaire du sécuritaire deviennent communes, et l'exceptionnalisation du banal où les petits gestes de tous les jours se transforment en objets de sécurité, codes cryptés du comportement humain et indicateurs des menaces futures. De concert, ces deux tendances placent le quotidien de millions d'individus dans la mire de la sécurité.

Dans cette mer de mesures individuelles, l'utilisation de la surveillance à des fins sécuritaires semble particulièrement révélatrice de la tendance générale. Il est attendu que la surveillance de masse comblera l'incapacité historique du dispositif de sécurité américain à lier les informations qui mena aux attentats terroristes du 11 septembre. Le *Report of the Joint Inquiry into the terrorist attacks of September 11, 2001*, publié par les comités de la Chambre des représentants et du Sénat américains sur le renseignement, a ainsi mis en évidence les lacunes du renseignement en montrant que les informations nécessaires à l'interception préemptive des auteurs des attentats étaient entre les mains des agences du renseignement, mais qu'ils avaient été incapables d'en tirer les conclusions nécessaires (Amoore & de Goede 2008b, 173-174). Dans ce contexte, l'omniscience gouvernementale doit assurer la sécurité nationale en connectant ces points qui restèrent isolés, perdus dans la masse d'informations. Ainsi, la surveillance occupe un rôle central dans la nouvelle logique de risque qui réorganise le rapport qu'entretient l'appareil de sécurité vis-à-vis de l'autre. Loin d'être anodine, la sécurisation du quotidien par la surveillance dichotomise davantage les sociétés occidentales en établissant des frontières difficilement perméables entre inclus et exclus (Adey 2006; Lyon 2001; Monahan 2006b; Monahan 2010; Amoore & de Goede 2008c; Haggerty & Ericson 2000). La surveillance assure d'abord la fonction essentielle de lecture et de décodage des activités quotidiennes des individus en plus d'une fonction d'écriture et de modelage du citoyen. Il faut inscrire dans les corps les pratiques jugées normales et à faible risque (Foucault 1975; Rouvroy & Berns 2010). D'autre part, par les moyens mis à sa disposition, la surveillance sécuritaire illustre la volonté d'omniscience et d'omnipotence qui soutient la sécurisation du quotidien. Ce dispositif tentaculaire, ou capillaire pour utiliser une expression moins connotée, doit capter le plus anodin des événements. Ces pratiques touchent toutes les classes sociales, transformant chacun, et certains plus que d'autres, en potentiel ennemi de l'État. « [T]oday the normal relationship between the state and its citizens, » nous dit Giorgio Agamben, « is defined by suspicion, police filing and control. The unspoken principle which rules our society can be stated like that: *every citizen is a potential terrorist* » (Agamben 2013).

La position centrale qu'occupe la surveillance dans ce processus de sécurisation du quotidien en fait un objet d'attention tant pour ses promoteurs que pour les critiques. Pour les uns, la surveillance assure une gouvernance ciblée qui touche uniquement les personnes fautives évitant ainsi à ceux qui respectent les normes les désagréments des contrôles sécuritaires. La surveillance offrirait une gouvernance souple et en douceur garantissant une mobilité permanente et maximisée (Amoore & de Goede 2005). Pour les autres, elle est annonciatrice d'un cauchemar présent ou à venir. Alarmés par la toute-puissance d'un appareil gouvernemental centralisé, opaque et omniscient, ils dénoncent les menaces que la surveillance fait peser sur la liberté et l'égalité, fondement de la démocratie. La portée de la surveillance imaginée dans ces œuvres de fiction n'est qu'une pâle copie des pratiques de surveillance qui assujettissent les citoyens occidentaux aujourd'hui.

Pourtant, cette position dichotomique vis-à-vis de la surveillance survit difficilement à l'analyse. Comme le dit Didier Bigo :

> relative ignorance of the technological developments in digitisation and datafication … has created a chasm between two forms of reasoning: technophilia versus technophobia. Technophilia considers that security will automatically (and un-problematically) emerge out of the progress of technology and industrial efforts. In contrast, technophobic argument sees only the dangers of technologies and seeks to control them from above by a series of norms of conduct… Bridging this chasm requires rethinking creatively about how society-scale digitisation, big data(fication) and large-scale surveillance affect contemporary democratic politics beyond technology or managerial processes (Bigo 2016).

Il faut s'intéresser la surveillance pour ce qu'elle est : la rencontre des technologies et de pratiques culturelles, plutôt que de débuter l'analyse submergé par les désirs ou les peurs. Dans les prochaines pages, je propose de survoler la littérature en études critiques de sécurité pour comprendre à la fois le terme de sécurité comme technologie de gouvernement, et la place de la surveillance dans cette architecture. Pour mieux saisir les possibilités offertes par la surveillance au-delà de son rôle d'instrument de la sécurité, je propose un détour par la littérature critique de surveillance qui invite à conceptualiser, en étroite relation avec les réflexions sur la place des technologies dans nos sociétés, la surveillance comme pratique sociale. Cette conceptualisation ouverte de la surveillance permet de comprendre ses failles et les opportunités d'une contestation de la surveillance par sa réappropriation.

2.1 Contre-orthodoxie : repenser la sécurité et les RI

Penser la surveillance comme instrument d'une sécurité nationale elle-même technologie de gouvernement assurant la gouvernance d'une population, d'un territoire et de la mobilité de la première dans le second est aux antipodes de l'orthodoxie des études de sécurité en Relations internationales. Traditionnellement consacré aux conflits militaires entre grandes puissances et au maintien hégémonique (Waltz 1979; Mearsheimer 1990; Kennedy 1987), le monolithe des études de sécurité s'est progressivement fissuré au fil des critiques ontologiques, épistémologiques et éthiques rejetant avec plus ou moins de violence le carcan du prisme d'analyse traditionnel. L'éclatement des études de sécurité s'est fait malgré la résistance d'une arrière-garde cherchant à en conserver les limites classiques sous prétexte que les critiques nuisent à la cohérence de la discipline. Si « [t]he boundaries of intellectual disciplines are permeable », écrit Stephen Walt, l'incertitude ontologique qui accompagne cette perméabilité n'affecterait toutefois pas les études de sécurité.

> The main focus of security studies is easy to identify, however: it is the phenomenon of war. … Accordingly, security studies may be defined as the study of the threat, use, and control of military force (Nye & Lynn-Jones, 1988). It explores the conditions that make the use of force more likely, the ways that the use of force affects individuals, states, and societies, and the specific policies that states adopt in order to prepare for, prevent, or engage in war (Walt 1991, 212).

L'argument d'autorité et la condescendance de l'auteur vis-à-vis de certaines critiques des études de sécurité qu'il accuse d'« academic irrelevance » (Walt 1991, 223) n'ont cependant pas réussi à freiner l'essor des remises en question de la perspective traditionnelle de la discipline. Événements, débats académiques et autres dynamiques institutionnelles ont amené à repenser les principaux concepts de la discipline pour faire place à de nouveaux enjeux et de nouvelles perspectives sur ce qu'est la sécurité, et comment celle-ci est étudiée[3].

[3] Insatisfaits de l'épistémologie positiviste et de l'ontologie stato-centrique dominantes en RI, de nombreux auteurs s'efforcent, à partir des années 1980, de montrer les failles des approches traditionnelles (Waltz 1979; Keohane 1984; Keohane 1986; Baldwin 1993) et ont exigé l'éclatement des frontières disciplinaires jugées stérilement obtuses. Inspirés notamment par les canons poststructuralistes français Michel Foucault, Jacques Derrida et Gilles Deleuze, ils étudient le complexe pouvoir-savoir des relations internationales. Partant du constat de Foucault selon lequel « il n'y a pas de relation de pouvoir sans constitution corrélative d'un champ de savoir, ni de savoir qui ne suppose et ne constitue en même temps des relations de pouvoir » (Foucault 1975, 36), ils s'attaquent aux monuments de la discipline en montrant l'historicité des postulats ontologiques : la causalité, l'objectivisme, la fétichisation des faits, ainsi que la prédominance de l'État, de l'anarchie et des dichotomies guerre/paix, et conflit/coopération comme objets d'études des RI (Ashley 1988; Ashley 1986; Walker 1993; George and Campbell 1990; Wendt 1992; Der Derian and Shapiro 1989). Ces catégories, plutôt que d'aider à résoudre les problèmes de la politique mondiale, sont accusées de contribuer

Le narratif de la discipline organise les critiques en sécurité autour de trois grandes opérations, chacune plus ou moins déstabilisatrice du paradigme dominant (Grondin, D'Aoust & Macleod 2010; Buzan & Hansen 2009; Peoples & Vaughan-Williams 2010). La première vise l'élargissement du concept de sécurité. Contestant la trop grande place accordée aux enjeux militaires dans les études de sécurité, ces critiques invitent à élargir l'éventail de menaces à la sécurité nationale[4] (Ullman 1983; Mathews 1989). L'invitation à dépasser les questions étroitement militaires en études de sécurité demeure néanmoins près du paradigme dominant des études de sécurité en conservant en son cœur l'État national comme objet référent.

La deuxième opération critique remet en question l'État comme unique objet référent des études de sécurité. L'extension du concept de sécurité se propose d'inclure de nouveaux objets à sécuriser comme l'individu, la société ou l'environnement. Figure de proue de cette démarche, Barry Buzan propose dans *People, State and Fear* (Buzan 1991) une révision de l'unité de l'État[5].

à la réification de politiques marquées par la violence et les inégalités (Smith 2004). Ces auteurs promeuvent au contraire la reconnaissance de la nature socialement constituée et constituante du savoir et la subjectivité du chercheur par rapport à son objet d'études. Plutôt que d'expliquer des phénomènes mondiaux, ils s'intéressent à la façon dont la définition des problèmes et catégories des relations internationales crée des inégalités, ignore de nombreuses relations de pouvoirs pourtant constitutives de la politique mondiale, et limite les possibilités d'action en jugeant impertinentes par défaut celles qui sont extérieures au cadre d'analyse dominant. Pour Bleiker, plutôt que de prendre les représentations pour acquis il faut chercher à comprendre « how representative practices themselves have come to constitute and shape political practices » (Bleiker 2001, 510). Ces auteurs étudient donc la manière dont les représentations, qu'il s'agisse de l'univers diplomatique (Der Derian 1987), de la sécurité internationale (Krause and Williams 1997), de l'identité américaine (Campbell 1998) ou encore du statut de la femme (Enloe 2004; Enloe 1990), divisent le monde entre inclus et exclus, réifiant les structures de pouvoir actuelles. Leurs approches sont éminemment, et sciemment, critiques : critiques des frontières de la discipline, et critique de l'état du monde politique. Ils réinsèrent par la critique une dimension éthique dans la discipline. « Critique is … inescapably ethical, » rappelle David Campbell, « because it is concerned with change » (Campbell 2013, 214). L'objectif est d'ouvrir les relations internationales aux Autres des RI, tenants des approches marginalisées, et aux Autres de la politique mondiale, la vaste majorité de la population mondiale exclue de (et par) l'élite occidentale dont le statut social et la position de pouvoir sont réifiés par les discours abstraits sur les relations internationales.

[4] Pour Richard Ullman, qui écrit au cœur de la nouvelle guerre froide de la décennie 1980, le monopole d'attention pour la question militaire pose des ornières qui écartent d'autres enjeux non moins significatifs à la sécurité nationale. Un tremblement de terre au niveau de la faille de San Andreas, par exemple, comme une guerre nucléaire avec l'Union soviétique, est peu probable, mais engendrerait d'importantes conséquences pour la sécurité nationale des États-Unis (Ullman 1983, 139). Pourtant l'enjeu reste éclipsé des débats sécuritaires, au même titre qu'une foule d'autres telle que la rareté des ressources, une attaque terroriste, la détérioration de l'environnement, les conflits dans les pays du tiers-monde, l'immigration ou la surpopulation urbaine (Ullman 1983, 134-135). Ces enjeux sont ignorés sous motif qu'ils relèvent de politique intérieure ou qu'ils sont secondaires aux intérêts des grandes puissances, même si leurs conséquences sur la sécurité nationale peuvent être très importantes.

[5] Pour l'auteur, l'État ne peut être réduit à cette boîte noire positionnée sur la scène internationale face à d'autres entités de même nature dont les structures internes sont inaccessibles ou du moins secondaires pour comprendre leurs puissances relatives respectives (Waltz 1979, 79-101). Au contraire, pour Buzan la nature interne de l'État, compris comme structure administrative et institutionnelle, mais aussi comme idée, c'est-à-dire comme nation et idéologie, est cruciale. De fait, la puissance d'un État n'est pas uniquement liée à sa capacité matérielle économique ou militaire, mais dépend également de sa stabilité interne. Un État aux institutions défaillantes ou au nationalisme contesté est un État faible. Ainsi, selon les forces et faiblesses de cette structure interne, les menaces les plus sérieuses contre un État

D'autres ont également cherché à dépasser l'État comme objet référent de la sécurité lui préférant plutôt l'individu. Partant du constat partagé que l'État, par ses exactions contre sa propre population, est souvent une menace à la sécurité de l'individu, l'École d'Aberystwyth et les tenants de la sécurité humaine appellent, chacun à leur façon, à la réinsertion de l'individu au cœur des considérations de sécurité (Booth 1991; Programme des Nations Unies pour le développement 1994). Plus encore, la sécurité humaine propose une inversion du paradigme traditionnel. L'État n'est pas simplement écarté comme référent unique ou principal de la sécurité, désormais c'est l'individu qui doit être protégé contre l'État (F. Gros 2008, 57-59). Dans cette perspective, l'État n'est plus nécessairement protecteur de l'individu, mais se transforme souvent en bourreau (Weiss 2004).

La troisième opération critique consiste en l'approfondissement du concept de sécurité, c'est-à-dire à rejeter, au profit d'une définition alternative, la vision matérialiste d'une sécurité qui s'obtiendrait par l'accumulation d'armements. Le concept de sécurisation proposé par l'École de Copenhague est emblématique de cette opération. Sous l'égide d'Ole Waever, la sécurisation conçoit la sécurité comme un acte de langage « où le simple fait d'affirmer que quelque chose est un enjeu de sécurité fait en sorte que celui-ci le devient » (Grondin, D'Aoust & Macleod 2010, 475). Influencé par les théories linguistiques de John Austin sur la performativité de l'acte de langage, Waever écrit :

> *In naming a certain development a security problem, the 'state' can claim a special right*, one that will, in the final instance, always be defined by the state and its elites. … What then *is* security? With the help of language theory, we can regard 'security' as a *speech act*. In this usage, security is not of interest as a sign that refers to something more real; the utterance *itself* is the act. … By uttering 'security,' a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it (Waever 1995, 54-5).

Parler de sécurité, énoncer un enjeu comme un enjeu de sécurité fait de celui-ci un enjeu de *sécurité*. Être qualifié de sécurité déplace un enjeu hors du cadre législatif normal vers le registre de l'exceptionnel réservé au souverain. Cela permet d'avoir recours à des mesures extraordinaires que les représentants du souverain peuvent invoquer pour contrer la présence de menaces existentielles. La sécurité ainsi définie n'est donc ni objective, dépendante de l'existence d'une menace réelle, ni

peuvent ne pas être militaires. Buzan propose par conséquent d'étendre le concept de sécurité à cinq objets référents qui composent l'État : le militaire, le politique, le sociétal, l'économique et l'environnemental.

subjective, dépendante de l'appréciation d'une situation menaçante, mais bien intersubjective. Elle est définie socialement par l'interaction entre l'énonciation d'une menace existentielle et la reconnaissance de cette menace par un auditoire qui garantira la légitimité de l'exception (Buzan, Waever & de Wilde 1998, 21-47). Le concept de sécurisation représente davantage qu'une extension du concept de sécurité. Non seulement ouvre-t-il la possibilité à un nombre accru d'enjeux de devenir objets référents de la sécurité, mais il conteste la définition matérialiste de la sécurité et fait de la sécurité un objet de langage, un acte discursif performatif.

L'École de Copenhague n'est pas seule à vouloir approfondir le concept de sécurité. L'École d'Aberystwyth par exemple lie la sécurité à l'émancipation (Booth 1991; Booth 2005; Nunes 2012). « Emancipation is the freeing of people (as individuals and groups) from those physical and human constraints which stop them carrying out what they would freely choose to do, » écrit Ken Booth avant de poursuivre :

> War and the threat of war is one of those constraints, together with poverty, poor education, political oppression and so on. Security and emancipation are two sides of the same coin. Emancipation, not power or order, produces true security. Emancipation, theoretically, is security (Booth 1991, 319).

Dans la même veine, pour les tenants de la sécurité humaine, la sécurité signifie « deux choses essentielles : se libérer de la peur et se prémunir contre le besoin » (Programme des Nations Unies pour le développement 1994, 25). Malgré l'apparente similarité, il faut noter la différence entre les deux approches : alors que la sécurité humaine tend à dépolitiser et déhistoriciser les menaces qui pèsent contre les individus, le projet émancipateur de l'école galloise est éminemment politique, normatif et inclusif tant des individus que des collectivités (CASE Collective 2006, 455-463).

De ces différents projets, le concept de sécurisation se démarque. Son influence sur les études de sécurité est considérable au point d'en faire, dans les mots de Steve Smith, « un des développements les plus intéressants dans l'étude contemporaine de sécurité » (Smith cité par Grondin, D'Aoust & Macleod 2010, 476). Le concept n'est toutefois pas sans ses critiques : trop élitiste et insuffisamment sociologique (Huysmans 2002) gardant sous silence les inégalités de genre (Hansen 2000), imprécise quant à la nature et au rôle de l'auditoire de l'acte de langage (Balzacq 2005), trop étroitement centré sur les mots de la sécurité dans un univers d'images (M. C. Williams 2003), contributrice de la sécurisation du monde (J. Eriksson 1999). D'inspiration schmittienne, le concept de sécurisation de Waever, malgré son importante influence sur les études

de sécurité, demeure pris dans une définition exclusive du politique qui laisse, en dernière analyse, peu, voire aucune place à la réconciliation avec l'autre (M. C. Williams 2003; Aradau 2004). En ce sens, le concept de sécurisation n'est pas différent des approches traditionnelles de la sécurité établies sur une politique d'exclusion de ce qui est extérieur à l'espace social de l'État national.

2.2 Dé-essentialiser le concept de sécurité : que fait-on au nom de la sécurité ?

En parallèle à ces trois opérations critiques, une série de remises en question radicale inspirée des approches poststructuralistes souhaitent repolitiser le concept de sécurité. Aux côtés des critiques épistémologiques et ontologiques se greffent donc une critique éthique : une volonté de contester les aprioris sur lesquels sont fondées les études et les pratiques de sécurité. « If the objective (or at least the outcome) of much scholarship in security studies has been to render the question and problem of security apolitical and largely static, » écrivent Michael C. Williams et Keith Krause, « critical theory takes the question of change as its foundation, in both an explanatory and an evaluative sense » (Williams et Krause cité par Peoples & Vaughan-Williams 2010, 2).

Cette volonté de repolitiser une discipline sclérosée et un concept naturalisé, d'insuffler un vent de changement s'accompagne nécessairement, pour R.B.J. Walker, d'une réflexion sur la nature du politique que soutient la sécurité. « Security cannot be understood, or reconceptualized, or reconstructed, » écrit-il, « without paying attention to the constitutive account of the political that has made the prevailing accounts of security seem so plausible » (Walker cité par Huysmans 2006, 33). La proximité entre les deux concepts dans la pensée occidentale moderne oblige donc à reconsidérer dans un même élan le concept de politique sur lequel celui de sécurité se fonde. Williams et Krause le rappellent : « security is a derivative concept; it is in itself meaningless. To have any meaning, *security* necessarily presupposes something to be secured; as a realm of study it cannot be self-referential » (M. C. Williams & Krause 1997, ix). Or, implicitement, la réponse traditionnellement apportée à cette question, à savoir ce qui doit être sécurisé, est l'État.

Pour Anthony Burke, cette association à l'État fait de la sécurité un pilier de la modernité. Elle constitue, dans les mots de l'auteur, ce « overarching political goal and practice that guarantees existence itself, that makes the possibility of the world possible » (A. Burke 2002, 3). En quête d'une justification séculaire à la collectivité politique, les penseurs de la modernité de Hobbes à Locke à Rousseau justifient le politique par le contrat social. L'individu s'associe à ses pairs pour

garantir sa sécurité et sa prospérité. Par ce contrat, l'individu soumet sa propre sécurité à celle de l'État qui obtient du coup la responsabilité d'assurer la protection du corps social en entier. Il doit aussi se protéger lui-même puisque la survie du corps social dépend de la survie de l'État (Campbell 1998, 43-51). Dans l'impossibilité de garantir une fondation religieuse ou métaphysique à l'existence de la collectivité, le discours de peur de l'autre devient central à la légitimité de l'État qui doit justifier son monopole sur la violence. Campbell explique :

> securing identity in the form of the state requires an emphasis on the unfinished and endangered nature of the world. In other words, discourses of 'danger' are central to the discourses of the 'state' and the discourses of 'man.' In place of the spiritual certitude that provided the vertical intensity to support the horizontal extensiveness of Christendom, the state requires discourses of 'danger' to provide a new theology of truth about who and what 'we' are by highlighting who or what 'we' are not, and what 'we' have to fear (Campbell 1998, 48).

Dans ce processus, la sécurité de l'État est scindée en deux sphères : intérieure et extérieure. La première devient la sphère d'intervention de la police, alors que l'appareil diplomatico-militaire doit veiller à l'équilibre des puissances dans la seconde. Les relations internationales, et le champ de savoir qui dit détenir la connaissance sur cet objet, sont ainsi intrinsèquement liées au politique, constitutives de la communauté politique (Foucault 2004b, 293-340; Campbell 1998; Walker 1993). Chaque communauté politique, détentrice de la souveraineté et par le fait même des clés de l'État, justifie son existence particulière en assurant l'homogénéité interne et protège son autonomie contre la menace que constitue l'autre (Hardt & Negri 2000, 83-101). « [L]a sécurité n'est [plus] simplement associée à la protection de l'État, » écrivent Grondin, D'Aoust et Macleod,

> elle est partie intégrante d'un état d'être (*state of being*) que l'on construit, renouvelle ou modifie (Burke, 2007). Défendre la sécurité de l'État, c'est en même temps participer à la consolidation de son identité… Parler de la sécurité nationale revient à cautionner l'idée de souveraineté, à la créer littéralement en établissant des frontières internes/externes (Grondin, D'Aoust & Macleod 2010, 477).

En liant sécurité et État, on comprend que « [t]he concept of security is not empty; it implicitly invokes and relies on a series of accepted prior visions of what is to be secured » (M. C. Williams & Krause 1997, x). L'association sécurité-État n'est pas sans conséquence. Elle postule un monde politique dans lequel l'État occupe une place prépondérante aux dépens de l'individu ou de la société internationale par exemple, mais aussi un monde qui oppose les communautés politiques les unes contre les autres. Le concept de sécurité repose ainsi sur une aporie. Malgré la

prétention à faire de la sécurité un concept universel auquel tous peuvent tendre, la notion de sécurité individuelle et nationale se justifie aux dépens de l'autre.

Les critiques du concept de sécurité montrent son instabilité. La métaphysique moderne qui lie dans un noble mensonge la sécurité à l'État n'est plus tenable. D'une part, les violences et menaces que font peser les États à l'endroit de leurs propres citoyens remettent en question les prémices de l'État protecteur (F. Gros 2008). Pour Burke, « [they] undermin[e] the illusory unity of a body politics that would subsume all differences beneath a common imagination of home » (A. Burke 2002, 4). D'autre part, nous dit Burke, les contestations, propositions et autres élargissements du concept de sécurité révèlent le manque de stabilité et l'absence de fondation du concept. Dans ce contexte, plutôt que de chercher à étirer le concept dans tous les sens au risque, comme l'écrit Walker, de faire face à un « epistemological overload » (Walker cité par A. Burke 2002, 4), il faut abandonner l'idée de trouver une définition préalable au concept. Ainsi, les études critiques de sécurité « no longer treat [security] as groups of signs (signifying elements referring to contents or representations), » écrivent Can Mutlu et Mark B. Salter paraphrasant Foucault, « but as practices that systematically form the objects of which they speak » (Mutlu & Salter 2013, 113). Elles refusent le concept de sécurité comme objet dont la signification serait évidente pour s'intéresser à ce qui est fait au nom de la sécurité :

> Central to [Critical security studies] is the shared assumption that security threats and insecurities are not simply objects to be studied or problems to be solved, but the product of social and political practices. CSS aims to understand how those practices work and their social and political implications (Aradau et coll. 2015, 1).

Les études critiques de sécurité, influencées notamment par les approches poststructuralistes, proposent une révision en profondeur du concept de sécurité tel qu'il est traditionnellement compris depuis la révolution moderne. En cherchant à repolitiser l'appareil théorique permettant de comprendre la politique mondiale, elles remettent en cause l'objectivité des concepts sur lesquels reposent le savoir et la pratique des Relations internationales. Cette critique est à la fois épistémologique, ontologique et éthique (Campbell 2013; Hansen 2006, 1-36; Grondin 2010a). Épistémologique, car elle remet en cause la prétention à l'objectivité du savoir qui anime les approches traditionnelles des études critiques de sécurité. Ontologique, car elle historicise le savoir : montre à travers la déconstruction derridienne, par exemple, l'absence de fondation des constructions discursives qui encadrent le monde politique ou, à travers la généalogie

foucaldienne, le processus de constitution d'un objet en tant qu'objet de savoir sur lequel il devient possible d'intervenir.

Enfin, la critique poststructuraliste est éthique, car elle invite à revoir les catégories qui ordonnent la politique mondiale et à dénaturaliser cet ordre social profondément exclusif et inégalitaire. Cette critique n'est toutefois pas simplement négative. « A critique is not a matter of saying that things are not right as they are, » écrit Foucault.

> It is a matter of pointing out on what kinds of assumptions, what kinds of familiar, unchallenged, unconsidered modes of thought the practices that we accept rest. … Criticism is a matter of flushing out that thought and trying to change it: to show that things are not as self-evident as one believed, to see what is accepted as self-evident will no longer be accepted as such. Practicing criticism is a matter of making facile gestures difficult (Foucault cité par Campbell 1998, 191).

La critique poststructuraliste se veut ainsi positive, forçant le politique au-delà des frontières. Pour Foucault, « [c]et *êthos* philosophique peut se caractériser comme une *attitude limite*. Il ne s'agit pas d'un comportement de rejet. On doit échapper à l'alternative du dehors et du dedans ; il faut être aux frontières. La critique, c'est bien l'analyse des limites et la réflexion sur elles » (Foucault 1994b, 574). Cette critique rejette l'exclusion de l'autre pour penser une politique non dichotomique où l'autre conserve une place aux côtés du soi (Connolly 1989; Mouffe 2000).

Dans ce contexte, les études critiques de sécurité approchent la sécurité dans une perspective sociale et historique plutôt que métaphysique, et observent sa participation à la gestion des populations. Suivant cette perspective, les études critiques de sécurité analysent les multiples rouages du contrôle « sécuritaire » : les connaissances et discours (Hansen 2006; Campbell 1998), les pratiques, procédures, planifications et luttes bureaucratiques (Bigo 2005; Neumann 2002; M. C. Williams 2007; Pouliot 2007), les affects (D'Aoust 2013; Managhan 2012), les objets (Salter 2015; Salter 2016; Amicelle, Aradau & Jeandesboz 2015), et les publics de sécurité (Walters & D'Aoust 2015). En filigrane, unifiant toutes ces perspectives avec un objectif critique commun, les études critiques de sécurité s'intéressent aux effets de la sécurité, aux protections, exclusions et autres marginalisations qui en résultent.

Les études critiques de sécurité constatent notamment le déploiement massif et intensif de mesures de sécurité qui, en ligne avec l'ordre économique et social néolibéral, « operates to mitigate insecurities through a series of political rationalities and technologies of governmentality » (Grondin 2010b, 78). Les mesures de sécurité gèrent la circulation et la contingence, assurent la

circulation des biens et des personnes tout en réduisant les risques à l'ordre politique. Contrairement à l'image statique de la sécurité et de la protection, symbolisée par le mur ou le bouclier, la sécurité doit, afin de permettre la maximisation de la société, assurer la circulation de ses forces (Pallister-Wilkins 2016). « Ce qu'on voit apparaître… » en adoptant une approche historique et sociologique de la sécurité, écrit Foucault,

> c'est un tout autre problème : non plus fixer et marquer le territoire, mais laisser faire les circulations, contrôler les circulations, trier les bonnes et les mauvaises, faire que ça bouge toujours, que ça se déplace sans cesse, que ça aille perpétuellement d'un point à un autre, mais d'une manière telle que les dangers inhérents à cette circulation en soient annulées (Foucault 2004b, 67).

Dans cette optique, les méthodes privilégiées sont l'identification des risques et des menaces existantes, l'intervention préemptive et la préparation contre les perturbations générées par de futurs événements déstabilisants qui ensemble contribuent à la sécurisation des sociétés occidentales (Amoore & de Goede 2008c; Hagmann & Dunn Cavelty 2012; Adey & Anderson 2012; Collier & Lakoff 2007; Dunn Cavelty, Kaufmann & Soby Kristensen 2015). Parallèlement, ces mesures intègrent à la dynamique sécuritaire une multitude de sphères sociales, la portée du dispositif de sécurité ne se limitant plus à la sphère militaire. Les politiques d'immigration (Bigo 1998; Huysmans 2006), la culture populaire (Weldes 1999; Caso & Hamilton 2015; Grayson, Davies & Philpott 2009), l'aide au développement (Duffield 2010a), l'environnement (Dalby 2002; Grove 2012), la santé globale (Elbe 2005; Aldis 2008; Fisher & Monahan 2011), la criminalité (Cockayne & Lupel 2009; Nordstrom 2007), les infrastructures (Coward 2009; Galland 2010; Aradau 2010) et l'organisation urbaine (Coaffee, O'Hare & Hawkesworth 2009; S. Graham 2009), pour ne nommer que ceux-ci, deviennent tous des espaces d'intervention du champ de la sécurité.

Malgré cette extension du registre d'intervention de la sécurité, les études critiques de sécurité observent que celle-ci demeure un mythe inatteignable, d'où l'importance d'analyser la sécurité dans sa perspective gouvernementale, de façon à comprendre les logiques, stratégies, technologies, pratiques et effets. Le contexte de la sécurité est précisément son impossibilité, car parler de la nécessité de protéger un objet contre une menace à venir crée du même coup l'insécurité liée à l'existence de la menace. Pour Ben Anderson, les mesures déployées par le dispositif de sécurité créent deux « suppléments au présent » : une menace et une promesse de sécurité. Les deux sont contradictoires, mais indissociables et contribuent à l'extension permanente de la sécurité. « Hence the radical ambiguity of security, » écrit Anderson. « It can never be fully achieved. We

can never be done with securing because it is dependent on invoking the future in a way that disrupts and opens up the here and now » (B. Anderson 2010, 229). Les pratiques de sécurité, dans la logique performative, créent ainsi les sentiments d'in/sécurité et le champ des professionnels de la sécurité. Cette impossibilité est reconnue et manipulée par les acteurs du champ de la sécurité qui peuvent ainsi justifier leur pertinence sociale (Bigo 2005; Grondin 2014). Ils peuvent le faire d'autant plus efficacement, ajouterait Anthony Burke, que la sécurité demeure un terme flou.

> Security forms a *political* technology *whose power partly derives from its aporetic structure*. A generalized opposition between society and its others has worked as an effective technology of fear to construct and police forms of national and ethnic identity… In short, security power lies in the very slipperiness of its significations, its ironic structure of meaning, its ability to have an almost universal appeal yet name very different arrangements of order and possibility for different groups of people. This is why it is pointless to try and stabilize security's ontology. It is better to track security's tactical and discursive power through its development as a constitutive account of the political (A. Burke 2002, 7).

2.3 Souveraineté, raison d'État, gouvernementalité : penser le gouvernement à travers Foucault

Les études critiques de sécurité remettent en question le concept de sécurité. Dans ce processus, plusieurs se tournent vers Foucault (Dillon & Neal 2011). Dans ses lectures au Collège de France (Foucault 2004b; Foucault 2004a; Foucault 1997), Foucault entreprend une généalogie de l'État moderne à travers laquelle il aborde plusieurs concepts-clés des RI — l'État, la sécurité, le pouvoir, le territoire, l'identité, la souveraineté, la mobilité. En continuité méthodologique avec ses précédents travaux sur la folie et les hôpitaux, la discipline et la prison, l'auteur s'intéresse au gouvernement et à l'État d'un point de vue extérieur, refusant de lui attribuer une existence ontologique a priori. Plutôt que d'entamer sa réflexion à partir des institutions, fonctions et objet du gouvernement et de l'État, Foucault s'intéresse aux technologies, stratégies et champs de savoir qui donnèrent naissance à l'État moderne libéral (Foucault 2004b, 120-122), aux « specific arts, practices and techniques, » écrit William Walters, « that have combined in different ways and at different times to make something called 'the state' thinkable and meaningful in the first place, and viable as a framework for conducting human behaviour » (Walters 2012, 12).

Partant du postulat que gouverner, « ce ne soit pas la même chose que "régner", ce ne soit pas la même chose que "commander" ou "faire la loi"… à supposer donc qu'il y ait une spécificité de ce qu'est que gouverner » (Foucault 2004b, 120), Foucault analyse les transformations dans « la

manière dont on conduit la conduite des hommes » (Foucault cité par Senellart 2004, 406) qui ont eu cours en Europe depuis la chrétienté et qui ont mené, observe-t-il, à la matérialisation de l'État et de l'art de gouvernement libéral tels qu'ils existent aujourd'hui. Dans cette perspective, l'État n'est pas un phénomène universel et anhistorique, mais une construction sociale circonscrite dans le temps et l'espace. La souveraineté, monopole du roi et point culminant de la communauté politique dans la tradition philosophique occidentale moderne, n'est pas la seule manifestation du pouvoir, c'est-à-dire la seule forme que prend l'exercice du gouvernement, ni même la forme emblématique de la conduite des humains par l'État moderne. Ainsi pour l'auteur, dans la genèse de l'État, la souveraineté apparaît comme une des différentes rationalités politiques utilisées en Occident aux côtés de la raison d'État et de la gouvernementalité qui sera, sans être exclusive, le mode de gouvernement libéral moderne. Chacune de ces rationalités de gouvernement conçoit le sujet à gouverner, l'objet du gouvernement et les pratiques de gouvernement différemment. « Sovereignty governs by means of a rule of law and the coercive capacity of political, administrative and judicial institutions, » résume Jef Huysmans.

> [Raison d'État] governs [through discipline] by administering the location and movement of individuals through the imposition of grids. … The grids shape what individual bodies can do, where they have to be, etc. at certain specified times. They are sustained by a panoptical power mechanism that internalizes the random possibility of surveillance in individuals… Govermentality governs a population rather than a people or individual bodies. It measures optimal developments in populations and creates conditions for these populations to develop within the boundaries that define their optimal status (Huysmans 2006, 39).

Articulée autour du pouvoir monarchique, la souveraineté fixe, par l'entremise du droit, la légitimité du pouvoir dans le corps du roi. C'est dans ce corps vivant, plutôt que dans la présence abstraite d'un État intemporel, que se loge la souveraineté (Foucault 1997). « Le roi est mort, vive le roi ! » clame la tradition royale française. C'est dans la permanence du corps monarchique que continue la souveraineté. La corporalité de la souveraineté se retrouve dans le rapport de domination qui s'installe entre le roi et son sujet, un rapport personnel. Le crime, ou le non-respect de la loi, s'inscrit ainsi dans une personnalisation du rapport souverain/sujet. « Le crime, outre sa victime immédiate, attaque le souverain ; » écrit Foucault, « il l'attaque personnellement puisque la loi vaut comme la volonté du souverain ; il l'attaque physiquement puisque la force de la loi, c'est la force du prince. » Dans ce contexte, poursuit-il, « [l']intervention du souverain n'est donc pas un arbitrage entre deux adversaires… c'est une réplique directe à celui qui l'a offensé » (Foucault 1975, 58-59). Le non-respect du droit qui circonscrit la souveraineté deviendra un

affront, un outrage direct au corps du roi, un crime de lèse-majesté contre lequel le roi imprimera dans le supplice la vengeance monarchique. Ainsi, le supplice, la justice pénale, tout comme la guerre découlent du même « droit du glaive » qui établit un rapport de domination personnel et absolu entre le roi et son sujet : une domination qui se matérialise dans le droit de vie et de mort. Cette domination absolue, à l'image du supplice, peut être « cruelle certes, mais non sauvage » (Foucault 1975, 50). Elle est encadrée par le régime de vérité particulier des supplices et, dans le cadre de la guerre, par l'invocation de la menace à l'existence du corps souverain (Foucault 1976, 177-178). Ce droit d'exception n'est pas arbitraire, mais circonscrit par le droit qui détermine ces moments d'excès (voir Schmitt 1988).

Quoique la tradition politique fasse de la souveraineté le cadre dominant pour comprendre l'État, nonobstant les transformations à l'environnement politique liées à la mondialisation qui ont cours depuis la fin du 20e siècle et qui pèsent sur elle (Dingwerth & Pattberg 2006; Krasner 2001; Rosenau 1992; Waltz 1999; Buzan, Held & McGrew 1998; Lévy 2008), Foucault démontre que la souveraineté comme mode de conduite des humains n'est pas si homogène. Elle est contestée dès le Moyen-Âge, en partie délaissée, en partie complétée par d'autres logiques de gouvernement : d'abord, par le pastoralisme chrétien, responsable de la conduite des âmes vers le paradis éternel, qui s'affiche tout au long du Moyen-Âge européen en parallèle au pouvoir terrestre du monarque ; ensuite par la raison d'État qui conçoit, à compter des 16e et 17e siècles, l'État au-delà du corps du roi (Walters 2012, 21-26). S'attarder exclusivement à la légitimation légale de la souveraineté ignore du coup les changements dans la conception de l'objet à gouverner et des outils à la disposition des gouvernants qui donnèrent à l'État son intelligibilité. En pensant au gouvernement plutôt qu'à la souveraineté, c'est la finalité qui change. Il ne s'agit plus de défendre un « bien commun » défini comme le respect des lois sur un territoire donné, mais de diriger des humains. « [L]a fin du gouvernement, » écrit Foucault, « … est à rechercher dans la perfection ou la maximalisation ou l'intensification des processus qu'il dirige, et les instruments du gouvernement, au lieu d'être des lois, vont être des tactiques diverses » (Foucault 2004b, 103).

Foucault identifie une nouvelle rationalité politique qui vient progressivement remplacer, à partir du 15e et 16e siècle, le rapport de souveraineté et penser la permanence du politique au-delà du corps du roi. L'État apparaît et devient l'objet du gouvernement de la raison d'État. D'une relation personnelle entre le suzerain et son sujet, le gouvernement devient une relation de permanence entre un État, dont l'existence est indépendante du corps vivant du monarque, et un

sujet dont le travail est crucial à la puissance de l'État. La rationalité de gouvernement qui s'établit dans les écrits dits cyniques des penseurs de l'État, les Machiavel, Bacon et Chemnitz, insère l'État dans la longue durée. À l'image de cette cosmologie naissante sous les impulsions de la révolution scientifique menée par Copernic, Galilée et Newton, l'État apparaît désormais comme une force autonome présente dans un univers composé d'autres forces concurrentes. Dans ce contexte, le roi a la tâche d'accroître les forces de l'État afin qu'il ne soit pas aspiré par la force d'attraction d'un autre État (Walters 2012, 26). « [L]'État fonctionne dans cette raison politique comme un objectif… » écrit Foucault.

> L'État c'est ce qui doit être au bout de l'opération de rationalisation de l'art de gouverner. C'est l'intégrité de l'État, c'est l'achèvement de l'État, c'est le renforcement de l'État… L'État est donc principe d'intelligibilité de ce qui est, mais c'est également ce qui doit être (Foucault 2004b, 294-295).

Objet d'intelligibilité du pouvoir, objet à protéger et à renforcer, l'État se retrouve dans un environnement hostile composé d'autres États dont il faudra naturellement se méfier. Pour ce faire et pour accroître les forces de l'État, la raison d'État propose deux instruments : un appareil diplomatico-militaire veillant à l'équilibre des forces — qui deviendra l'objet des Relations internationales présenté dans ce contexte comme acteur sur l'échiquier international (Waltz 1979) ou comme voix dans le concert des nations (Keohane 1984) —, et la police qui agira non pas comme bras judiciaire du roi, mais qui s'affairera à la croissance interne des forces de l'État.

La police détient un rôle-clé. À travers la régulation étroite des comportements et des circulations, celle-ci doit créer un ordre social productif et harmonieux. Elle intègre ainsi un troisième élément au code binaire du droit à savoir la transformation de l'individu (Foucault 2004b, 7). Menée par les pratiques disciplinaires de surveillance, de normalisation et d'examen, la police poursuivra deux objectifs : la maximisation de l'individu à travers une discipline du corps et l'incorporation de l'individu à la puissance de l'État. « Concrètement la police devra donc être quoi ? » interroge Foucault.

> Eh bien, elle devra se donner comme instrument tout ce qui est nécessaire et suffisant pour que cette activité de l'homme s'intègre effectivement à l'État, à ses forces, au développement des forces de l'État, et elle devra faire en sorte que l'État puisse en retour stimuler, déterminer, orienter cette activité d'une manière qui soit effectivement utile à l'État. D'un mot, il s'agit de la création de l'utilité étatique, à partir de, et à travers l'activité des hommes (Foucault 2004b, 330).

Dans cette optique, la police crée un ensemble de savoirs, d'institutions et de techniques dédiés au dressage de l'individu, à « la majoration de ses aptitudes, [à] l'extorsion de ses forces, [à] la croissance parallèle de son utilité et de sa docilité, [à] son intégration à des systèmes de contrôle efficaces et économiques » (Foucault 1976, 183).

Avec la raison d'État et la minutieuse régulation individuelle par la police apparaît un nouvel intérêt pour le gouvernement de l'individu, absent de la souveraineté. Le bonheur de l'individu devient objet de gouvernement. Cela n'est pas désintéressé, puisqu'il s'agit de « faire du bonheur des hommes l'utilité de l'État, faire du bonheur des hommes la force même de l'État » (Foucault 2004b, 334). Cette attention portée à la conduite des individus, à la façon dont ils mènent leur vie constitue une fracture importante d'avec la souveraineté, une importation partielle des thèmes pastoraux pour l'autogouvernement du soi qui seront davantage réaffirmés par la gouvernementalité libérale.

Constatant les limites et les paradoxes créés par les effets inattendus des régulations policières[6], certains penseurs et gestionnaires de l'État rejettent à partir de la fin du 18e siècle cette volonté de contrôle de la raison d'État au profit d'une approche plus souple du gouvernement l'économie, la population et la liberté. Rejetant la malléabilité infinie des individus postulée par la raison d'État et les excès de gouvernement qu'exigent ses exercices de transformations disciplinaires, les économistes définissent l'exercice du pouvoir comme la maximisation d'une vie « libre » et indépendante de l'État que l'État devra savoir orienter à distance (Foucault 2004b, 32-43). Avec « la pensée des économistes, » écrit Foucault,

> va réapparaître la naturalité [des mécanismes sociaux]… Ce ne sont pas des processus de la nature elle-même… c'est une naturalité spécifique aux rapports des hommes entre eux, à ce qui se passe spontanément lorsqu'ils cohabitent, lorsqu'ils sont ensemble, lorsqu'ils échangent, lorsqu'ils travaillent, lorsqu'ils produisent… c'est la naturalité de la société (Foucault 2004b, 357).

Face à ces mécanismes naturels qui deviennent, dès lors que l'on reconnaît leur statut « naturel », impossibles d'éviter, le gouvernement concernera la prise en charge d'une société civile « comme champ spécifique de naturalité propre à l'homme », indépendante de l'État, posé « comme vis-à-vis de l'État », qu'il faudra connaître pour pouvoir administrer (Foucault 2004b, 357).

[6] Comme dans l'emblématique cas de la régulation des disettes de grains où le maintien des prix bas plutôt que de permettre à tous d'acheter le grain contribue à sa rareté.

Pour les physiocrates et les économistes de la fin du 18e siècle, la question est donc celle d'introduire l'économie, « that is to say, the correct manner of managing individuals, goods and wealth within the family » dans le gouvernement de l'État en tenant compte de la naturalité du social (Foucault dans Amoore 2013, 15-16). Dans ce contexte, la loi du marché, qui fixe « naturellement » le prix des denrées en fonction de l'offre et de la demande, s'établit comme guide de la gouvernance libérale. « the market will assume the status of a special place in the conduct of liberal governance, » écrit Walters, « it will appear as a 'natural' realm of processes located outside the political sphere, a zone of reality that will serve as a test of the frugality and wisdom of any state policy » (Walters 2012, 31).

Cette société « libre » et naturelle comporte deux visages. D'abord, celui d'une population autonome qu'il faut distinguer du peuple ou de l'individu. La population ne fait pas référence à l'entité politique collective issue du contrat social ni à la somme d'individus qui s'entassent côte à côte. La population existe à part entière, en tant que « *sui generis* reality, possessing its own properties and tendencies—a rate of crime, a rate of suicide, a rate of unemployment, a rate of birth and death » (Walters 2012, 34). La population est l'ensemble naturel d'éléments individuels et de forces autonomes qui composent la société. Elle est à la fois collective et individuelle, et surtout active : mue par le désir de ses individus (Foucault 2004b, 74-75). « La population, » écrit Foucault,

> c'est un ensemble d'éléments à l'intérieur duquel on peut remarquer des constantes et des régularités jusque dans les accidents, à l'intérieur duquel on peut repérer l'universel du désir produisant régulièrement le bénéfice de tous, et à propos duquel on peut repérer un certain nombre de variables dont il est dépendant et qui sont susceptibles de le modifier. … On a une population dont la nature est telle que c'est à l'intérieur de cette nature, à l'aide de cette nature, à propos de cette nature que le souverain doit déployer des procédures réfléchies de gouvernement (Foucault 2004b, 76-77).

Le deuxième visage de la société libre est celui du sujet économique rationnel, en quête d'une maximisation de ses préférences, qui existence non pas en terme transcendantal, mais comme produit social ou événement historique.

La reconnaissance de l'existence de ces deux sujets, population et sujet économique, est centrale, car elle justifie la frugalité du gouvernement. Plutôt que de s'interposer à l'intérieur de la population, par exemple en forçant la transformation individuelle, le gouvernement devra manipuler les intérêts, ou les désirs, que les individus chercheront à atteindre par eux-mêmes.

La gouvernementalité libérale visera ainsi la conduite de phénomènes naturels indépendants d'elle-même à l'intérieur d'un espace non plus clos, mais ouvert, un espace de circulation intérieur et entre les territoires (Walters 2012, 30-36).

Contrairement à l'esprit disciplinaire qui décortique chaque mouvement en vue de reconstituer la séquence la plus efficace, la rationalité économique laissera aux sujets le soin de leur propre maximisation et celle de la collectivité (Foucault 2004b, 7-8). « Le bonheur de l'ensemble, le bonheur de tous et de tout, il va dépendre de quoi, » demande Foucault.

> Non plus justement de cette intervention autoritaire de l'État qui va réglementer, sous la forme de la police, l'espace, le territoire et la population [et qui voulait] faire du bonheur des hommes l'utilité de l'État. Le bien de tous [dans la gouvernementalité libérale] va être assuré par le comportement de chacun dès lors que l'État, dès lors que le gouvernement saura laisser jouer les mécanismes de l'intérêt particulier qui se trouveront ainsi, par des phénomènes de cumulation et de régulation, servir à tous (Foucault 2004b, 354).

En ce sens, le gouvernement libéral devient l'art de la conduite de la liberté qu'il faut cultiver et protéger afin d'accroître le travail et l'échange. Dans cette optique, le gouvernement joue discrètement de poids et contrepoids, de statistiques et de normes, de probabilité et de calculs de risque, pour mesurer, influencer et diriger le constant mouvement des éléments disparates d'une population qui existent indépendamment de l'État.

Ainsi, l'État devra savoir gouverner, même face aux événements perturbateurs, en découvrant les relations normales qui habitent les populations gouvernées. Ce sera la naissance des sciences humaines « qui analysent [l'homme] comme être vivant, individu travaillant, sujet parlant » et qui émergent en parallèle de cette « population comme corrélatif de pouvoir et comme objet de savoir » (Foucault 2004b, 81). Ce savoir d'expert permet d'établir un gouvernement de normalisation qui procèdera par l'identification des cas (maladies, famines ou autres événements indésirables) et leur distribution dans une population « circonscrite dans le temps ou dans l'espace », de reconnaître les risques qui guettent chacun. Ce calcul de risque permettra à son tour de montrer les dangers, c'est-à-dire que les risques

> ne sont pas les mêmes pour tous les individus, à tous les âges, dans toutes les conditions, dans tous les lieux ou les milieux [qu'il] y a donc des risques différentiels qui font apparaître, en quelque sorte, des zones de plus haut risque et des zones, au contraire, de risque moins élevé (Foucault 2004b, 63).

La connaissance des mécanismes naturels des populations et leur normalisation par le gouvernement permettront de distribuer les risques et les dangers et d'établir les normes de conduite qui guideront l'action des individus (Foucault 2004b, 62-64). Contrairement à la raison d'État, la norme n'est plus fixée indépendamment de la population, mais résulte de la connaissance de celle-ci.

Si l'apparition de ces rationalités de gouvernement diffère dans le temps, montrant une chronologie du Moyen-Âge, à la Renaissance à l'époque moderne, il ne faut pas les penser selon une perspective téléologique ni prétendre qu'une viendrait remplacer définitivement l'autre. Pour l'auteur, plutôt que de remplacement, il faut parler de chevauchements et influences ; d'une relation triangulaire qui s'établit entre les trois (Foucault 2004b, 111). Néanmoins, on constate, à travers les transformations des rationalités de gouvernement, un déplacement d'abord de l'objet du gouvernement vers la vie humaine, ce que Foucault appelle la biopolitique, qui apparaît avec la raison d'État et se confirme avec la gouvernementalité libérale. Ce que le gouvernement doit désormais diriger, c'est la vie afin qu'elle se maximise. « [A]u vieux droit [souverain] de faire mourir ou de laisser vivre s'est substitué un pouvoir de faire vivre ou de rejeter dans la mort », écrit Foucault (Foucault 1976, 181). Le gouvernement de la vie humaine s'articule autour de deux pôles. Le premier sous l'égide de la discipline vise le dressage et la transformation du corps en corps docile en vue d'en tirer une productivité maximale ; le second, la conduite de l'humain pensé comme espèce vivante dans ses processus biologiques. Pour Foucault,

> [l]a mise en place au cours de l'âge classique de cette grande technologie à double face — anatomique et biologique, individualisante et spécifiante, tournée vers les performances du corps et regardant vers les processus de la vie — caractérise un pouvoir dont la plus haute fonction désormais n'est peut-être plus de tuer mais d'investir la vie de part en part (Foucault 1976, 183).

En marge du glaive du souverain qui sanctionne le droit de vie et de mort et du panoptique disciplinaire qui fixe l'individu dans une séquence préétablie, s'impose progressivement un dispositif de sécurité qui laisse libre cours à la circulation d'une population dans les limites de déviation acceptables par rapport à une norme optimale et d'une réflexion sur les aménagements sociaux qui permettent de modifier statistiquement le taux de délinquance (Foucault 2004b, 8).

L'intérêt de la gouvernementalité n'est pas d'y trouver une théorie complète sur l'état du monde (néo)libéral, mais une méthodologie, une sensibilité pour les microrelations de pouvoir, les

stratégies et technologies de gouvernement, et les résistances qui habitent la conduite des conduites humaines qui cadre bien avec les études critiques de sécurité (Walters 2012, 45). Pour Nikolas Rose, Pat O'Malley et Mariana Valverde, avec la gouvernementalité Foucault propose un

> ethos of investigation, a way of asking questions, a focus not upon why certain things happened, but how they happened and the difference that that made in relation to what had gone before. Above all, the aim of such studies is critical, but not critique—to identify and describe differences and hence to help make criticism possible (Rose, O'Malley & Valverde 2006, 101).

La gouvernementalité offre en outre un cadre intéressant pour comprendre la cohabitation d'une diversité de mécanismes de pouvoir (Huxley 2007, 187). La gouvernementalité invite à s'intéresser aux mécanismes de pouvoir au-delà de la souveraineté et de l'État. L'État n'est plus l'essence même du gouvernement (Miller & Rose 1990, 3). Ainsi, alors que les analyses politiques classiques situent l'État au cœur du politique pour s'intéresser ensuite aux institutions, fonctions et actions de l'État, la gouvernementalité se déplace à l'extérieur de l'État pour étudier les relations de pouvoir inhérentes au gouvernement. Le gouvernement devient un ensemble de technologies, de stratégies et de programmes qui diffèrent selon l'économie de pouvoir. La gouvernementalité permet alors d'analyser sous les trois angles des « technologies », de « l'analyse stratégique » et de la « constitution des champs, domaines et objets de savoir » (Foucault 2004b, 119-122), la diversité des modes de gouvernement et des micropouvoirs se manifestant dans des pratiques quotidiennes qui guident la conduite des humains. Ces mécanismes de pouvoir ne sont ni entièrement autonomes ni tous issus de l'État lui-même.

Dans le contexte de la gouvernementalité, la vision classique de l'État, détenteur unique de la souveraineté et garant de la sécurité nationale, « breaks down into a vast range of practices and private and public institutions that enact and develop strategies of government that arrange the conduct of freedom in modern societies » (Huysmans 2006, 40). Le pouvoir d'exception du souverain, remis à l'avant-scène par l'établissement de camps de prisonniers et de migrants, et les exécutions ciblées par drones (Agamben 1998; Chamayou 2013), n'est plus un moment de décision unique, mais le produit d'un long et complexe dispositif qui met en relation rationalité de gouvernement, technologie et subjectivité. « Though sovereign decisions of many kinds … may appear as sudden flashes, » rappelle Amoore,

> their apparent immediacy conceals a complex of calculation, consulting, analysis, algorithmic modelling and risk management that is the condition of possibility of

> contemporary security. … The sovereign strike is always something more, something in excess of a single flash of decision. … [The] very moment of the decision on the exception is a moment teeming with activity—with the authorization of new forms of authority, novel techniques of accounting for people and population, rafts of dividing practice that travel across social domains, thriving forms of control that circulate within the exception itself. The sovereign decision on the exception is not a void then; it is a productive space where things happen, a space filled with people, practices, techniques, and judgments whose effects may be violent or prejudicial in ways that we had not previously imagined. To profess the emptiness of the exception is to miss the politics that demands examination and response (Amoore 2013, 2 et 52).

La gouvernementalité permet plutôt de constater comment elles deviennent parties prenantes de « l'orbite de l'État » (Walters 2012, 51). Avec la gouvernementalité, écrit Gilles Deleuze,

> the State itself appears as the overall effect or result of a series of interacting wheels or structures which are located at a completely different level, and which constitute a "microphysics of power". Not only private systems but explicit parts of the machinery of State have an origin, a behaviour and a function which the State ratifies, controls or is even content to cover rather than institute (Deleuze cité par Walters 2012, 52).

L'État demeure, mais son monopole sur le gouvernement se dissout dans la multiplication et la capillarité des mécanismes de pouvoir. Dans le même élan, l'État ne se comprend plus en terme oppressif : l'État n'est plus cette pyramide de consentement et d'obéissance imaginée depuis de La Boétie (Bleiker 2000), mais un ensemble de technologies, de programmes et de stratégies qui guident la conduite des individus. Suivant le schéma conceptuel de la gouvernementalité, écrit Jacques Donzelot,

> [w]e would have then not a power and those who undergo it, but, as Foucault shows, *technologies*, that is to say always local and multiple, intertwining coherent or contradictory forms of activating and managing a population, and *strategies,* the formulae of government … theories which explain reality only to the extent that they enable the implementation of a program, the generation of actions; they provide through their coherence a 'practical object' (*practicable)* for corrective intervention of government programmes of redirection (Donzelot cité par Rose, O'Malley & Valverde 2006, 88).

Au-delà de la question de l'État, la gouvernementalité met à l'avant-scène le rôle des technologies, de la rationalité et du sujet. Cet intérêt pour les technologies ne signifie pas une nette distinction entre le monde matériel et celui des idées. « Rather, it is to suggest a particular kind of inquiry, one that draws our attention to the myriad devices, artefacts and objects that mediate power relations and populate our world » (Walters 2012, 62). Pour gouverner, l'État a besoin de technologies, procédures et autres dispositifs. Dans cette perspective, la technologie occupe donc

une position centrale, mais elle n'est ni un simple instrument au profit d'un objectif social particulier ni le moteur inéluctable de l'essor ou du déclin des sociétés humaines. Il s'agit de demander à la suite de Mitchell Dean : « by what means, mechanisms, procedures, instruments, tactics, techniques, technologies and vocabularies is authority constituted and rule accomplished » (Dean 2010, 42) ?

La gouvernementalité attire enfin l'attention sur la participation active des humains dans le gouvernement de leur propre conduite, dans ce qu'ils concevront comme leur propre finalité. Pour Foucault, le problème du gouvernement est de comprendre « how men govern (themselves and others) by the production of truth » (Foucault 1991, 79). Le gouvernement qui agit à distance par l'entremise du sujet autonome — « a subject, » écrit Huxley, « which is produced, not repressed, and is governed and governs itself as having capacities to act » (Huxley 2007, 188). L'expression « conduite des conduites » devenue emblématique illustre le rôle clé que la gouvernementalité attribue au sujet, rôle qui se module en fonction des « conceptions of the nature and obligations of those who [are] its subjects, those who [are] to be governed » (Rose, O'Malley & Valverde 2006, 86). Ces obligations ne sont toutefois pas à comprendre comme des formes d'oppression, mais s'inscrivent dans la définition de cette liberté devenue essentielle au gouvernement. La production du sujet passe ainsi par la mise en place de technologies de soi comme l'éthique, la pastorale chrétienne (Foucault 2004b), la discipline (Foucault 1975), l'aveu (Foucault 1976, 78-94), ou la liberté. Ces technologies d'agentivité, pour reprendre l'expression de Dean, « "seek to deploy our possibilities of agency" as a tactic or mode of governing » (Dean cité par Sending & Neumann 2006, 657). Avec l'invention de la liberté, écrivent ainsi Rose, O'Malley et Valverde, « [s]ubjects were obliged to be free and were required to conduct themselves responsibly, to account for their own lives and their vicissitudes in terms of their freedom » (Rose, O'Malley & Valverde 2006, 90–91). Les technologies de soi font toutefois l'objet de résistance et de tactiques de contre-conduite créant des marges d'où émergent des mutations et transformations dans les stratégies et technologies de gouvernement (Foucault 2004b, 363-365; Reynolds & Fitzpatrick 1999).

La gouvernementalité invite en définitive à s'intéresser à l'émergence, la permanence et les transformations des mécanismes de pouvoir qui conduisent les humains. Ces mécanismes ne se limitent pas à l'institution État ni ne relèvent d'une pensée entièrement cohérente. Au contraire, la gouvernementalité soulève l'hétérogénéité des pratiques, programmes, stratégies, technologies et savoirs qui s'additionnent, se complètent ou se concurrencent. Elle permet de penser les relations

de pouvoir dans la pluralité et de situer ces relations de pouvoir dans un contexte historique de lutte et d'émergence.

2.4 Sécurisation permanente : gouverner par le risque et l'outil de surveillance

Avec les transformations de l'objectif du gouvernement, c'est-à-dire le maintien de l'ordre social nécessaire à la promotion de la bonne vie, les objectifs de sécurité se déplacent. Plutôt que de chercher à préserver un territoire, le dispositif de sécurité veut assurer la continuité de la circulation des forces de vie contre les événements déstabilisateurs. Du coup, l'objet à protéger, le référent de la sécurité, passe du territoire, vu comme socle de l'État, à la population, constituante naturelle de la société (Dillon & Reid 2001; F. Gros 2008; Salter 2006). Ce qui ne signifie pas pour autant un désintérêt pour le territoire. Celui-ci est strié de nouvelles frontières qui sont autant de points de contrôle des mobilités, transformant l'environnement en technologie de sécurité (Deleuze 1990; Amoore 2013).

Ce recentrage de la sécurité sur la population entraîne dans son sillage une reconsidération des menaces. Tout ce qui peut porter atteinte à la bonne vie et au fonctionnement de la société devient un risque contre lequel il faut se prémunir. La menace ne se limite donc pas à l'apocalypse nucléaire, peur viscérale symbolique de la guerre froide, ni à l'invasion par une armée ennemie. Le spectre du risque est beaucoup plus large et devient un objet à administrer comme le montrent les évaluations ou registres nationaux de risque. Ces évaluations cherchent à identifier tous les risques, dangers, événements ou aléas auxquels un État pourrait faire face afin de les ordonner sur une échelle de priorité. Il ne s'agit pas simplement d'identifier les probabilités statistiques, mais comme le note Amoore, de dresser le portrait des risques possibles (Amoore 2013). C'est ainsi que Sécurité publique Canada définit le risque comme la « [c]ombinaison de la possibilité qu'un aléa donné se produise et des conséquences potentielles pouvant y être associées » (Sécurité publique Canada 2012, 85). Dans cette optique, les évaluations tous risques doivent permettre de répertorier la « gamme complète des risques, qu'ils soient naturels ou d'origine humaine » (Sécurité publique Canada 2012, 85). Pour Jonas Hagmann et Myriam Dunn Cavelty,

> [r]isk registers aim to represent public danger as broadly as possible, in the tradition of an 'all hazards approach'. Only through the identification of all possible hazards, the reasoning goes, can a complete national risk portfolio be assembled and policy responses prioritized and streamlined (see Netherlands, 2008: 5). Following this rationale, the central role of risk

> registers is not to debate what endangers popular well-being and what does not, but to make comprehensive information about all kinds of potential dangers available and comparable and, in the process, to make political programmes actionable (Heng, 2006a,b) (Hagmann & Dunn Cavelty 2012, 84).

La comparaison entre les différents risques existants doit permettre d'établir un plan d'action objectif, en accordant aux enjeux à faible probabilité, mais à grandes conséquences un intérêt particulier.

Au-delà des enjeux quant à la méthodologie déployée pour identifier, évaluer et comparer les risques, ce qui est intéressant ici c'est, d'une part, l'étendue du spectre des risques qui doivent être pris en compte par le dispositif de sécurité nationale. D'un feu de forêt ou d'un tremblement de terre, menaces naturelles, à la contamination à grande échelle de l'environnement, de médicaments ou de l'eau à de la désobéissance civile et au terrorisme, tout devient une source potentielle, quoique différenciée, de risque (Sécurité publique Canada 2012, 72). Cette extension infinie du risque contribue à une sécurisation continuelle, toujours à refaire, comme le dit Anderson, et qui englobe l'ensemble de la sphère sociale. Tout et tous, dans le plus menu détail de leur fonctionnement ou de leur vie quotidienne, se trouvent insérés dans une logique de sécurité sans que cela soit toujours conscient.

D'autre part, cet intérêt pour l'identification des risques afin de pouvoir déployer les mesures de prévention ou d'atténuation nécessaires invite à considérer le risque comme une technologie de gouvernement permettant de maintenir l'ordre social et de maximiser le profit. Le risque ne se réduit plus à cette crainte de l'inconnu, intrinsèque à la nature humaine, ou comme une prise en compte de notre limite à contrôler les produits de la modernité tardive (Beck 2009; Giddens 1991; Rasmussen 2002; M. J. Williams 2008; Mythen & Walklate 2008). Pour Aradau, définir le risque comme angoisse pose problème :

> « [it does] not account for how security problematizations function in concrete contexts, except as expressions of the unfunctional imaginary of security. … Rather than assuming a form of risk or disorientation characteristic of (post)modernity, problematizing the problematization of security focuses on the heterogeneity of representations and shows how interventions are made up of and assembled from various elements » (Aradau 2008, 54).

Même si le risque pourrait être nourri par ces craintes, pour comprendre ce qui est fait au nom de la sécurité, il devient plus pertinent de s'intéresser au risque comme technologie de gouvernement, comme stratégies et pratiques pour évaluer et prédire les conséquences qu'un

événement particulier peut avoir sur la vie d'une population et le fonctionnement de la société. Pour reprendre les mots de Nikolas Rose, dans la perspective foucaldienne, le risque est « [a] family of ways of thinking and acting, involving calculations about probable futures in the present followed by interventions into the present in order to control that potential future » (Rose cité dans Aradau & Van Munster 2008, 25). Cette perspective sur le risque permet de poser la question du gouvernement du risque et porte l'attention sur la planification d'actions et de politiques visant à assurer le respect des normes de fonctionnement social par la population. Le risque devient un objet de calcul et de gestion, d'évaluation de réussite ou d'échec, un outil de classification et de régulation (Foucault 2004b; Aradau & Van Munster 2007).

En ce sens, le risque est performatif : créateur d'ordre. « [T]he identification of risk is not the same as recognizing the uncertainty of future events, » écrivent Claudia Aradau et Rens Van Munster. « On the contrary, the identification and management of risk is a way of organizing reality. … Identifying the future as bearing catastrophic risks is therefore linked with visions of order and the ways to constitute and reproduce it » (Aradau & Van Munster 2008, 25–26). Cela devient possible toutefois, lorsqu'on reconnaît que le risque, malgré son imprévisibilité, est un phénomène sur lequel il est possible d'agir : en prenant en charge des évaluations tous risques, en mettant en place des mesures de prévention ou d'atténuation des répercussions afin de construire une société résiliente, en intervenant préemptivement (B. Anderson 2010). La gestion du risque est demande une attention minutieuse. Selon Sécurité publique Canada,

> [l]e traitement du risque est un processus d'élaboration, de sélection d'application de contrôles. Les traitements qui portent sur des conséquences négatives sont également connus comme une atténuation, une élimination, une prévention, une réduction, une répression et une correction de risque. Les options de traitement peuvent comprendre, sans s'y limiter : éviter le risque en décidant de ne pas poursuivre l'activité qui crée le risque ; supprimer la source du risque ; changer la nature ou l'ampleur de la vraisemblance ; changer les conséquences ; partager le risque avec une autre partie ; ou conserver le risque par choix (Sécurité publique Canada 2010, 23).

La conception de la sécurité en termes de risque permet d'agir dans le présent, malgré l'impossibilité réelle à prévoir avec certitude la nature de l'événement qui viendra perturber le fonctionnement de la société. À travers ces processus d'anticipation du futur que sont les scénarios et les évaluations de risque, le dispositif de sécurité ne cherche pas tant à l'identifier avec certitude qu'à transformer un futur incertain en objet d'intervention dans le présent (Salter 2008a; B. Anderson 2010). En voulant identifier tous les risques, en particulier ceux qui sont à faible

probabilité, mais engendrant de graves répercussions, ces « unknown unknowns » pour reprendre les mots de l'ancien Secrétaire à la Défense américain Donald Rumsfeld, ces processus dépassent les méthodologies d'évaluation du risque inspirées du génie. En favorisant l'imagination de dommages irréversibles et la scénarisation du pire pour penser l'impensable, le risque de sécurité introduit, comme le suggère Marieke de Goede dans son analyse de la prémédiation de sécurité, une nouvelle culture face à l'impensable (de Goede 2008b; Aradau & Van Munster 2008). Pour Foucault,

> la question qui se pose [avec le risque] sera de savoir comment maintenir, au fond, un type de [méfait], à l'intérieur de limites qui soient socialement et économiquement acceptables et autour d'une moyenne qu'on va considérer comme… optimales pour un fonctionnement social donné (Foucault 2004b, 7).

Or, les répercussions du risque impensable de sécurité sont trop importantes pour que le dispositif de sécurité accepte qu'il se produise, le jetant dans un paradoxe entre les moyens déployés et la possibilité d'empêcher un événement inconnu de survenir. Le renforcement de la résilience de la société afin d'assurer ses capacités à surmonter un choc traumatique illustre la prise en compte de ce paradoxe par le dispositif de sécurité (Dunn Cavelty, Kaufmann & Soby Kristensen 2015). Face aux événements à faible probabilité, mais engendrant de graves répercussions, la politique du risque zéro s'applique.

Les efforts consentis pour éviter l'impensable entraînent un bouleversement de la culture traditionnelle du risque renversant le fardeau de la preuve et favorisant l'action préemptive, légitimant une intervention avant qu'un événement ne survienne, malgré l'incertitude qui l'entoure (Aradau & Van Munster 2008; Amoore & de Goede 2008b). L'impensable est introduit dans le calcul du risque au prix d'une dépolitisation et d'un accroissement de l'économie de la peur. Le dispositif de sécurité n'a pas à justifier les origines ou à expliquer les conséquences de l'insertion d'un événement dans le calcul de risque, la volonté d'empêcher à tout prix qu'il se produise servant de paravent à toute contestation. L'acte d'imagination qui lui a donné naissance et la possibilité théorique qu'il se produise suffisent à l'isoler des critiques (Hagmann & Dunn Cavelty 2012; Amoore 2009b). Pour de Goede,

> [n]ot only does security premediation offer a fantasy of control and rational management of the uncertain future that 'depoliticises the limits of knowledge' (Best, 2006: 13–14); more worrying still is the fact that premediation is performative. This does not mean that disastrous imagined futures will inevitably play out, but it does mean that the imagination

> of some scenarios over others, the visualization of some futures and not others, entails profoundly political work that enables and constrains political decisionmaking in the present (de Goede 2008b, 171).

La dépolitisation de la sécurité engendrée par le risque est une des conséquences de cette conception de la menace déployée par le dispositif de sécurité. Amoore et de Goede identifient trois autres bouleversements provenant du risque : une fragilisation des concepts de souveraineté et de responsabilité, un passage temporel de la prévention vers la préemption, et un processus de (dé)construction identitaire (Amoore & de Goede 2008a). La part croissante de la gestion du risque entretenue par les acteurs privés fragilise la notion de souverain concédant des pouvoirs de décision à ce que les auteurs appellent, reprenant l'expression de Butler, des petits souverains (*petty sovereigns*) sur lesquels le public n'a peu sinon aucun contrôle. Amoore s'inquiète également des conséquences de la scénarisation du risque de sécurité sur la prise de décision. Qu'advient-il de la prise de décision lorsque toute action est scénarisée ? Pour l'auteure, suivant ici Jacques Derrida, la prise de décision implique un choix dans le contexte d'un futur incertain. Or, comme le futur d'un événement et de l'intervention est planifié à travers les scénarios de risque, il n'y a plus de décision possible, mais uniquement une série d'engrenages préprogrammés qui s'enclenche à la suite de l'alignement des bonnes variables. Dans ce contexte, le risque remet en question le concept de souveraineté en créant un flou autour de la personne qui prend la décision, c'est-à-dire autour du souverain, et en faisant disparaître l'acte de la décision et du même coup le fondement de la souveraineté (Amoore & de Goede 2008b, 180-183; Amoore 2011, 37-39).

Le dispositif de sécurité, qui agit de plus en plus par anticipation dans une logique de préemption, marque une rupture importante par rapport à l'approche préventive du risque. Alors que la prévention cherche à modifier l'environnement à la source du comportement répréhensible à travers des mesures non punitives, la préemption criminalise la source du risque avant même qu'il se produise. « Although pre-crime is justified on the basis of preventing crimes, » écrivent Jude McCulloch et Sharon Pickering,

> … pre-crime is not crime prevention as it is widely understood within criminology. Crime prevention is understood as non-punitive measures that reduce opportunities to commit crime or address the broader context in which people commit crimes through a range of social and environmental strategies (Sutton *et al.* 2008). Counter-terrorism pre-crime measures envisage specific serious harms and criminalize those whom it is believed will commit these imaginary future harms, while ignoring broader social and environmental factors. In short, pre-crime focuses on rooting out future terrorists rather than what might be thought of as root causes. Pre-crime measures are those measures that link substantial

> coercive police or state action to suspicion without the need for charge, prosecution or conviction. Pre-crime also includes laws and the police powers attached to them that expand the remit of the criminal law beyond the extant offences of conspiracy and attempts to include activities or associations that are deemed to precede the substantive offence targeted for prevention (McCulloch & Pickering 2009, 629–630).

Les deux ont ainsi un rapport au temps et au risque différent qui s'exprime dans l'intervention punitive. Dans la prévention, l'intervention punitive survient après l'événement, dans le contexte traditionnel d'une enquête et d'une condamnation. Au contraire, dans la logique préemptive, l'action punitive est prévue avant l'événement. L'événement lui-même pourrait ne jamais survenir, mais son imagination, sa mise en scénario, dans lequel une série d'activités, d'associations ou de transactions sont jugées révélatrices d'un comportement futur, et la gravité des conséquences qui lui sont associées légitiment l'intervention, en contravention d'avec le cadre légal conventionnel.

Enfin, le dispositif de sécurité transforme les processus de (dé)construction identitaire des individus qu'il soumet. Dans la recherche des comportements à risque, les identités des individus sont découpées en tranches d'informations, correspondant par exemple à un achat, un appel ou un déplacement, qui sont ensuite réassemblées pour former un profil de risque (Haggerty & Ericson 2000; Rouvroy & Berns 2010; Amoore & de Goede 2005; Raley 2013; Cheney-Lippold 2011). Ce travail identitaire a pour effet de sécuriser le quotidien occidental. À travers cette attention portée aux plus petits gestes quotidiens de chaque individu, le dispositif de risque métamorphose le banal en objet de sécurité de la plus haute importance. Le quotidien devient menaçant.

En sus de ces points de tension créés par le dispositif de sécurité et l'approche du risque relevés par Amoore et de Goede, je souhaite faire deux observations. Comme le faisait remarquer Foucault, le dispositif de sécurité démontre un croisement des genres de gouvernance. Même si l'exceptionnalité de la souveraineté peut davantage marquer l'imaginaire, le dispositif de sécurité déploie également des mesures disciplinaires et panoptiques (Bell 2015; Hristova 2014; Amoore 2007) et gouvernementales (Corry 2014; Adey 2006; Duffield 2010a). Sans prétendre à une cohérence parfaite entre toutes ces mesures et les agences qui les mettent en œuvre, s'en tenir exclusivement à un sommet du triangle ou forger une distinction nette entre chacune d'entre elles serait réducteur de la division des tâches et des chevauchements qui existent.

Définir la sécurité et le risque comme technologie de gouvernement mise en place pour assurer la gouvernance de plus en plus étroite des populations au nom de l'ordre et de la prospérité

nationale permet de comprendre la sécurisation du quotidien. La sécurité se fonde sur un besoin constant de connaissance pour pouvoir procéder aux évaluations de risque. Or, alors même que l'origine des risques à l'ordre social s'élargit continuellement, que les risques sont potentiellement plus déstabilisants, le besoin d'information se fait également plus pressant, d'où le sentiment de devoir collecter toute information afin de construire la banque de données la plus exhaustive possible. « You need the haystack to find the needle, » pour reprendre les mots du général Keith B. Alexander, directeur de la NSA de 2005 à 2014 (Gellman & Soltani 2013b). Cette volonté d'amasser toujours plus d'informations est fondée sur le constat, post-9 septembre 2001, que le défi pour le dispositif de sécurité consiste à établir des liens entre les informations disponibles. La connaissance des événements futurs existe dans les traces laissées ici et là. « In the aftermath of 9/11, the Madrid and London bombings, » écrivent Amoore et de Goede, « political authorities in the West have pursued the idea that knowledge about future risk is *always already present* in the data, if only information on transactions patterns can be effectively integrated and mined » (Amoore & de Goede 2008b, 174). La tâche du dispositif de sécurité consiste alors à trouver les informations pour pouvoir ensuite les analyser et les projeter dans le bon scénario de sécurité.

Dans ce contexte, la surveillance des individus, des infrastructures, des mobilités, des espaces urbains devient constante et omniprésente. La surveillance de masse des populations telle que mise à jour par les révélations d'Edward Snowden s'insère dans cet élargissement des considérations sécuritaires, participant à la sécurisation de l'espace numérique, mettant à jour le besoin d'omniscience et le sentiment que le risque et l'information permettant de le débusquer peuvent venir de partout. Dans tout ce processus de risque, la surveillance est à la fois présente et absente. Sans la surveillance, il est impossible pour le dispositif de sécurité d'observer la population et de calculer les déviations par rapport à la norme. Elle est les yeux du risque, une des clés matérielles pour faire fonctionner le dispositif. La surveillance est un des instruments du dispositif de sécurité, déployé dans une perspective de contrôle par la structure institutionnelle sécuritaire.

2.5 Au-delà du risque : la surveillance comme pratique culturelle et résistance

Les sociétés occidentales contemporaines sont soumises à une surveillance omniprésente qu'il est pratiquement impossible d'éviter (Lyon 2001; Marx 2002; Introna & Murakami Wood 2004; Monahan 2006b; K. Ball, Haggerty & Lyon 2012). Toutefois, réduire la surveillance à sa

cristallisation institutionnelle dans le dispositif de sécurité et à la structure de contrôle du risque rend mal la portée sociale de la surveillance. L'ubiquité de la surveillance ne s'explique toutefois pas uniquement par le dispositif de sécurité et les pratiques commerciales des grands acteurs de l'économie numérique, mais parce que la surveillance transcende les espaces publics et privés : elle est présente sur la rue, dans les transports en commun, dans les centres commerciaux, les écoles, les maisons, etc. Toutes ces formes de surveillance participent à la formation de ce qu'Haggerty et Ericson ont appelé un assemblage de surveillance, la combinaison d'une multitude de systèmes de surveillance (Haggerty & Ericson 2000, 610). L'assemblage soumet ainsi les populations occidentales aux structures de contrôle que sont le néolibéralisme et la sécurité et participe au rêve d'une gouvernance ciblée, diminuant les interventions et les blocages aux forces naturelles de la société (Valverde & Mopas 2004).

Dans cet assemblage, la surveillance n'est pas simplement une technologie. Comme l'explique Lyon, la surveillance est une pratique de gouvernement qui fonctionne par la catégorisation sociale (Lyon 2003; Gandy 2012). Quoique cette pratique ne soit pas nouvelle, l'omniprésence des technologies de l'information et des communications a rendu possibles un raffinement encore inégalé des catégories et l'automatisation du processus de catégorisation sociale (Monahan 2010, 9-10). Si les effets disciplinaires et restrictifs de la surveillance sont régulièrement réitérés, Lyon rappelle que la croissance de la surveillance est étroitement liée au développement de l'État-providence et à la démocratisation des droits sociaux et politiques. L'État se devait de connaître sa population pour lui fournir des services (Lyon 1994; Lyon 2001; Lyon 2010). Pour plusieurs, la surveillance est également une technologie permettant d'assurer la protection des enfants à la maison ou à l'école et un instrument de socialisation (Katz 2008; Katz 2006; Regan & Steeves 2010). En ce sens, réduire la surveillance à l'objet de toutes les peurs ou accuser les utilisateurs de fausses consciences est simpliste. Le rapport à la surveillance ne peut pas se limiter à cet imaginaire d'une technologie de contrôle emprisonnant le citoyen dans un panoptique ouvert et sans frontière. La surveillance doit se comprendre en fonction de ce qu'elle permet ou ne permet pas, en d'autres mots à son effet. Lyon propose ainsi d'étudier et d'évaluer la surveillance selon trois thèmes : la participation permise ou contrainte par la surveillance, la subjectivité que celle-ci contribue à construire, et son objectif. Dans la même veine, plusieurs auteurs se sont intéressés au potentiel émancipateur de la surveillance (Albrechtslund & Dubbeld 2005; Albrechtslund & Lauritsen 2013; Ellerbrok 2010; Regan & Steeves 2010). Monahan, Philips et Murakami Wood,

éditeurs d'un numéro spécial dans la revue *Surveillance & Society* sur la question, invitent à s'intéresser au design de la surveillance pour mieux comprendre si elle permet une plus grande égalité et favorise la participation et de quelle manière elle s'y prend (Monahan, Phillips & Murakami Wood 2010).

Les observations sur l'efficacité et la nature totalisante de la surveillance sécuritaire ne parviennent pas, par exemple, à expliquer la légitimité que beaucoup accordent à la surveillance, cette volonté d'être surveillé et de participer activement à sa propre surveillance et à celle des autres. Comment expliquer, comme le demande John McGrath, qu'autant de personnes souhaitent participer à des émissions de téléréalité (McGrath 2004) ? Comment expliquer que l'on accepte de surveiller nos enfants dans les écoles ou à la maison (Katz 2006; Katz 2008; Nelson & Garey 2009) ? De s'exposer dans les médias sociaux (Regan & Steeves 2010; Marwick 2012) ? Plus généralement, comment expliquer que l'on se soumette volontairement à la surveillance (Ellerbrok 2010; Ellerbrok 2011; Marx 2006; Albrechtslund & Dubbeld 2005) ? Pourtant la question de la participation individuelle à la surveillance, et en sous main celle de la nature totalisante de l'assemblage de surveillance et de l'agentivité de ceux qui lui sont soumis, est cruciale.

Une position mitoyenne entre la technophilie sécuritaire qui voit dans la surveillance l'omniscience nécessaire à la sécurisation d'une nation en péril et la technophobie paralysée par les scénarios dystopiques est nécessaire. Une position mitoyenne prend le temps de remettre la surveillance dans son contexte. Certes, la surveillance telle qu'elle est utilisée par les appareils de sécurité occidentaux contribue à la sécurisation du quotidien, au contrôle et au modelage de subjectivités. Elle est discriminatoire et disciplinaire. Toutefois, malgré les valeurs et fonctions qui se matérialisent dans la technologie, celle-ci demeure néanmoins ambivalente, ouverte à la réappropriation. L'art de surveillance, malgré ses échecs et limites comme ont pu le soulever les membres du F.A.T. Lab, offre une manifestation de réappropriation des technologies de surveillance et une contestation de la monopolisation de la surveillance par les dispositifs de sécurité occidentaux.

Dans leur remise en question des postulats conventionnels de la sécurité, les études critiques de sécurité proposent de s'intéresser à celle-ci non plus à partir des associations traditionnelles entre sécurité, État, et instabilité extérieure, mais sous l'angle du gouvernement. Sous celui-ci, la sécurité est une technologie de gouvernement développée, orchestrée et déployée par un ensemble

d'acteurs, dont l'État, afin d'assurer le maintien de l'ordre social et la maximisation de la société conformément aux normes économiques néolibérales. Plus récemment, en lien notamment, avec l'ascension de la menace terroriste au sommet de la pyramide des peurs sociales, le dispositif de sécurité s'est organisé autour de la notion de risque plus fluide et managériale que le concept de menace (Corry 2014). En parallèle au risque, la surveillance a acquis une importance particulière pour permettre d'accumuler l'information nécessaire au risque. Alors que les études critiques de sécurité tentent de déboulonner les grands mythes étatiques pour mieux éclairer la contingence de la sécurité, un danger pointe : celui d'ériger un nouveau mythe, gouvernemental celui-là, où la structure de pouvoir issue du dispositif de sécurité serait également cohérente et totalisante. « [T]he contemporary politics of possibility poses a specific and unique problem for the capacity of critical response and intervention, » écrit Amoore.

> That is to say, the politics of possibility appears to occupy the same terrain—of unknown subjects, acting upon the excess, thinking nonlinear relations—that has for so long provided resource for politics and critique. … The politics of possibility says that no person or thing may land in unexpected places, no person or thing may arrive anywhere unless they are already anticipated, risk scored, and biometrically anchored. All life in the politics of possibility has, in Gilles Deleuze's terms, a definite article—*the* life—identifiable, locatable, securable. The life that is the object of technologies of possibility is life as it is manifested in the individual, properly belonging to specified moments. The shapes not yet imagined are imagined by means of inferring definitive life—rendered thinkable by association rule, linkage analysis, data mining, and risk visualization. The bell-shaped curve of probabilities is replaced by the imagination of the possibilities that dwell in the "tail risk," the unknown is made amenable to knowledge (Amoore 2013, 155 & 157).

Afin de pouvoir continuer d'affirmer la fragilité de cette structure de pouvoir et pour répondre à la question de la participation à la surveillance, il faut accepter de séparer la surveillance sécuritaire du concept plus large de surveillance. La surveillance sécuritaire qui s'exerce à travers la logique du risque est une pratique de la surveillance, mais ne représente pas l'entièreté des possibilités qu'offre le concept. Abstraction faite du cadre sécuritaire, comment peut-on définir la surveillance ? Pour Haggerty et Samatas, la « surveillance involves assorted forms of monitoring, typically for the ultimate purpose of intervening in the world » (Haggerty & Samatas 2010, 2). Dans cette définition, il est possible de distinguer deux éléments. Premièrement, un objet, une forme de surveillance, un regard. La surveillance implique un instrument, comme un système de télévision en circuit fermé, ou une technique, telle que la surveillance des pairs. Deuxièmement, la surveillance comporte un but, une intention. Il ne s'agit pas seulement de voir, mais bien de voir

pour agir. Cela peut aussi bien être pour contrôler des individus indésirables, comme dans le cadre sécuritaire, que pour assurer des soins (Lyon 2001).

Monahan propose une définition sensiblement différente de la surveillance. Pour l'auteur, la surveillance doit être pensée au-delà de l'instrument, plus largement comme une pratique sociale à laquelle se greffent des acteurs, des technologies et des effets :

> Rather than analyzing surveillance technologies, for instance, as exogenous tools that are mobilized by actors to deal with perceived problems or needs, studying surveillance as cultural practice would understand these technologies a priori as agential (as 'actants' within a social system) and constitutive of knowledge, experience, and relationship (Monahan 2011, 496).

En même temps, pour Monahan, la surveillance demeure une pratique de contrôle. « [S]urveillance can be defined, » écrit-il, « as the systematic monitoring of people or groups in order to regulate or govern their behavior » (Monahan 2011, 498). En mettant à l'avant-scène l'idée de contrôle, Monahan accentue la nature politique et contraignante de toutes formes d'intervention. La rationalité de surveillance n'est pas simplement un agir au sens large, mais une action de régulation et de gouverne qui passe nécessairement par une forme de pouvoir et de contrôle, peu importe qu'il s'agisse du contrôle des autres ou de soi, comme l'on voit dans le cadre des pratiques de quantification du soi, ou que la surveillance soit bien ou mal intentionnée. En effet, une offre de soin ou de protection peut très bien s'avérer restrictive, malgré les bonnes intentions qui la sous-tendent, que ce soit au minimum dans la nécessité d'être enregistré et classé pour pouvoir en bénéficier (Lyon 2010). La surveillance est une pratique politique, une pratique de contrôle.

En outre, Monahan rappelle la nature intrinsèquement politique des technologies de surveillance. Un objet technique n'est jamais neutre, mais toujours inscrit politiquement à travers son design. En effet, un objet est construit de façon à assurer ou maximiser l'atteinte d'un objectif préalablement défini et son design constitue en soi une contrainte d'utilisation pour celui qui n'en partage pas le savoir technique (Feenberg 1999; Winner 2006; C. Weber & Lacy 2011). Par conséquent, l'argument voulant que la surveillance soit neutre en soi, mais que ce soit son utilisation qui pose problème est incomplet. Il faut plutôt chercher à réinsérer la politique dans la technologie ou, pour reprendre les mots de Monahan : « [to] frame technologies, including those of surveillance, as political in their own right, apart from how they are used » (Monahan, Phillips & Murakami Wood 2010, 92). Plus qu'un instrument du risque, la surveillance est une pratique

culturelle menée par des acteurs, des institutions, à l'aide de technologies, suivant des stratégies et rationalités planifiées sans être pour autant parfaitement cohérentes, et ayant des effets de pouvoir.

Torin Monahan, David J. Phillips et David Murakami Wood refusent de restreindre la surveillance au contrôle économique et sécuritaire. Pour les auteurs, son potentiel est multiple. « There may be an understandable predilection in Surveillance Studies of concentrating on institutional actors impinging on the rights and activities of others » écrivent-ils.

> After all, as John Gilliom reminds us, the word surveillance connotes domination: "If we think of surveillance as just *watching*, we err, because surveillance is never really just watching. It's not just vision, but *super*vision. It's not just sight, but *over*sight. Surveillance assumes, advances, and/or creates a relationship of domination" (Gilliom 2010: 205). The question for us is how can it be otherwise? Or, put differently, how might traditionally marginalized groups use surveillance to challenge their positions of marginality? Or, even broader, how can surveillance be designed, employed, and regulated to contribute to democratic practices and/or the social good (Monahan, Phillips & Murakami Wood 2010, 106–107)?

Pour les auteurs, « [s]urveillance involves not merely data collection, but creating social meaning from the data, and using that meaning to inform action. Data must be interpreted and that interpretation deployed » (Monahan, Phillips & Murakami Wood 2010, 110; voir également McGrath 2004). Cela n'empêche pas de voir dans la surveillance une forme de contrôle. Cette attitude vis-à-vis de la surveillance permet plutôt d'aborder ces enjeux sous un angle qui n'est pas nécessairement péjoratif, connoté négativement, mais de percevoir un plus large éventail du potentiel de la surveillance. « Taking seriously the social construction of surveillance necessitates a rejection of absolutes, » écrivent Monahan, Phillips et Wood.

> It becomes more difficult to say that some forms of surveillance are "good" and others "bad." Such value judgments depend on one's position in the system, and it should be the task of scholars to try to understand competing positions in a symmetrical and sympathetic fashion (Monahan, Phillips & Murakami Wood 2010, 107).

Cette définition ouvre la réflexion politique sur la surveillance en liant instrument, pratique et performativité de la surveillance. En outre, elle ouvre la possibilité d'une participation à la surveillance qui ne serait pas déterminée, c'est-à-dire une participation qui ne serait pas le résultat du dressage sécuritaire ou dans le but d'assurer le fonctionnement de cette surveillance sécuritaire. En d'autres mots, repenser le statut de la surveillance permet d'envisager la possibilité d'une agentivité dans la surveillance. L'ouverture à une participation alternative à la surveillance introduit sur le plan éthique la possibilité d'une relation autre à la surveillance, question qui s'insère

dans la préoccupation du champ pour les inégalités sociales causées par les politiques de sécurité (A. Burke 2002; J. Eriksson 1999; Hansen 2011; Huysmans 2006; Booth 2005; Krause & Williams 1997).

L'idée d'une participation autre à la surveillance ramène à l'idée de contestation et de résistance qui transparaît du concept de gouvernementalité. Dans la conception traditionnelle du pouvoir et de la résistance, le pouvoir est monopolisé par un groupe organisé et cohérent, généralement une minorité, et utilisé pour se maintenir au sommet de la pyramide sociale. Dans ce contexte, la résistance est vue comme un projet émancipateur dans lequel la reprise du pouvoir permet la création d'une nouvelle société plus libre et plus égalitaire. La résistance est alors conçue comme un geste de rupture. Le refus révolutionnaire et l'action d'éclat doivent assurer l'effondrement du pouvoir. Si tous retirent leur consentement, l'architecture d'autorité perdra son pouvoir, jetant à terre le régime existant et ses leaders, et permettant aux contestataires de s'approprier le pouvoir nécessaire à la mise en place d'une nouvelle société. Similairement, l'action d'éclat peut permettre de subtiliser aux autorités les assises du pouvoir. Ainsi, la prise de la Bastille et celle du palais d'Hiver auront permis de transférer les clés du pouvoir des mains des autorités vers celles des contestataires (Bleiker 2000; Raley 2009; Mittelman & Chin 2005).

Cette conception de la résistance, qui oppose participation et contestation de l'ordre, reprise autant par les mouvances marxisantes qu'anarchistes, fers de lance traditionnels de la résistance (Amoore 2005; R. W. Cox 1983; Gill 2002; Hardt & Negri 2009; Churchill 1998), postule implicitement la possibilité de sortir du système de pouvoir pour s'y opposer. La résistance vis-à-vis d'un ordre établi est extérieure à celui-ci et rendue possible par la confrontation de l'autorité détentrice du pouvoir et chargée du maintien de l'ordre. Dans cette projection de la résistance, l'héroïsme, le coup d'éclat et plus généralement l'action, opposée à l'inaction de la réflexion et de la critique, assurent le passage vers l'après. Toutefois, les moments révolutionnaires n'ont pas toujours le succès espéré. Tocqueville déjà montrait la permanence des institutions d'ancien régime malgré les tentatives des révolutionnaires de trancher avec le monde précédent et d'établir la société française libre sur un nouveau socle (de Tocqueville 1967). Les structures de pouvoir ont la vie dure. Les reculs vécus à la suite des printemps arabes semblent montrer encore une fois les difficultés des transformations révolutionnaires.

Dans le contexte de l'assemblage de surveillance ou de la surveillance mise en place par le dispositif de sécurité cela pose problème. Quelle est l'autorité issue de la structure de la surveillance qu'il faudrait contester ? La NSA ? La volonté de l'ancien directeur de l'agence, Keith Alexander, d'amasser toutes les données de communication ? Le gouvernement américain ayant autorisé la surveillance ? Google ? Facebook ? L'industrie des télécommunications dans son ensemble ? L'univers numérique ? Le néolibéralisme ? Le capitalisme ? L'avarice humaine ? Les terroristes ? Les efforts pour contrer le terrorisme ? Les citoyens inconscients des transformations sociales liées à la surveillance ? *24*, *Homeland* et autres séries de télévision et films complices ? L'échec des activistes à protéger nos droits ? La surveillance sécuritaire est composée d'acteurs disparates, de technologies, de procédures et de savoirs provenant de sources innombrables et dont la logique même demande d'être partout et de tout voir. La difficulté à attribuer les responsabilités dans l'expansion de la surveillance et de sa réarticulation à des fins sécuritaires complique la possibilité d'un rejet simple et univoque. « Storming the Winter Palace is no longer an option », rappelle Rita Raley (Raley 2009, 24), non pas à cause de l'inégalité des forces en présence, mais à cause de la pluralité des sites de pouvoir et de contestation.

Pour Foucault, la contestation révolutionnaire est une illusion. Le pouvoir n'est pas un échafaudage dont on pourrait simplement saper la base, ou un Léviathan auquel on pourrait mettre une tête moins hideuse. Pour Foucault, la résistance est inséparable du pouvoir. Elle est en constant rapport de force avec lui. De même que la liberté est un produit de la gouvernementalité afin de permettre aux individus de maximiser leurs profits, la résistance n'est pas extérieure au pouvoir. « The conduct of conduct covers the shaping or guiding of possible actions and norms by a diverse range of actors and institutions, » écrit dans Carl Death.

> … Freedom is therefore not in opposition to modern government, but is rather an essential technique, or product, of power. The free citizen and the free market, for example, are cornerstones of modern techniques of rule. By extension, resistance, commonly seen as an assertion of freedom, is itself bound up within networks of governmentality; and liberal democracy's toleration of dissent and protest within certain limits works, paradoxically, to reinforce as well as challenge dominant power relations (Death 2010, 238–239).

La résistance n'est pas une libération du pouvoir, mais cet Autre avec lequel le pouvoir est mis en relation. Or, comme le pouvoir ne peut être emmagasiné et qu'il se manifeste à travers des rapports de force multiples avec la résistance, il n'existe ni siège monopolistique du pouvoir ni, par conséquent, monopole de la résistance. « Il n'y a donc pas », pour reprendre Foucault, « par rapport

au pouvoir *un* lieu du grand Refus — âme de la révolte, foyer de toutes les rébellions, loi pure du révolutionnaire. Mais *des* résistances… Elles sont l'autre terme, dans les relations de pouvoir ; elles s'y inscrivent comme l'irréductible vis-à-vis » (Foucault 1976, 126-127). Le pouvoir comme la résistance apparaissent en de nombreux points de friction, non pas uniquement dans les grands épisodes révolutionnaires.

La résistance se manifestera donc de façon locale, tacticienne et éphémère. La contestation de l'ordre politique se fait ainsi dans une pluralité d'espaces et de temps qui permettra de contrer l'objectivation du savoir (Foucault 1976, 126; Raley 2009, 26-27). « Perhaps the notion that revolutionary resistance no longer requires a single spatiality, or Foucault's notion that "there is no single locus of great Refusal," » écrit Raley,

> means that power will not, cannot, reconstitute either on-site or in the hands of a limited few. If we have only a "plurality of resistances," a "being against," always and everywhere …, then in fact the teleology of revolutionary organization itself is disrupted. Instead of a single, spectacular disruption, we have a "multiplicity of discontinuous sites of enunciation" (Raley 2009, 24–25).

La contestation de l'ordre politique se fait ainsi dans une pluralité d'espaces et de temps qui permettra de contrer l'objectivation du savoir. Parce que le savoir n'est pas neutre, porteur de vérité, mais participe à la stabilisation du monde politique contre l'incertitude qui l'habite, le savoir représente le maillon faible des structures de pouvoir.

> Understood as both an instrument of power and a point of resistance or opposition, discourse 'transmits and produces power' while it also renders it fragile and 'makes it possible to thwart it' (Foucault 1976: 101). Read in these terms, the search for a great refusal overlooks the very site where the fragility and vulnerability of power relations may lie — in the discursive articulation between power and knowledge (Amoore 2006a, 259).

La critique du savoir permet à son tour de résister les conduites encouragées par l'ordre politique, la subjectivité imposée par les structures de pouvoir, nécessaire à ces structures de pouvoir et qui nous en rendent complices devient un cheval de bataille clé.

> [T]hough we may not be able to think of refusing 'it' in a clear and unambiguous way (whether it is war, globalization, poverty…), we can think of refusing what it makes of us. Our double standpoint within the exercise of power and the instances of resistance implies that we may be both vehicles of discourse and the means by which that discourse is undermined (Amoore 2006a, 259).

La contestation des conduites par la pratique de contre-conduite n'est pas extérieure au pouvoir, mais le fragilise et s'assure que son exercice n'est jamais lisse. « [A] counter-conducts approach looks within government to see how forms of resistance rely upon, and are even implicated within, the strategies, techniques and power relationships they oppose, » écrit Death (Death 2010, 240). Penser la participation alternative ou l'agentivité dans la surveillance ouvre la porte à une surveillance en contact étroit avec le pouvoir, néanmoins résistante, que ce soit à travers « [the] correct[ion of] power asymmetries » (Monahan 2010, 103) ou la réappropriation à d'autres usages que ceux convenus (Amicelle, Aradau & Jeandesboz 2015, 300–302).

2.6 Conclusion : vers une contre-conduite de la surveillance

Comment peut-on penser la surveillance à l'ère post-Snowden, cette ère où tout et tous sont soumis à la force disciplinaire de la surveillance du dispositif de sécurité américain ? S'il faut reconnaître l'étendue de la surveillance des communications à des fins de sécurité, et du même coup constater une volonté de centralisation des capacités de surveillance des données mondiales au sein des dispositifs américains et occidentaux, au point de revalider dans une certaine mesure l'hypothèse panoptique de Foucault, on ne peut limiter l'analyse de la surveillance et de la sécurité aux révélations de Snowden. D'une part, la surveillance n'explique pas à elle seule la lourde question sécuritaire. D'autre part, l'utilisation de la surveillance par l'État pour identifier les complots terroristes, et les risques à la sécurité nationale plus généralement, n'explique pas à elle seule la portée sociale de la surveillance.

La sécurité nationale est au cœur de la réflexion en Relations internationales depuis son institutionnalisation au début du vingtième siècle. Les postulats fondamentaux du concept, au premier chef l'État et la souveraineté, ont été et demeurent contestés, notamment par les études critiques de sécurité. Ces auteurs invitent à repolitiser le concept de sécurité pour chercher à comprendre, plutôt que de présupposer, ce que l'on fait au nom de la sécurité. Inspirée notamment par la philosophie de Michel Foucault, cette démarche épistémologique, ontologique et éthique conteste les prétentions à l'objectivité qui habitent les postulats traditionnels, dissèque l'État pour mieux visualiser les discours, pratiques et technologies mis en place pour assurer la sécurité nationale, et refuse la dichotomie entre le soi et l'autre. De là, les études critiques de sécurité redéfinissent le concept de sécurité et sa métaphysique : la sécurité est une technologie de

gouvernement, déployée pour guider et délimiter l'étendue d'action de sujets autonomes, et dont il est possible de tracer les transformations à travers le temps.

Le risque est une figure-clé de ces technologies de gouvernement contemporaine. Différent de la menace en ce qu'il est plus évasif et incertain, le risque structure la rationalité des dispositifs de sécurité. Face à l'éventail presque infini de risques à la stabilité de l'ordre social, le dispositif de sécurité intervient pour contrer les vulnérabilités : par des évaluations de risque, préemptivement pour éviter les événements à faible probabilité, mais à grandes conséquences, en se préparant pour faciliter la reconstruction post-catastrophe, etc. Le dispositif de sécurité se retrouve aux prises avec le difficile arbitrage entre la volonté d'éviter à tout prix une catastrophe d'ampleur et l'impossibilité de prévoir avec certitude, et plus encore de prévenir, un événement futur. Pour mener ce travail, la capacité d'acquérir les informations permettant l'évaluation et la projection des risques, c'est-à-dire de surveiller l'environnement, les circulations et les populations, est cruciale.

On ne peut toutefois restreindre la surveillance à son rôle de soutien logistique dans le dispositif de sécurité. Certes, la surveillance participe à la technologie de gouvernement qu'est le risque. Les technologies de surveillance sont toutefois déployées par une variété d'acteurs et d'institutions et une multitude de motivations qui dépassent largement le spectre sécuritaire. Dans cette perspective, contraindre la surveillance au statut de technologie instrumentale au risque ne fait pas honneur à la diversité de contextes où la surveillance apparaît, qu'il s'agisse de son utilisation commerciale, dans les médias sociaux, pour des fins de divertissement, pour conforter des parents inquiets, etc. Il devient plus utile, à des fins d'analyse, c'est-à-dire pour comprendre les structures et relations de pouvoirs qui s'y rattachent, de penser la surveillance comme une pratique sociale liant des acteurs, des institutions, des pratiques, des rationalités, des technologies et des effets. Ce faisant, on ouvre la porte à la réappropriation de la surveillance.

Les révélations de Snowden constituent un moment de rupture important. Il a nourri de nombreuses contestations fournissant un imaginaire ou des informations avec lesquels alimenter les critiques. Parmi ce lot, je tourne mon attention vers l'art. Souvent dans une dynamique de questionnement critique, l'art de surveillance est à la fois des pratiques de surveillance et des formes de contestation. Il constitue une manifestation de réappropriation des technologies de surveillance et une contestation de la monopolisation de la surveillance par l'assemblage de sécurité. En plus d'être éclairante par les enjeux soulevés, l'hybridité des technologies et pratiques

de l’art de surveillance offre un exemple de la complexité des dynamiques de pouvoir et de contre-pouvoir.

3 Politique de l'esthétique, art de résistance : vers une communauté d'artistes numériques contestataires de la surveillance algorithmique

> *The pursuit of thinking with artistic texts rather than generating and testing explanations is neither a retreat into abstractions that lack contact with the world nor an avoidance of ethical and political concerns. It is a practice of critique that should be understood both as a challenge to epistemological certainties and as a positive engagement with actual experiences and issues pertaining to them. That practice requires one to resist the institutionalized knowledge that contributes to coercive structures, to — in Foucault's terms — make those knowledge practices "fragile, temporary [and thus to turn those practices into] events, nothing less than events.*
>
> Michael J. Shapiro[1]

La nature de la relation entre l'art et la politique proposée par le tournant esthétique en Relations internationales (RI) s'inscrit dans une perspective résolument critique à la fois des frontières disciplinaires des RI et de la politique mondiale. Comme l'écrivent Alex Danchev et Debbie Lisle : « art matters, ethically and politically; affectively and intellectually. It is another way of apprehending the world. It has consequences. Not only does it make us feel, or feel differently, it also makes us think, and think again » (Danchev & Lisle 2009, 775). Pour ces auteurs, l'art et l'esthétique ébranlent les fausses « certitudes » et autres travers des approches dominantes en RI, élargissent la compréhension de la politique mondiale, éclairent et contestent la normalisation des structures de pouvoir (Bleiker 2001). Cela est possible, parce que l'art dérange, bouscule les conventions et l'ordre établi, s'ouvre vers l'alternative. Pour le tournant esthétique, cette ouverture à cette autre-chose-possible fait de l'art et de l'esthétique un espace privilégié de contestation et de résistance aux consensus actuels.

Porté par cet espoir de changement qui habite l'art, un grand nombre d'auteurs s'est intéressé à l'art, le décortiquant afin de comprendre le message politique caché en son sein (Neumann 1999; S. Chan, Mandaville & Bleiker 2001; Mandaville & Williams 2003; Sylvester 2009; Bleiker 2009; Moore 2010; Danchev 2009). La mobilisation de l'art en RI crée toutefois des vagues. Pour Cerwyn Moore et Laura J. Shepherd, cette recherche du message politique de l'art est

[1] (Shapiro 2013, xv)

souvent faite au prix d'une sous-théorisation du rapport entre l'art et les RI et d'un évitement, volontaire ou non, de littératures existantes sur l'art et la politique mondiale (Moore & Shepherd 2010, 303-305; Holden 2010). En outre, en faisant de l'art une image iconique, ces auteurs risquent de le fétichiser camouflant les rapports de pouvoir et de lui attribuer une pertinence politique sans approfondir ou clarifier de quelle façon l'art offre une avenue de résistance à la politique mondiale. Comme le rappelle Roland Bleiker, l'art n'est, par défaut, ni favorable au statu quo ni critique : « art can be as regressive as progressive. And so can politics. In fact, the very notions of progress and regress are highly arbitrary. Art takes place beyond these temporal and arbitrary spheres of judgement » (Bleiker 2009, 180). La difficulté consiste alors à trouver et à définir cet espace extérieur au jugement individuel permettant d'attribuer une dimension politique et sociale à l'art. Afin de dépasser la lecture du message de l'art, Bleiker, Moore et Shepherd, et plusieurs autres encouragent une plus grande théorisation du tournant esthétique. Implicitement, les auteurs appellent à dépasser le glissant concept d'art.

Parler d'esthétique plutôt que d'art s'inscrit dans la riche tradition philosophique occidentale. Dans sa conception moderne, la définition d'esthétique provient du 18^{e} siècle. Alexander Gottlieb Baumgarten baptisait l'esthétique « the science for directing the inferior faculty of cognition or the science of how something is to be sensitively cognized » (Guyer 2003, 25). Aujourd'hui, pour la philosophie continentale du moins, l'esthétique est la branche de la philosophie qui s'intéresse à la théorisation de l'expérience et à l'art comme site d'expérience. Pour Christopher Kul-Want, l'esthétique se situe au cœur du « changement paradigmatique », amorcé depuis Emmanuel Kant, qui a fait passer les préoccupations philosophiques « from the emphasis on metaphysical and Cartesian conceptions of truth to a preoccupation with experience and the instability of the subject » (Kul-Want 2010, 1).

S'intéresser à l'esthétique permet ainsi de pousser la réflexion au-delà de l'objet d'art. Mais pour accommoder la diversité des thèmes issus de la philosophie de l'art — l'art comme pratique et objet, les propriétés esthétiques, et l'expérience esthétique, l'ontologie de l'art, les représentations, l'expression d'émotions, l'interprétation de l'art, le jugement esthétique et le beau pour ne nommer que ceux-là (Levinson 2003, 4-9) — le tournant esthétique doit faire preuve d'une large souplesse au point de frôler, parfois, la luxation. Selon les auteurs, l'esthétique permet ainsi de s'intéresser au sublime, concept frère du beau (Bleiker 2009, 67-83; Jabri 2006; Devetak 2005; Shapiro 2018) ; au jugement esthétique (K. Ferguson 1996) ; à l'esthétique comme mode

d'organisation du monde sensible (Mirzoeff 2011; Shapiro 2013) ; à l'esthétique comme contestation du statu quo (Amoore 2006a; Shapiro 2013; Bleiker 2009) ; à l'art comme performance politique (Raley 2009; Amoore and Hall 2010; Taylor 2013) ; à la culture populaire — en particulier au cinéma hollywoodien — comme manifestation et constituante d'une culture politique (Weldes 2003; Grayson, Davies & Philpott 2009) ; aux émotions véhiculées par l'art (Bleiker 2009; Carter & McCormack 2006; Duncombe & Bleiker 2015) ; à l'interprétation de l'art (Holden 2006), à la politique de l'objet d'art (Sylvester 2009; A. Scott 2004).

Cette relation multiple avec l'esthétique peut être due à la nature inclusive — voire évasive — du concept d'esthétique. En fait, il est tentant de dire avec Nicolas Kompridis que l'esthétique refuse les frontières définitionnelles. Pour Kompridis, il faut comprendre l'esthétique comme le refuge des négligés, ce que les approches rationalistes dominantes excluent. « [M]uch of what is excluded or marginalized in the debates over what counts as cognition, reason, experience, meaning and agency ends up in the aesthetic category, a massive refuse bin for what we cannot fit into our received categories of understanding » (Kompridis 2014, xvi). Composé de négligés, le tournant esthétique s'intéresse aux négligés des RI. Les perceptions et l'instabilité du sujet rationnel, deux thèmes centraux de la philosophie de l'art, sont réarticulés par le tournant esthétique afin de faire des représentations et des émotions, deux dénominateurs communs. L'esthétique permet de reconnaître le savoir offert par les représentations, l'émotion et l'imagination négligées par le rationalisme dominant. Bleiker, qui offre une des théorisations les plus abouties du tournant esthétique, démontre ainsi la pertinence de l'art et de l'esthétique en RI. Le tournant esthétique, comme d'autres figures de la critique poststructuraliste (Hansen 2006, 73-92), souhaite briser les contraintes ontologiques de la discipline qui imposent, pour reprendre les mots de Bleiker, « an exclusive and often very narrow reliance on diplomatic documents, statistic data, political speeches, academic treatises and other traditional sources of knowledge about the international » (Bleiker 2009, 30). Poursuivant cette réflexion, je souhaite aussi démontrer la pertinence de l'art comme mode de résistance aux structures de pouvoir que Bleiker semble toujours en proie de laisser de côté dans sa discussion disciplinaire. Contournant les risques de fétichisation de la démarche artistique, je porte mon attention sur une communauté d'artistes numériques qui font de leur art une critique explicite des technologies et pratiques de surveillance.

3.1 La politique de l'esthétique (I, II & III) : l'antimimétisme et l'antirationalisme pour une nouvelle réflexion éthique

Le registre des perceptions, opposées par leur subjectivité à la neutralité objective des observations dites scientifiques, est un des grands négligés des RI. Michael Shapiro tout comme Roland Bleiker d'ailleurs (Bleiker 2001) campent en premier lieu le tournant esthétique dans l'univers sensible. Retournant à l'origine épistémique du mot, Shapiro rappelle : « in its original connotation aesthetics — *aisthitikos*, from the Greek — referred to the sensory aspect of perception » (Shapiro 2013, 30). Pour l'auteur, l'esthétique accorde un statut ontologique central aux perceptions. Dans la tradition (post)kantienne, les perceptions sont des objets de savoir en soi qui ne sont plus liés à l'existence métaphysique d'Idées desquelles les représentations ne seraient que pâles copies. Dans *Critique de la raison pure*, Kant libère ainsi la philosophie occidentale du monde des apparences dans lequel l'avait enfermé Platon (Kul-Want 2010, 4-5; Kant & Kul-Want 2010). Les représentations sont des réalités qu'il convient d'étudier pour ce qu'elles sont (Shapiro 2013, 1-2).

Dans la foulée de la critique poststructuraliste, le tournant esthétique s'intéresse à la nature sociale des représentations et se positionne, de fait, en porte-à-faux face aux approches dominantes des RI. Pour Bleiker, les approches positivistes « seek to represent politics as realistically and authentically as possible, aiming to capture the world politics as it 'really' is » (Bleiker 2009, 19). C'est ce qu'il nomme la prétention mimétique. Les représentations y sont des véhicules vers une réalité extérieure et objective. Dans ce contexte, le chercheur n'a pas à interpréter ces faits pour les comprendre puisqu'ils constituent une copie de la réalité. Cette copie peut être juste ou imprécise, utile ou inutile. Elle n'a d'autre valeur que son instrumentalité à atteindre une entité qui la dépasse et qui constitue le véritable objet d'étude. Le statut mimétique des représentations permet d'assurer la neutralité de l'observateur et de conserver une stricte séparation entre le chercheur et l'objet d'études (Bleiker 2009, 20). De cette façon, les approches dominantes en RI nient la nature esthétique, perceptible, du monde politique. Puisque les représentations ne sont autres que des duplicatas, ils ne laissent pas de place à l'expérience comme rapport au monde. Au mieux, l'expérience imprécise d'un événement peut-elle montrer les limites de la psychologie humaine (Jervis 1976).

La théorie esthétique conteste la prétention mimétique à pouvoir atteindre une réalité extérieure à la représentation. Bleiker rappelle que les perceptions n'ont pas d'existence a priori, il

faut chercher à comprendre la nature de ces expériences et leur origine comme phénomène individuel et social (Bleiker 2001, 513-514). Ces représentations, indissociables du politique, sont constitutives du soi et de notre rapport au monde. « [P]olitical reality does not exist in an a priori way, » écrit-il. « It comes into being only through the process of representation » (Bleiker 2001, 512). Or, la critique du mimétisme cherche à ouvrir ce processus de représentation. Pour celle-ci, la relation entre représenté (signifié) et représentant (signifiant) ainsi qu'avec l'observateur est plus complexe, et certainement pas neutre et objectif. Il est donc nécessaire de porter une plus grande attention à la façon dont ces représentations sont construites d'une part, et aux effets contraignants ou permissifs de ces représentations sur les pratiques politiques d'autre part. Cette attention ne doit pas être interprétée comme un déni de réalité comme certains opposants au projet postmoderne laisse entendre, mais met plutôt l'accent sur la nature politique des représentations. Pour Bleiker :

> To foreground the politics of representation is not to deny the existence of facts or to claim that the 'real' world does not really exist. It is, rather, to acknowledge that a political event cannot determine from what perspective and in what context it is seen. … Our effort to make sense of this event can thus never be reduced to the event itself. … It is a process through which we organise our understanding of reality (Bleiker 2009, 21).

Le processus de compréhension du réel est politique dans la mesure où il est fondé sur une interprétation du monde. Bleiker illustre cette idée en se tournant vers le tableau « Ceci n'est pas une pipe » de René Magritte. Que la représentation d'une pipe ne soit pas une pipe relève de l'évidence. Plus fondamentalement toutefois, Magritte invite, à travers ce tableau, à se questionner sur la nature même des représentations :

> [it] challenges the very notion of mimesis. It draws attention to what, in Saussurian language, is called the arbitrariness of the sign: the fact that the relationship between signifier (the drawing of the pipe) and the signified (the pipe) is contingent on a range of interpretative steps (Bleiker 2009, 22).

Le passage de l'interprétation d'un signifié à son objectivation comme signifiant s'inscrit dans des rapports de force qui politisent la représentation. En ce sens, « [r]epresentation is always an act of power » (Bleiker 2009, 24). Prétendre à la neutralité d'une représentation l'est également. Or, les approches mimétiques nient le processus d'interprétation des événements et la présence du politique dans la constitution de représentations en postulant l'objectivité du duplicata.

Reprenant l'interprétation de Kant proposé par Deleuze, Bleiker remarque que l'approche mimétique postule l'harmonie des facultés sous l'autorité de la raison. La domination de la raison

permet de voir un objet d'une seule façon : de lui attribuer son sens commun. Toutefois, cette harmonie imposée, qui fait disparaître la tension entre les différentes facultés, se fait au prix d'une perte d'expérience. L'esthétique permet de contester la conception traditionnelle des représentations et de se réapproprier toutes nos facultés comme sources indépendantes de savoir. Bleiker explique :

> By examining how the beautiful and the sublime generate an inherent tension between imagination and reason, [Kant] sought to find ways for allowing each faculty to cultivate its unique insights and passions. But what is communicated across irreducible differences between faculties should not and cannot result in a shared recognition of objects. These traversing and transgressing insights neither converge in common sense nor are they necessarily the object of any one faculty in particular. Rather than embarking on a project that requires synchronisation and submissive integration, aesthetics promotes productive interactions across different faculties (Bleiker 2001, 514).

Les multiples façons de percevoir un objet, mises au jour par l'esthétique, permettent de contester l'autorité de la raison sur l'imagination en démontrant l'importance de la dernière comme sources de savoir.

> It is in this sense, that Kant, despite his often problematic search for a transcendental subject, has inspired a tradition of critical thought that affirms contingencies and actively engages the struggle between reproductive and productive thought or, as Michael Shapiro prefers to put it, between 'the demands of reason and the work of imagination' (Bleiker 2001, 513–514).

Le potentiel transformateur de l'expérience et du savoir esthétiques constitue la deuxième pierre d'assise théorique du tournant esthétique. L'art n'est pas une représentation comme une autre. Il fait place à l'émotion et permet de saisir ces aspects du monde politique qui sont ignorés par les approches dominantes et d'imaginer le monde autrement. Notant la floraison de livres et de films portant sur les attentats terroristes du 11 septembre 2001, Bleiker y voit un exemple de l'importance de la créativité esthétique pour comprendre le monde politique. La raison, « unable to grasp the event in its totality », reste muette face au 11 septembre 2001, propose Bleiker. « The result is a form of crisis, a plunge into pain and loss that leaves one puzzled, unable to answer key questions or even express the emotions that are felt. This is one of the reasons why the immediate response to 9/11 was one of shock and a stunned silence » (Bleiker 2009, 51). Devant cette limite de la raison, l'esthétique offre une autre source de savoir pour comprendre l'expérience traumatique en capturant certains silences ignorés par les représentations conventionnelles du 11 septembre 2001. L'esthétique permet de voir ce que l'on ne peut plus voir, ce qui se cache au-delà des

représentations conventionnelles et de revaloriser le savoir émotionnel. Comme la pratique artistique active la fibre émotionnelle, elle devient un moyen privilégié pour accéder à ce savoir qui habite les événements. Discutant Martha Nussbaum, Bleiker explique :

> Literature, music and other works of art offer possibilities to express emotional insights in ways that cannot easily be achieved through conventional accounts of events. *Aesthetic engagements focus on the human reactions to and emotional interpretations of events, rather than their mere factual occurrence.* This is why, Nussbaum stresses, emotional intelligence and aesthetic ways of representing them should be accepted, alongside more conventional sources, as legitimate elements in the formulation of ethical and political judgements. … The aesthetic, in turn, could thus be seen as offering an alternative response, a creative enchantment that takes its place in a broad spectrum of different forms of reasons (Bleiker 2009, 62; je souligne).

Le savoir produit par l'esthétique est différent de celui offert par la raison, car il met l'accent sur l'émotion déclenchée par les événements. Il permet de contester le sens commun d'un objet imposé par l'harmonie rationnelle, « the ultimate act of political power » (Smith cité par Bleiker 2009, 29), tout en proposant une « multiplication of common senses » (Bleiker 2001, 515). En plus de montrer, comme dans la critique du mimétisme, comment les représentations sont constituées par les structures de pouvoir, et constituantes de celles-ci, l'imagination et les émotions offrent la possibilité de comprendre le monde différemment, de percevoir les structures de pouvoir qui ne relèvent pas de la raison. L'esthétique doit permettre de voir au-delà de ce qui est.

> Good photography, Higgins argues, seeks not scientific authenticity, but artistic representation. It allows us to move beyond a merely external depiction of the world. It may help us see and deal with the spirit of a period or event. This is why the best photographic art strives to capture, as Higgins puts it, 'that which you cannot see'. Rather than superimposing an externally perceived image, it seeks to bring out multiplicities and ambiguities (Bleiker 2009, 11–12).

L'expérience esthétique remet en cause la primauté de la raison et son rôle dans l'organisation du monde. Il ébranle les structures de pouvoir sans pour autant proposer de solutions ou d'alternatives concrètes. L'art, pour être politiquement pertinent, ne doit pas chercher à reproduire le rationalisme actuel, mais à le déstabiliser et générer la pensée imaginative nécessaire à la contestation du sens commun. Face aux dangers de l'objectivation de relations de pouvoir en phénomènes « naturels », l'esthétique ramène dans la sphère politique ces enjeux gardés sous silences et soulève des questions : quels autres mondes sont possibles ?

L'esthétique est donc, pour l'auteur, incompatible avec la technique artistique instrumentalisée par les luttes politiques. Au contraire, est esthétique l'art qui sera politique (critique), sans être soumis à un projet politique particulier, c'est-à-dire sans proposer de réponses toutes faites aux problèmes du moment. Plutôt que de se voir dicter son contenu politique par un message activiste, progressiste ou réactionnaire, l'art politique invite à la réflexion critique, à penser le monde hors du schème des luttes existantes. Citant l'artiste Gao Xingjian, Bleiker précise :

> 'the writer writes what he wants without concern for recompense not only to affirm his self but also to challenge society'. It is in this challenge, even if apolitical in nature, that art becomes political. It is so, as Gao aptly puts it, not by waving a flag or by shouting a slogan or driving a war chariot, but by breaking taboos and promoting 'uncompromising independence and spiritual freedom' (Bleiker 2009, 2).

La frontière est ainsi tracée « between works of art that simply assert and those that actually lead to a better understanding » (Bleiker 2009, 8). C'est sur cette base que Bleiker conteste la pertinence esthétique de l'art activiste comme étant « neither very political nor very poetic » (Bleiker 2000, 272).

Pour Bleiker, l'art ne se réduit donc pas à la vocation d'instrument des luttes politiques, ce que Campbell et Shapiro appellent le « straitjacket of the ideational » (Campbell & Shapiro 2007, 133). Dans une lecture proprement instrumentale, la forme artistique est circonstancielle. Les médiums de l'art que sont l'architecture, la peinture, le cinéma, etc. peuvent être utilisés aussi bien à des fins de propagandes que de contestation de l'ordre établi. Il est, au même titre que n'importe quel autre art (compris au sens de technique), jugé exclusivement par son succès à atteindre son objectif. Comme l'explique Gordon Graham, dans ce contexte l'art devient secondaire à l'objectif : à la théorie, ou l'Idée, qui l'informe.

> Art can be used [as a means] of course …; when it is, it is reduced to a kind of technology or craft, a device for doing something else that need not be in any way artistic. … The value of a craft, a means to an end, resides entirely in its products, so that other means to the same end will do just as well (G. Graham 2005, 41).

Pour Bleiker, l'art dans sa forme esthétique n'est pas simplement au service du politique — même si certains acteurs politiques peuvent approcher l'art en terme instrumental (Campbell & Shapiro 2007, 133-134; Weldes & Rowley 2015; Bleiker 2009, 134-138) —, mais conteste le politique en déstabilisant les représentations dominantes du monde.

> Overtly committed art forms often do no more than promote a particular position. They may be political, yes, but not aesthetically so. They are simply another way of expressing a political message. The fact that this message is conveyed through a song, a poem, a novel, a painting or a film is a mere coincidence. It has little or nothing to do with the aesthetic qualities of the art form itself. Aesthetic politics, by contrast, has to do with the ability of artistic engagements to challenge, in a more fundamental way, how we think about and represent the political (Bleiker 2009, 8).

Le tournant esthétique rejette ainsi la dichotomie formelle que certains tentent d'imposer entre l'autonomie et la politisation de l'art (Shusterman 2003, 781; Goehr 2003, 472-473), tout en lui reconnaissant une pertinence politique. Bleiker justifie cette position mitoyenne de l'esthétique par le savoir nouveau qu'offre l'esthétique et qui conteste la mainmise du mimétisme rationaliste. « This is why one of the main political challenges today, » explique Bleiker :

> may consist not in retaining the autonomous sphere of art, but in rendering the aesthetic central again, not only as an alternative to technological reason, but as a way of promoting non-coercive relationships among different faculties. … Indeed, the sensibility that the aesthetic promotes, and that instrumental reason is unable to apprehend, revolves precisely around the unknown, the unseen and the unthought (Bleiker 2009, 46).

L'art est ainsi libéré du rôle d'instrument du politique. Le statut critique de l'art ne signifie toutefois pas que tout art soit résistant, engagé dans une lutte politique au sens où la gauche révolutionnaire ou progressiste le comprend. Au risque de me répéter, Bleiker rappelle que l'« art can be as regressive as progressive » (Bleiker 2009, 180). Certains artistes ont pu par le passé embrasser les projets les plus réactionnaires. De même, la beauté et l'harmonie de l'art, selon la thèse de Benjamin, peuvent séduire et attirer vers le fascisme, « but in itself this does not preclude the aesthetic from playing the opposite role » (Bleiker 2009, 10). En fait, l'esthétique se distingue par son attitude critique et son ambivalence éthique qui ouvre la porte à une remise en question des fondements de l'ordre politique, des structures de pouvoir. C'est dans ce contexte que pour Bleiker, l'esthétique est liée à l'éthique. L'ambivalence esthétique doit permettre de réévaluer les ordres moraux existants à la vue des horreurs et souffrances qu'ils causent. Il n'est donc pas dans le même registre que les propositions politiques qui prescrivent solutions et réponses aux problèmes du vivre ensemble.

> Aesthetics adds a different dimension to our understanding of the political and, by consequence, to the ethical discourses that are central to waging political debates. Since art is not the language of habit, since it searches for the new, the different, the neglected, it may even create a certain 'mental and emotional alertness' — an encouragement to reflect upon and rethink what has been taken for granted, to move beyond dogma and promote debate about issues that would otherwise remain silenced or marginalised. … It is in this sense that

> art is ethically relevant: it challenges the modern tendency to reduce the political to the rational. And, by doing so, aesthetics can expose political practices whose problematic dimensions are no longer recognised because of years of habit have turned them into common sense… It is not a black-and-white ethics, one that clearly stipulates a set of rights, rules and regulations. … The ethical significance of the aesthetic emerges from the effort to open up different perspectives and options, from being mindful about the potentially problematic nature of all ethical systems that rely on fixed principles. … Ethics, then, becomes a mode of being rather than a set of principles: the cultivation of an attitude that emerges from seeing things in different and insightful ways (Bleiker 2009, 12).

En ce sens, la relation entre l'esthétique et le politique est anti-dogmatique. Reproduire des discours de certitudes à travers l'art, même des discours « progressifs », limite l'imagination et plonge la critique esthétique dans les eaux troubles des discours de vérité. Et c'est précisément dans les moments les plus dramatiques où les frontières morales deviennent nébuleuses que la sensibilité esthétique est la plus importante.

> It is in such moments that the inspiration of aesthetic sources can become crucial to ethical and political debates for they are not bound by the force of habit : they allow us to review and rethink the taken-for-granted principles that caused havoc in the first place; … they give us spaces to reflect before we need to make difficult decisions and they remind us that these very political decisions are a responsibility we have to actively assume, rather than rely upon rules and norms that were written for a different time and a different set of political challenges (Bleiker 2009, 13).

En s'opposant au rationalisme dominant des RI, l'esthétique de Bleiker est ancrée dans la volonté de revaloriser le spectre complet des perceptions. Il propose une remise en cause du mimétisme et du sens commun que celui-ci impose. Il invite du même coup à comprendre les processus de constitution de ces représentations dominantes afin d'éclairer la nature contingente de structures de pouvoir ossifiées et d'ouvrir la porte à un monde alternatif. La pratique artistique s'avère être une source privilégiée de ce processus critique. En mobilisant l'émotion contenue dans les événements, l'art propose un rapport au monde esthétique qui vient offrir un contrepoids au monopole de la raison en RI. Pour Bleiker, il ne s'agit pas avec l'esthétique de nier la pertinence des autres approches et théories des RI, mais bien d'ajouter au travail actuel des RI avec une perspective qui intègre et valorise ce qu'elles ignorent.

3.2 L'art de résistance (I, II & III) : l'esthétique de la politique, la visibilité et la redistribution du partage du sensible

À travers la critique du mimétisme et du rationalisme, le tournant esthétique mène un triple projet. L'analyse du processus de constitution du monde pose la question du comment : quelles

sont les conditions de possibilité qui ont permis le déploiement du monde tel qui est ? En parallèle à cette connaissance critique des limites du monde présent, l'esthétique propose un nouveau savoir qui permet de contester et compléter le diktat de la raison. L'esthétique autorise enfin l'imagination et la création, favorise les croisements et rencontres impromptus, et réanime les utopies décimées par le langage technicien et bureaucratique de la politique rationaliste. Ce rapport au monde esthétique se réapproprie la surprise, le doute et la créativité et joue de l'ambivalence des catégories actuelles pour les déstabiliser. En d'autres mots, l'esthétique force à penser. « To *think* (rather than to seek to explain) in this sense is to invent and apply conceptual frames and create juxtapositions that disrupt and/or render historically contingent accepted knowledge practices, » écrit Shapiro.

> It is to compose the discourse of investigation with critical juxtapositions that unbind what are ordinarily presumed to belong together and thereby to challenge institutionalized ways of reproducing and understanding phenomena. … To *think* rather than reproduce accepted knowledge frames is to create the conditions of possibility for imagining alternative worlds (and thus to be able to recognize the political commitments sequestered in every political imaginary) (Shapiro 2013, xv).

À travers l'ironie et les collages, la célébration des incohérences et la superposition d'éléments incompatibles, l'esthétique disloque le sens commun, soulève des questions, ramène au premier plan les relations de pouvoir naturalisées et offre une nouvelle fenêtre pour éclairer ce monde politique complexe, contingent, fuyant, trop souvent prisonnier des dichotomies réductrices et obscures, et du même coup ouvre la voie à sa contestation.

Ce faisant, le tournant esthétique se consacre à la démonstration de la pertinence politique de l'art, mais laisse en pan la réflexion sur la nature esthétique de la politique. Bleiker reconnaît d'ailleurs ce parti-pris lorsqu'il invite à élargir la portée du tournant esthétique :

> There is a need for more thorough interactions between different approaches to the aesthetic turn, between those who primarily draw inspiration from aesthetic sources to rethink political dilemmas — as I have done in this book — and those who focus more on how political dynamics themselves have an inherent aesthetic dimension that needs to be recognised and understood (Bleiker 2009, 187).

La dimension esthétique de la politique peut s'interpréter, comme Bleiker semble l'indiquer ailleurs, en relation avec les événements de rupture tels que les attentats du 11 septembre 2001 (Bleiker 2009, 67-83) ou encore, dans le contexte de la surveillance algorithmique, les révélations Snowden. Ces événements créent des moments d'incompréhension qui nécessitent d'être réintroduit dans des schémas cognitifs.

D'autres explications existent. Dans la tradition marxisante, l'esthétique de la politique se comprend comme une fétichisation de la représentation qui fait disparaître ou remplace le réel. Le pouvoir utilise le plaisir esthétique pour masquer la réalité des structures de domination, assurer son contrôle des populations et sa pérennité. L'art se voit remettre la lourde responsabilité de démystifier ces fausses représentations (Andersen, Vuori & Mutlu 2015, 105-108). « The aesthicization of politics, » résume Boris Groys,

> is what we would call branding, or design, which presents politics as a seductive spectacle. … Politics become a way to seduce people. On the other hand, the politicization of art is a way to get free of that and to act purely politically — beyond aesthetics, beyond art, beyond seduction, beyond spectacle (Boris Groys cité par Azoulay 2011, 243).

La tradition marxisante confère ainsi à l'esthétique un pouvoir séducteur dangereux et un rôle de résistance politique particulier. Ces deux parties sont liées, mais n'en demeurent pas moins distinctes, car la « critique of appearance [that] present[s] dystopic views of a loss of authenticity as well as posit[s] fears of the power of images » (Andersen, Vuori & Mutlu 2015, 105) dépend d'une élévation de l'art comme forme privilégiée de résistance (Azoulay 2011, 244).

La dialectique entre art et politique permet ultimement de découvrir la vérité sur l'ordre politique, de révéler les structures de pouvoir cachées par des représentations fautives, mensongères. Dans un premier temps, la transformation du monde politique sous les effets de la technologie et du contrôle des représentations entraîne une perte de compréhension et de contrôle. Chez Max Horkheimer et Theodor Adorno (Horkheimer & Adorno 1974; Gracyk 2013), Guy Debord (Debord 1996) et Jean Baudrillard (Baudrillard 1981) par exemple, le rapport à la structure d'apparence masque la réalité et corrompt le sujet qui perd ainsi ses intérêts réels de vue. Cette structure extérieure crée une distance entre le sujet et le réel qui empêche la vie politique authentique. Comme le résume Jacques Rancière, discutant plus spécifiquement de la société du spectacle de Debord :

> Le spectacle est le règne de la vision et la vision est l'extériorité, c'est-à-dire dépossession de soi. La maladie de l'homme de spectacle peut se résumer en une brève formule : « Plus il contemple, moins il est. » … La « contemplation » que Debord dénonce, c'est la contemplation de l'apparence séparée de sa vérité, c'est le spectacle de souffrance produit par cette séparation. « La séparation est l'alpha et l'oméga du spectacle. » Ce que l'homme contemple dans le spectacle est l'activité qui lui a été dérobée, c'est sa propre essence, devenue étrangère, retournée contre lui, organisatrice d'un monde collectif dont la réalité est celle de cette dépossession (Rancière 2008, 12-13).

Dans un second temps, l'art permet de percer ce mur d'illusions et de voir la réalité du monde qui se dissimule sous couvert du spectacle technologique moderne. Dans ce contexte, l'art possède un pouvoir de démystification : il doit savoir briser l'illusion du spectacle en montrant au spectateur ce qu'il ne sait pas ou ne veut pas voir. Que la réalité soit masquée par la propagande comme chez Adorno et Horkheimer ou que la réalité soit elle-même devenue une illusion comme chez Debord et Baudrillard, l'art doit permettre de révéler l'existence de ces inversions entre le réel et l'irréel. « Le dispositif critique vis[e] ainsi un double effet : une prise de conscience de la réalité cachée et un sentiment de culpabilité à l'égard de la réalité déniée » (Rancière 2008, 33). L'art est alors pédagogique et provocateur. La connaissance étant insuffisante pour causer l'action, il est espéré que la culpabilité saura générer une volonté de résistance et de changement nécessaire à la réappropriation individuelle et collective de l'espace politique. Mais aujourd'hui avec la « réalité devenue gazeuse, liquide, immatérielle de la domination » (Rancière 2008, 42), la tradition marxisante se retrouve prise dans une léthargie mélancolique qui freine l'action sociale. Pour Rancière,

> le marxisme de la dénonciation des mythologies de la marchandise, des illusions de la société de consommation et de l'empire du spectacle… est aujourd'hui devenu un savoir désenchanté du règne de la marchandise et du spectacle, de l'équivalence de toute chose avec toute autre de toute chose avec sa propre image. Cette sagesse postmarxiste et post-situationniste… peint… la loi de la domination comme une force s'emparant de tout ce qui prétend la contester. Elle fait de toute protestation un spectacle et de tout spectacle une marchandise (Rancière 2008, 38-39).

Face à un ennemi plus grand que nature et avec des formes de protestation aussi irréelles que la réalité des structures de domination, la critique marxisante, et avec elle sa perspective de l'art politique, se perd dans un cycle d'inversion permanent, duquel seul ressort un sentiment de culpabilité engendré par l'inévitable participation à ce cercle de domination (Rancière 2008, 38-48).

Dans la perspective poststructuraliste qu'adopte le tournant esthétique, la représentation n'est pas une copie trompeuse de la réalité. La représentation, mystique dans la tradition marxisante, est dans le courant poststructuraliste banale et effective. Parce que la représentation possède une existence à part entière, elle ne peut remplacer la réalité. Elle constitue un objet en soi, indépendante et réelle. « One of the core issues in the question of the 'real' and separation from it, is the link between the represented and representation, » écrivent Rune Saugmann Andersen, Juha A. Vuori et Can E. Mutlu.

> What Debord and Benjamin left under-articulated is that a representation is merely an *equivalent*, not a duplicate. A photograph does not steal the soul of the one photographed, but merely produces an equivalent which resembles the target of the lens. Indeed, as Mitchell (2011, xvii) notes, all metaphors and images are 'errors' in the sense that they are simulations, imitations, and not the thing they purport to be. … This entails that appearance and the thing itself have to be separate in the examination of representations and ideas, and that to study the representation of a thing is not to study the thing itself. … Of consequence here is how images play with the relations of the sayable and the visible (Rancière 2008; 2011). … For Rancière (2007: 116) entities of representation are fictional entities, and thereby exempt from judgements of existence or ontological consistency. Yet, this has nothing to do with the reality — or unreality — of things. Political, scholarly and even fictional statements can still shape reality. Statements on the real, or of pure fiction, can have a modulating effect on the 'seeable, the doable, and the sayable' (ibid.). … Methodologically, this leads us to the study of the performativity of images and visuality rather than representation (Andersen, Vuori & Mutlu 2015, 108).

La réalité de la représentation invite à s'intéresser à son effet. Plutôt que de masquer le réel, la représentation construit le réel et l'ordre social et politique. Héritier de Foucault, Nicholas Mirzoeff explique que la visibilité est un mode d'organisation et de stratification du monde sensible qui délimite ce qui est perceptible de ce qui ne l'est pas.

> Despite its name, [visuality] is not composed simply of visual perceptions in the physical sense but is formed by a set of relations combining information, imagination, and insight into a rendition of physical and psychic space. … [It is] a discursive practice for rendering and regulating the real that has material effects (Mirzoeff 2011, 476).

Partie prenante du processus de normalisation du contrôle de l'État, le concept de visibilité rappelle que les structures de pouvoir sont fondées sur l'univers perceptible. Inversement, les perceptions ne sont pas neutres, mais délimitées par le pouvoir qui rend certaines choses visibles et d'autres invisibles. Chaque mode de visibilité est le produit d'opérations de classification, de séparation et finalement d'une esthétisation de l'ordre sensible qui prétend détenir l'autorité sur le réel, sur « that-which-must-be-made-sense-of » (Pasolini cité par Mirzoeff 2011, 477).

Pour Monahan, « [visuality] manifests in a set of extractive and dehumanizing complexes … that are institutionalized through bureaucratic and scientific apparatuses that render classifications true and population governable » (Monahan 2015, 2). Après avoir identifié et catégorisé les individus composant la population à gouverner, la visibilité sépare les classes créées. Cette ségrégation est organisationnelle, c'est-à-dire qu'elle vise à la fois le bon fonctionnement de la société en séparant les groupes de droits et pouvoirs distincts et en les gouvernant conformément à leur statut, en les privilégiant, en les marginalisant ou en les abandonnant à leur sort. Ce processus leur attribue également des possibilités d'agir, refusant aux groupes marginalisés le droit de se

mobiliser. Enfin, le processus d'esthétisation de l'ordre social légitime les structures de pouvoir par la répétition et la construction d'un sens commun le faisant apparaître normal et naturel. « As Frantz Fanon had it, such repeated experience generates an "aesthetic of respect for the status quo," the aesthetics of the proper, of duty, of what is felt to be right and hence pleasing, ultimately even beautiful » (Mirzoeff 2011, 476). Dans ce contexte, l'esthétisation, la normalisation de l'ordre social, ne doit pas être perçu comme un voile dissimulant l'ordre réel comme dans la tradition marxiste. *L'esthétisation est plutôt le produit ou l'effet de la restriction des frontières sensibles et cognitives du monde politique.* Les structures sociales ne sont pas uniquement le résultat d'une rationalité commune, mais aussi d'une sensibilité commune.

Jacques Rancière nomme cette structure sociale le partage du sensible et rappelle que l'univers politique est éminemment esthétique. À la base de toute politique se retrouve l'établissement des conditions d'intelligibilité du monde commun qui déterminent les droits d'accès à l'univers politique : qui peut prendre part aux décisions collectives et sous quelle condition d'intelligibilité est-il possible d'y prendre part. L'organisation politique du monde est établie sur la reconnaissance sensible de communs et la répartition de parts précises.

> Cette répartition des parts et des places se fonde sur un partage des espaces, des temps et des formes d'activité qui détermine la manière même dont un commun se prête à participation et dont les uns et les autres ont part à ce partage. Ce citoyen, dit Aristote, est celui qui *a part* au fait de gouverner et d'être gouverné. Mais une autre forme de partage précède cet avoir part : celui qui détermine ceux qui y ont part. … Cela définit le fait d'être ou non visible dans un espace commun, doué d'une parole commune, etc. (Rancière 2000, 12-13).

Le partage du sensible détermine qui a droit de cité. Il dépasse ainsi les considérations de distribution des richesses. Les distinctions entre les dirigeants et les esclaves et ouvriers d'Aristote et Platon, légitimées par la structure des âmes chez un ou la métaphysique chez l'autre, constituent une forme du partage du sensible. La voix de l'esclave et de l'ouvrier, tous deux incapables de raison, ne pouvait être entendue dans la délibération politique. Pour Rancière, cette distribution des parts démontre la nature profondément esthétique du politique : elle révèle l'autorité du pouvoir sur les sens, et l'étroite proximité entre le droit d'être et la capacité à dire et à être entendu. « Il y a donc, à la base de la politique, une « esthétique » qui n'a rien à voir avec cette « esthétisation de la politique », propre à l'« âge des masses », dont parle Benjamin, » explique Rancière.

> Cette esthétique n'est pas à entendre au sens d'une saisie perverse de la politique par une volonté d'art, par la pensée du peuple comme œuvre d'art. Si l'on tient à l'analogie, on peut

> l'entendre en sens kantien — éventuellement revisité par Foucault —, comme le système des formes *a priori* déterminant ce qui se donne à ressentir. C'est un découpage des temps et des espaces, du visible et de l'invisible, de la parole et du bruit qui définit à la fois le lieu et l'enjeu de la politique comme forme d'expérience (Rancière 2000, 13-14).

On retrouve ainsi chez Rancière l'essence du projet poststructuraliste, c'est-à-dire la recherche des exclusions induites dans le langage, qu'il réussit à phraser en termes esthétiques, parlant plus largement de l'expérience sensible en général, plutôt que de se limiter à l'expérience de l'œil, et poursuit la réflexion, dans ce contexte, sur les pratiques artistiques contestataires.

Les conflits politiques et des luttes de pouvoir s'articulent sur la base de cette première définition (méta)politique du partage du sensible. « La politique porte sur ce qu'on voit et ce qu'on peut en dire, sur ce qui a la compétence pour voir et la qualité pour dire, sur les propriétés des espaces et les possibles du temps » (Rancière 2000, 14). Est politique ce qui participe au (re)partage de ces conditions d'intelligibilité. C'est donc sur la base du partage du sensible que se comprend la dichotomie entre résistance et pouvoir, ou entre politique et police dans les termes de Rancière.

Au cœur de la mésentente rancièrienne, la politique s'oppose à la police. Ici, la police ne se limite pas au bras armé de l'exécutif. Il s'agit de l'ordre social qui détermine le champ des expériences du partage du sensible. Face à la « logic of the police … [that] distributes bodies within the space of visibility … political acts … shift bodies from the places assigned to them, thus making visible 'what have no business being seen' » (Norval 2014, 198–199). Le moment politique met en scène la déclaration d'un tort. Un individu ou un groupe d'individus jusque-là invisibles brisent leur position dans l'ordre social pour revendiquer une redistribution des parts. La déclaration du tort est politique, car elle bouscule le partage du sensible. Elle est aussi performative en produisant de nouveaux sujets politiques dont l'identité ne sera pas prédéterminée, mais relationnelle, produite par la déclaration du tort (Rancière 1999, 27; Chambers 2009, 11).

> Politics is a matter of subjects or, rather, modes of subjectification. … the production through a series of actions of a body and a capacity for enunciation not previously identifiable within a given field of experience, whose identification is thus part of the reconfiguration of the field of experience (Rancière 1999, 35).

Rancière se pose ici en faux vis-à-vis de la tradition marxisante qui fait du moment politique la manifestation du prolétariat. La politique n'est pas le moment d'affirmation d'une communauté existante, mais la performance d'un sujet qui prend forme à même la déclaration d'un tort, même si ultimement la consolidation de cette subjectivité demeure floue. Le moment de résistance est

donc spontané et immanent, issu de l'ordre social sans pour autant être prédéterminé ni par l'organisation des structures de production ni par une avant-garde responsable de sa mise en œuvre (Norval 2014, 204).

Le concept de visibilité permet de penser l'inséparabilité de la politique de l'esthétique et de l'esthétique du politique. La pratique esthétique est dépendante, imbriquée dans une sensibilité, un système de perception. Pour Jenny Edkins et Adrian Kear qui citent Rancière :

> "If there is such a thing as an 'aesthetics of politics', it lies in the reconfiguration of the distribution of the common through political processes of subjectivation. Correspondingly, if there is a politics of aesthetics, it lies in the practices and modes of visibility of art that reconfigures the fabric of sensory experience"… [In this context] politics and performance [as artistic intervention]… reveal the fundamental inter-connection yet ultimate separation of the aesthetics of politics and the politics of aesthetics in terms of form and effect, elaborating and demonstrating at every turn their inter-animation by aesthetic subjects in the practice of aesthetic politics (Edkins & Kear 2013, 8).

Pour Rancière, la politique des pratiques artistiques se comprend donc en relation au partage du sensible, mais aussi en relation au régime esthétique, « un régime spécifique d'identification et de pensée des arts » (Rancière 2000, 10), qui conteste les hiérarchies sociales. Ce régime des arts est particulier

> parce que l'identification de l'art ne s'y fait plus par une distinction au sein des manières de faire, mais par la distinction d'un mode d'être sensible propre aux produits de l'art. … Ce sensible, soustrait à ses connexions ordinaires, est habité par une puissance hétérogène, la puissance d'une pensée qui est elle-même devenue étrangère à elle-même : produit identique à du non-produit, savoir transformé en non-savoir. … Le régime esthétique des arts est celui qui proprement identifie l'art au singulier et délie cet art de toute règle spécifique, de toutes hiérarchies des sujets, des genres et des arts. Mais il le fait en faisant voler en éclats la barrière mimétique qui distinguait les manières de faire de l'art des autres manières de faire et séparait ses règles de l'ordre des occupations sociales (Rancière 2000, 31-33).

L'ignorance esthétique ouvre ce moment de confusion et d'émergence où les certitudes d'avant sont ébranlées : « [i]t consists in the disjunction between sensible equipment and the ends that it must serve » (Rancière 2014, 269). L'ignorance esthétique offre du coup un moment de construction d'un nouveau récit, d'un nouveau monde, d'un nouveau partage du sensible : « [T]he singularity of the aesthetic experience is the singularity of an as if » qui permet d'ignorer le présent ordre social pour en reconstruire un nouveau.

> The aesthetic judgment acts as if the palace were not an object of possession and domination. … This as if is no illusion. It is a redistribution of the sensible… As such it is the answer to another as if: the ethical order of the city, according to Plato, must be viewed as if God had

> put gold in the souls of the men who were destined to rule and iron in the souls of those who were destined to work and be ruled. It was a matter of belief. … The ethical ordering of social occupations ultimately occurs in the mode of an as if. The aesthetic rupture breaks this order by constructing another as if (Rancière 2014, 269-270).

La fracture esthétique rompt avec les frontières cognitives de classe et de champ imposées par la sociologie de l'art (Rancière 2014, 269) et permet d'imaginer l'organisation du monde conformément aux valeurs d'égalisation et de destruction des hiérarchies qui anime le régime esthétique (Rancière 2010, 296). Pour l'auteur, le moment politique est un moment de devenir identitaire. Le moment politique est une performance. Dans ce contexte, les performances artistiques de nature politique déstabilisent l'apparente normalité de la partition des parts et rôles attribués par la police, et en parallèle perturbent les subjectivités créées par cet ordre social et sur lesquelles celui-ci dépend. Du même coup, elles produisent un espace d'apparition pour les nouveaux sujets.

> Aesthetic experience has a political effect to the extent that the loss of destination that it presupposes disturbs the way in which bodies fit their functions and destinations. What it produces is no rhetoric of persuasion about what has to be done. Nor is it the framing of a collective body. It is a multiplication of connections and disconnections that reframe the relation between bodies, the world where they live and the way in which they are 'equipped' for fitting in it. It is a multiplicity of folds and gaps in the fabric of common experience that change the cartography of the perceptible, the thinkable and the feasible. As such, it allows for new modes of political construction of common objects and new possibilities of collective enunciation (Rancière cité par Shapiro 2013, 30-31).

L'expérience crée un moment de mésentente qui se caractérise par la déstabilisation des structures existantes de manière à ouvrir un nouvel espace de pensée. L'expérience esthétique déstabilise les disciplines et les significations politiques existantes permettant la reconnaissance de la contingence de la forme actuelle du monde. L'esthétique libère la pensée et l'amène au-delà des limites des combinaisons de sens de l'ordre social.

> An aesthetics of knowledge creates forms of supplementation that allow us to redistribute the configuration of the topoi, the places of the same and the different, the balance of knowledge and ignorance. It implies a practice of discourse that reinscribes the force of descriptions and arguments in the war of discourses in which no definite border separates the voice of the object of science from the logos of the science that takes it as its object. It means that it reinscribes them in the equality of a common language and the common capacity to invent objects, stories, and arguments (Rancière 2014, 279–280).

3.3 Dé-fétichiser l'esthétique : l'art comme pratique de résistance

La charge émotive du tournant esthétique et l'espoir contenus dans ces propositions critiques sont immenses. Si, d'un point de vue moins engagé, il est possible de restreindre l'esthétique à l'idée de « resource for making sense of political life » (Kompridis 2014, xvi) comme le proposent de prime abord Kompridis et Bleiker, rapidement la ressource esthétique est associée au potentiel créatif de l'art comme alternative à des modes de pensée trop étroits. Pour reprendre les mots de Lia Haro et Romand Cole :

> aesthetic energy with poetic commitment and sensibility is precisely what we urgently need to address [contemporary] challenges in genuinely transformative ways. When all else has failed to create enduring change, it may be time to tap dance towards a new model of political engagement (Haro & Coles 2014, 124).

Or, les dangers d'un tel investissement de l'esthétique sont réels. Comme le fait remarquer Anne McClintock dans le contexte sensiblement différent de la résistance postcoloniale, le culte de l'ambivalence, de l'étrangeté et de la déstabilisation esthétique des modes dominants de représentation risque de fétichiser le statut résistant de l'esthétique.

> While recognizing the vital importance of the concept of ambivalence … the question is whether it is sufficient to locate agency in the internal fissures of discourse. Locating agency in ambivalence runs the risk of what can be called a fetishism of form: the projection of historical agency onto formal abstractions that are anthropomorphized and given a life of their own. … In the process, social relations between humans appear to metamorphize into structural relations between forms through a formalist fetishism that effectively elides the messier questions of historical change and social activism (McClintock 1995, 64).

En négligeant de s'intéresser concrètement à l'impact de ce type de contestation, c'est-à-dire en oubliant de regarder son engagement direct avec les structures de pouvoir, le tournant esthétique risquerait d'associer à l'esthétique un potentiel « naturellement » ou ontologiquement déstabilisant. McClintock n'est pas seule dans la critique de l'ambivalence et de l'esthétique. Pour Gerard Holden, le tournant esthétique fait de la critique esthétique un concept fourre-tout, déconnecté de la philosophie de l'art, servant qu'à justifier les prises de position contre l'« US foreign policy or the white heterosexual American family » (Holden 2006, 816). L'espoir critique investi dans l'art risque d'invalider l'architecture théorique sur laquelle il est établi (Frost 2010), oubliant la fragilité des discours et attribuant à l'art un pouvoir qui ne peut être déterminé qu'empiriquement. « Because images are polysemous and ambiguous, » écrivent Andersen, Vuori et Mutlu, « we cannot close off their operation by theoretical fiat. The genre of images on its own does not preordain whether or

not an image can work towards critique and emancipation. Such questions are to be examined empirically » (Andersen, Vuori & Mutlu 2015, 92).

S'intéresser aux pratiques artistiques ne signifie pas reproduire une sociologie de l'art où la classe détermine le jugement artistique et les dynamiques de champ, la pertinence esthétique des œuvres comme Rancière reproche à Bourdieu de faire. Une telle entreprise suit la démarche entamée par la littérature sur la culture populaire et la politique mondiale (Doucet 2005; Devetak 2005; Grayson, Davies & Philpott 2009; Pusca 2008; Weldes 2003; C. Weber 2006). Pour cette littérature, la culture populaire constitue « a vehicle for the analysis of various political representations and dynamics but also in part constituted through those representations and dynamics » (Moore & Shepherd 2010, 305). Cette approche insiste sur la nécessité d'interroger le contexte de production comme de consommation des représentations. Pour Christina Rowley :

> work on popular culture […] recognises the need to investigate 'how these products are actively interpreted and used by people… Popular culture is … a terrain, a site of struggles over meaning which involves taking account of both texts (representations) and practices (their active consumption and interpretation)' (Rowley cité par Moore & Shepherd 2010, 307).

En se détachant d'une lecture uniquement inter/textuelle des représentations, cette littérature conçoit la culture populaire comme des objets et pratiques politiques insérés dans des contextes culturels particuliers et auxquels elle reconnaît un pouvoir performatif, et par le fait même la possibilité de la réappropriation et de la contestation.

Dans ce contexte toutefois, l'art se fond dans la culture populaire (Knight 2003). À ce titre, l'art, parti de la culture populaire, n'est pas différent des autres formes de représentations sinon que pour des raisons sociales. Ainsi gobé par la culture populaire, l'art devient un lieu privilégié pour comprendre les relations internationales. Toutefois, ceci s'explique non par le fait que la culture populaire est précisément un art ou détient en soi quelque chose d'esthétique, mais parce qu'elle se retrouve largement diffusée dans le quotidien et donc facilement accessible et décodable par le commun des mortels. Christina Rowley justifie ainsi l'attention à la culture populaire :

> The ways in which people make sense of world politics is, in large part, via the knowledge and understanding created through interactions with the world in the realm of the popular, the mundane and the everyday: the workplace, holidays, TV shows, advertisements. … As Jutta Weldes has demonstrated, popular cultural texts such as magazines, novels, films and television shows, are important because they are all implicated in the production of common sense, and therefore in the 'manufacture of consent' for states' foreign policies (1999: 119,

> 2003a). Popular cultural artefacts not only make use of the same background meanings (cultural resources) as do policy-makers, in order to construct a compelling vision of the world, they also create more and new cultural resources on which other cultural and state actors — and people more generally — can draw (Rowley 2010, 309-310).

Si la forme artistique que prend la culture populaire est importante, ce n'est pas pour sa nature esthétique, mais pour des raisons socio-économiques, pour des raisons institutionnelles, pour les caractéristiques propres au média, etc. qui permettent d'éclairer les structures de pouvoir d'une façon particulière (Rowley 2010; Kress & Van Leeuwen 2006).

En évacuant l'esthétique, cette approche se retrouve aux prises avec un dilemme quand vient le temps de justifier la pertinence politique de l'art comme objet particulier. À partir du moment où l'on fait exploser la définition de l'art, tout devient art. Du même coup, l'art perd toute valeur analytique. Pour Gordon Graham, les théories postmodernistes de l'art obligent en rejetant la distinction entre art et non-art, comme le fait l'approche pop culturelle qui inclut l'art dans la catégorie fourre-tout de culture populaire, à abandonner toute théorie de l'art. Toutes les représentations étant égales entre elles dans la constitution d'un système plus complexe de représentations, le concept d'art perd sa pertinence. Tout peut devenir art. Ainsi, sans objet d'étude particulier, la théorie de l'art devient inutile. Or, pour l'auteur, abandonner entièrement la théorie de l'art est une erreur, car dans ce contexte le postmodernisme ne peut rendre compte de son propre intérêt pour l'art qu'il discute abondamment alors même qu'il l'évacue ontologiquement (G. Graham 2005, 242-243). Pour Graham, sans théorie de l'art, la seule issue pour les postmodernes réside dans la validation de leur objet d'étude — l'art — par sa fonction sociale (G. Graham 2005, 249). Or, répondre à la question de la pertinence de l'art par sa fonction sociale n'évacue pas la présence de l'art, mais constitue plutôt un postulat sur la pertinence sociale de l'art qui doit être empiriquement vérifiée.

La littérature sur la culture populaire, si elle refuse de reconnaître une objectivité à l'art qu'elle gobe non sans raison dans la culture populaire, lui attribue néanmoins une pertinence sociale : les techniques de l'art représentent un vecteur d'information sur la politique mondiale co-constitutif du rapport au monde des individus qui y ont accès. Au risque de me répéter, c'est en terme social que Rowley justifie la pertinence de la culture populaire pour comprendre les relations internationales : « The ways in which people make sense of world politics is, in large part, via the knowledge and understanding created through interactions with the world in the realm of the popular, the mundane and the everyday: the workplace, holidays, TV shows, advertisements »

(Rowley 2010, 309). En outre, l'approche pop culturelle reconnaît la pertinence de l'art par la relation entre l'émotion et la politique. L'art fait place aux émotions qui habitent les événements politiques. L'émotion, d'abord expérience subjective, participe à des phénomènes sociaux tels que la construction de l'identité nationale et de son corollaire l'Autre. Dans cette optique, l'art agit comme amplificateur. Il contribue à la contagion des émotions parmi un vaste public et à l'édification ou la contestation de phénomènes sociaux (Carter & McCormack 2006; Duncombe & Bleiker 2015; Dodds 2015; Carter & McCormack 2010). Ce faisant, s'intéresser à l'art permet de compenser les lacunes de la raison, de réintégrer dans un schéma cognitif autant les événements spectaculaires et sublimes, tels que les attentats du 11 septembre 2001 ou la guerre en Irak, que les événements communs que la raison est incapable ou n'est plus capable de comprendre. Toutefois, dans les deux cas, que la culture populaire et les arts servent de média privilégié pour comprendre la politique mondiale, cela est à démontrer empiriquement. Mais cette démonstration est toujours à refaire, car elle est à la fois postulat et conclusion.

Au risque de profaner l'art et l'esthétique (G. Graham 2005, 221-250), l'analyse esthétique doit réintégrer les pratiques. Si l'on peut admettre, à la suite de Shapiro, que l'esthétique « focus[es] on encounters that disrupt 'habitual conditions of sensible experience' and thereby solicit critical thinking » (Shapiro 2013, 30), il faut éviter de fétichiser la résistance esthétique. Discutant de l'effet des médias, Nick Couldry propose de théoriser les médias comme pratiques « to sidestep the insoluble problems over how to prove 'media effects' (i.e. a convincing causal chain from the circulation of a media text, or a pattern of media consumption, to changes in the behaviour of audiences) » (Couldry 2004, 117). Plutôt que de chercher à éviter la question de l'effet ou, comme dans le contexte du tournant esthétique, de postuler son effet, il faut plutôt, paraphrasant Couldry, poser la question : « What, quite simply, are people *doing* in relation to art across a whole range of situations and contexts? » (Couldry 2004, 119) Pour Couldry, c'est en portant attention à la multiplicité des relations que les gens entretiennent avec les médias qu'il devient possible de comprendre comment les médias, ou les arts, contribuent à ancrer certaines significations dans le sens commun ou à les contester.

3.4 Donner corps à la résistance esthétique à la surveillance algorithmique : vers la constitution d'une communauté d'artistes numériques

Dans le contexte post-Snowden, l'identification de l'art résistant à la surveillance algorithmique fait face à un certain nombre de défis. L'abondance et la diversité des projets en offrent deux. L'abondance de la production artistique oblige une incursion en profondeur dans un champ immensément vaste et parfois obscur. Certaines œuvres sans diffusion institutionnelle se retrouvent à avoir un auditoire réduit ou de niche (Spahr 2010; Kwan 2013; Gschrey 2010; Derr 2010). En outre, parce que la production d'œuvre est permanente, cela signifie être continuellement en retard et dépassé par les événements. Cela oblige à faire des choix déchirants et à ignorer de nouveaux projets stimulants (The Glass Room 2017). La diversité des thèmes et des techniques abordés par les artistes pose également problème lorsque vient le temps d'identifier l'art de résistance. D'une part, la multiplicité des thèmes discutés dans les projets risque de créer une impression d'incohérence. Certaines œuvres s'intéressent à la surveillance de la présence publique[2]. D'autres abordent le thème de l'identité à l'ère numérique[3] ou encore des relations sociales et des médias sociaux[4]. Certaines cherchent des outils pour assurer leur vie privée[5], contestent l'hétéronormativité[6] ou la discrimination raciale[7] amplifiée par la surveillance. Certaines portent leur réflexion sur les infrastructures de la surveillance[8] alors que d'autres attirent l'attention

[2] Voir, par exemple, *9-Eyes* de Jon Rafman (Rafman 2015), *Conversnitch* de Brian House et Kyle McDonald (House and McDonald 2014), *Evidence Locker* de Jill Magid (Magid 2014), *Faceless* de Manu Luksch (Luksch, n.d.), *Sorting Daemon* de David Rokeby (Rokeby 2010), ou encore *Public Access Me* de Jonas Lund (Lund 2014).

[3] Voir, par exemple, *Karen* de Blast Theory (Blast Theory 2018), *Internet Cache Self-Portrait Series* de Evan Roth (Roth 2015), *Database* de Tobias Zimmer, *JML, Inc.* de Jennifer Lyn Morone (Morone 2015), ou encore *psk series* d'Addie Wagenknecht et Peter Sunde (Kane 2016).

[4] Voir, par exemple, *pplkpr* de Kyle McDonald et Lauren McCarthy (McDonald and McCarthy 2014), *Zero Likes* de Sam Hains (Gillespie 2017), *Please Don't Like This* de Jonas Brucker-Cohen (Brucker-Cohen 2016), ou encore *High retention, slow delivery* de Constant Dullaart (Dullaart 2015a).

[5] Voir, par exemple, *Kill Your Phone* d'Aram Bartholl (Bartholl 2014), *Stealth Wear* d'Adam Harvey (A. Harvey 2015), *ZXX* de Sang Mun (Mun 2012), *Zapped!* de Preemptive Media (da Costa, Schulte, and Singer 2015), *bionymous.me* d'Heather Dewey-Hagborg (Dewey-Hagborg 2015), *AdNauseam* de Mushon Zer-Aviv (Zer-Aviv 2015), ou encore *MicJammer* d'Alison Burtch (Burtch 2015)

[6] Voir, par exemple, *Face Weaponization Suite* de Zach Blas (Blas 2014), *Webcam Venus* de Pablo Garcia, *Cobra Club* de Robert Yang (Yang 2015), ou encore *Body Anxiety* de Leah Scharger et Jennifer Chan (Schrager and Chan 2015b).

[7] Voir, par exemple, *Tracking Transience* d'Hasan Elahi (Elahi 2013) et *Domestic Tension (Shooting an Iraqi)* de Wafaa Bilal.

[8] Voir, par exemple, *Transparency Grenade* de Julian Oliver (Oliver 2015), *Seeing Networks* d'Ingrid Burrington, (Burrington 2017), *Citizen Ex* de James Bridle (Bridle 2015f), *The Realm of Rough Telepathy* d'Ingrid Burrington et Meredith Whittaker (Burrington and Whittaker 2016), *Email Miles* de Jonas Brucker-Cohen (Brucker-Cohen 2016), *Ascension Island* de Simon Norfolk (Norfolk 2015), ou encore *Code Names of the Surveillance State* de Trevor Paglen (Paglen 2017a).

sur les individus qui composent les agences de surveillance ou rendent possible la surveillance[9]. D'autres encore s'intéressent au savoir algorithmique[10]. Cette diversité est doublée d'une diversité de format utilisé par l'art de surveillance : photographie, film, texte méditatif, jeu vidéo, collage, application, site Web, bijou, vêtement, coupe de cheveux, boîtier pour téléphone cellulaire, police d'écriture, fusil à balle de peinture, projection vidéo, graffiti, etc. Certaines œuvres se distinguent difficilement d'un programme informatique ou d'un objet technologique soulevant la question de l'identification de l'art.

Face à ce défi, je prends appui, dans l'identification de l'art de surveillance, sur la définition proposée par John McGrath et Robert J. Sweeny. Pour les auteurs, l'art de surveillance se définit par une remise en question des formes de contrôle liées à la surveillance contemporaine plutôt que par une forme particulière. « [I]f there is a 'surveillance art', » écrivent-ils,

> it is perhaps not an art which just uses surveillance technology, nor just takes surveillance as a theme, but one which, in line with the fundamental shift towards interactivity in much of our 21st century cultural production, allows us to act upon our surveyed/surveying world in a way which however momentarily and playfully, destabilises binary forms of power and control (McGrath & Sweeny 2010, 91; Brighenti 2010a; Gurses, Teran & Luksch 2010).

Avec cet objectif de déstabilisation esthétique à l'esprit, je restreins l'analyse à des projets qui s'identifient comme artistiques ou que le milieu artistique revendique. Je limite également le corpus à des œuvres qui s'intéressent explicitement au thème de la sécurité à l'ère post-Snowden. Ces œuvres discutent de la sécurité et lient la question à d'autres thèmes issus de l'ensemble technologie-culture-pouvoir. Ils répondent à leur façon à la sortie du lanceur d'alerte, composent son public. Ils participent du coup à l'écriture du monde entamée par Snowden, illustrant ou rendant le jargon technique visible et lui proposant une alternative.

Pour William Walters et Anne-Marie D'Aoust, les publics se définissent comme des « zones of political communication, engagement, and understanding », des « lively, affective and creative assemblies, and as modalities of engaging, mobilising and informing subjects » (Walters & D'Aoust 2015, 51). Les publics ont des existences spontanées et transitoires. Ils se manifestent à la suite d'un événement, d'un discours ou d'une œuvre qui motivent sa mise en commun, mais

[9] Voir, par exemple, *ICWATCH* (J. Cox 2015), *Overexposed* de Paolo Cirio (Cirio 2015), *Intelexit* de Peng! (Peng! 2016), *Technologies of Care* d'Elisa Giardana Papa (Soulellis 2016), ou encore *WatchTower* de James Coupe (Coupe 2017).

[10] Voir, par exemple, *Five Eyes/Hyperstacks* de James Bridle (Bridle 2015g), *ScareMail* de Ben Grosser (Grosser 2015) et *Deli Near Info* d'Harm Vanden Dorpel (van den Dorpel 2016).

qui limitent aussi sa durée, leur fin amenant à la dispersion du public. Au sein des publics, mais aussi en relation avec l'extérieur, les acteurs qui y participent déploient des stratégies pour obtenir l'attention et l'aval des autres et promouvoir leurs définitions des enjeux. Ces stratégies nécessitent un travail d'interprétation du monde social et matériel afin d'en maximiser l'efficacité. Les publics sont ainsi étroitement reliés aux objets matériels qui constituent les enjeux initiaux ou sont instrumentalisés. Les publics définissent également l'interprétation sociale des objets (Walters & D'Aoust 2015, 53-55). Pour les auteurs, reconstituer les publics permet d'étudier les « diagrammes de pouvoir », c'est-à-dire « how particular elements, practices, and identities, are constellated in a given conjuncture » (Walters & D'Aoust 2015, 57) et du même coup les modes de contestation qui s'imbriquent ou refusent ces arrangements de pouvoir.

Penser ces artistes comme un public des révélations Snowden permet de briser le regard individualisant que l'analyse d'œuvre peut encourager. Comme le suggère Kennan Ferguson, le jugement, les valeurs et le goût ne relèvent pas de la libre expression individuelle, mais sont constitués par l'identité du sujet observant et dépendants de celle-ci (K. Ferguson 1996). En même temps, la théorisation de l'esthétique inspirée par les Bleiker, Shapiro et Rancière refuse la soumission de l'art à la détermination sociologique. Dans ce contexte, s'intéresser à ces artistes comme un public offre une voie médiane pour analyser les pratiques artistiques tout en conservant le pouvoir déstabilisateur de l'esthétique. Le public permet de reconnaître une entité sociale, une histoire et des structures idéationnelles et institutionnelles, et un pouvoir performatif et créatif.

Valentin Gros, Marieke de Goede et Beste Isleyen se sont déjà intéressés à l'idée d'un public de Snowden (V. Gros, de Goede & Isleyen 2017). Pour les auteurs, les audiences publiques tenues par la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen en 2013-2014 ont servi d'espace politique pour discuter, expliquer et contextualiser les révélations Snowden en Europe. Ce faisant, les audiences publiques, suggèrent-ils, « worked hard to define the problem in particular ways and set the limits of public debate on the issues » (V. Gros, de Goede & Isleyen 2017, 75). Approcher les audiences publiques sous cet angle permet aux auteurs de montrer le processus de normalisation des documents révélés et la revendication par la Commission LIBE d'une responsabilité politique à l'égard de la surveillance de masse que les autorités de sécurité nationale lui niaient. Cette approche aura aussi permis aux auteurs d'illustrer « the material difficulty of contesting surveillance practices politically, » concluent-ils.

> … With regard to secret security issues, a lot of the work of politics is in drawing together a public platform in the first place. Before political dialogue can take place, there needs to be a material platform for discussion, a basic set of shared assumptions, and a language in which to speak. Normative critiques of surveillance often overlook the difficult, material, work needed to stage such political dialogue in the first place (V. Gros, de Goede & Isleyen 2017, 86).

L'adoption de définitions communes et d'un cadre commun de réflexion sur les enjeux de la surveillance de masse par la Commission LIBE permet à terme d'en penser les limites : « the materiality of the ways in which partial documents on secret surveillance practices are rendered into (public) evidence both enables and conditions the possibility for political contestation » (V. Gros, de Goede & Isleyen 2017, 86).

La communauté d'artistes numériques que j'étudie dans ma thèse et qui constitue un public de Snowden définit la surveillance de masse, les enjeux et les limites à travers les arts plutôt que par le biais d'institutions politiques officielles. Comme pour la Commission LIBE, elle est un public de Snowden parce que les révélations ont eu un effet catalyseur sur la production d'art et l'organisation de festivals. Cet effet s'est fait sentir et se dissipe également, de nouveaux thèmes d'exploration artistique, notamment le traitement algorithmique des mégadonnées par les grands joueurs de l'économie numérique, refont surface (The Glass Room 2017; Gansing et coll. 2018). Certes, cette communauté n'est pas une entité formalisée par les procédures d'une institution officielle. Elle ne demeure pas moins une communauté qui circonscrit ce public, lui donne une cohérence artistique et une durée dans le temps. Parmi les premiers utopistes Internet, cette communauté d'artistes joue aujourd'hui un rôle de critique des tendances sociales liées aux technologies numériques. Soit individuellement ou organisés autour de groupes et centres artistiques, ces artistes et leur relève poursuivent le travail d'expérimentation et de réflexion sur le lien entre technologie, culture et pouvoir avec un regard critique[11]. Cette communauté retrouve périodiquement son corps social en se croisant dans les expositions, en se rassemblant autour de festivals, en fréquentant les mêmes lieux de formation et organisations[12].

Dans ce contexte, la spontanéité du public semble s'opposer à la durée de la communauté. Toutefois, plutôt que de les opposer, je propose de les superposer : cette communauté d'artistes,

11 Voir les rétrospectives Ctrl [Space] (Levin, Frohne, and Weibel 2002), Electronic Superhighway (2016-1966) (Kholeif 2018) et Net Art Anthology (Rhizome 2016) tenues respectivement au Zentrum für Kunst und Medientechnologie de Karlsruhe (Allemagne), à la Whitechapel Gallery de Londres et présentée en ligne par Rhizome.

12 Mentionnons notamment les festivals et événements récurrents *transmediale*, *ars electronica*, *seven on seven*, les institutions *Rhizome*, *Furtherfield*, *Eyebeam*, *Tactical Technology Collective*.

sensibles aux enjeux sociaux et politiques liés à Internet et aux technologies numériques, a réagi activement aux révélations Snowden, s'inscrivant, pendant ce laps de temps, comme un public de Snowden et contribuant au débat sur la surveillance de masse et la sécurisation numérique. Cette superposition donne une cohérence et un corps social aux pratiques artistiques tout en permettant d'établir des frontières au corpus d'œuvres à étudier.

Le festival d'art numérique berlinois *transmediale* illustre bien le moment où il devient un public de Snowden. Important lieu de convergence depuis trois décennies de cette communauté hybride d'artistes, d'activistes, de technologistes et d'universitaires[13], le festival consacra ainsi les thèmes des événements 2014 et 2015 aux reculs de la révolution numérique et à la surveillance de masse. Le thème de l'édition 2014 du festival, intitulé « Afterglow : The revolution is over. Welcome to the afterglow. », aborde l'ambivalence face à l'exploitation économique et sécuritaire d'Internet :

> The digital revolution was a dinner party but its afterglow is not. The once utopian promises of high-definition audiovisuals, real-time electronic communication and infinite storage possibilities are just some of the digital culture perspectives that are now widely disseminated. At the same time as these phenomena are still shrouded in the glossy aesthetics of the digital, their tarnished appeal cannot be denied in a world where 'big data' is also the 'big brother' of mass surveillance and where the 'cloud' is made of the metals and minerals of the 'earth' on which data centers are built. Far from immaterial and neutral, our post-digital culture is one where tech is deeply embedded in the geophysical and geopolitical. This is evident at the significant 'other sites' of digital culture such as e-waste dumps, mines, mass-digitisation companies and security agencies.
>
> transmediale 2014 proposed the post-digital moment of 'afterglow' as a diagnosis of the current status of the digital hovering between 'trash and treasure'. afterglow conjures up the ambivalent state of digital culture, where what seems to remain from the digital revolution is a paradoxical nostalgia for the futuristic high-tech it once promised us but that is now crumbling in our hands (transmediale 2014b).

Déchets ou trésors, les conséquences de la révolution numérique, vingt ans après la popularisation d'Internet, sont équivoques, au point de faire voler en éclat les anciens mythes et promesses. L'édition 2015 du festival *transmediale*, « CAPTURE ALL », poursuit cette réflexion sur les effets pervers, contrôlants et répressifs de la révolution numérique :

[13] Lors des dernières éditions, *transmediale* accueilla notamment : Jacob Applebaum, Didier Bigo, William Binney, Wendy Hui Kyong Chun, Jordan Crandall, Kate Crawford, Stephen Graham, Richard Grusin, David Lyon, Evgeny Morozov, Trevor Paglen, Lisa Parks, Jussi Parrikka, Laura Poitras, Antoinette Rouvroy, Tiziana Terranova, McKencie Wark, Ai Weiwei.

> While debates rage over government and corporations operating to covertly "collect, process and exploit" all communication flows, are our own roles and responsibilities perhaps being downplayed? … In a situation where the notion of a "full take" of all communication seems symptomatic of how the state has incorporated a cybernetic feedback ideology with deep historical roots, it is undeniable that we need perspectives that go beyond the role of the individual. However, the "self" has also become the contemporary notion of an individual at the intersection of subjectivity and data flows. In the logic of 'capture all', life is increasingly governed by never-ending predictive control. Value can now potentially be extracted from everything, and productivity measurement can be applied to all aspects of life (transmediale 2015).

Dans ce contexte totalisant, où les mots-clés des pratiques gouvernementales et économiques sont « collect, process and exploit *all* communication flows » et « *full* take », où le jeu et le divertissement deviennent des lieux et des méthodes d'extraction de valeur marchande, quelle place reste-t-il à une agentivité individuelle qui ne serait pas le résultat d'une forme de contrôle social, ou réinsérer dans les canaux de l'économie capitaliste ?

Le festival berlinois n'est pas seul à soulever ces enjeux. De l'autre côté de l'Atlantique, Eyebeam[14], studio et laboratoire de recherche pour artistes numériques situé à New York, organisait à l'automne 2013 une série d'événements sous le thème *PRISM Breakup*. Inspiré par l'initiative en ligne *Prism Break* (Zhong 2017) et le *Security in a Box*, projet conjoint du groupe d'artistes Tactical Technology Collective et du groupe de défense des droits humains Front Line Defenders (Tactical Technology CollectiveFront Line Defenders 2017), *PRISM Breakup* rassemblait des artistes autour des enjeux de surveillance et de protection de la vie privée. Même si la surveillance gouvernementale est une forme de surveillance aux côtés de pratiques commerciales, elle constitue pour les organisateurs un catalyseur qui forcent les individus à agir, ainsi le thème faisant référence au programme de la NSA :

> In the contemporary digital era, privacy has become a luxury for the initiated. Google and Facebook mine your personal data for a profit, the government monitors your phone calls, even shopping malls track the mobile phones connected to their wifi. In the wake of revelations about the NSA PRISM program, many citizens are left wondering what they can do to protect their privacy. We believe everyone has a right to define their own digital privacy, understand how it is being compromised, and feel empowered to protect it (Eyebeam 2013).

[14] Dont sont issus notamment Cory Archangel, Jordan Crandall, McKenzie Wark parmi bon nombre d'artistes numériques contemporains, notamment Zach Blas, James Bridle, Ingrid Burrington, Paolo Cirion, Brian House et Evan Roth.

Dans tous ces cas, les artistes positionnent leur art comme forme de contestation, de résistance, aux dynamiques de contrôle, d'appropriation privée (« enclosure ») et de sécurisation de l'espace numérique. Que reste-t-il de l'utopie d'Internet, à l'image du village global promis par la révolution technologique de Marshall McLuhan, qui promettait un espace de rencontre, de dialogue, et d'épanouissement individuel et collectif ? Guidant ces réflexions artistiques est l'espoir de faire renaître ou de préserver certaines parties de l'utopie disparue. Ainsi, « afterglow », « CAPTURE ALL » et « PRISM Breakup » finissent-ils par des appels à la révision de la culture numérique actuelle et à la résistance :

> The challenge that this moment poses is how to use that state of post-digital culture between trash and treasure as a still not overdetermined space from which to invent new speculative thought and practice. Are there means of renewal in the excess, overflow and waste products of the digital afterglow (transmediale 2014b)?
>
> We may be able to formulate paths to resist the "full take" of mass surveillance, but can we equally define a resistance to the 'capture all' logic as its gamifying tendency spreads throughout the whole of our culture (transmediale 2015)?
>
> We also recognize that security and privacy, especially at the hardware level, is tricky, but that's not going to stop us from trying to determine how it can best be protected (Eyebeam 2013).

Cette communauté artistique partage également un même éthos de l'esthétique. La critique artistique se manifeste par la création de nouvelles façons de concevoir ce qui est connu, par la recherche de « new connections between art, culture, and technology. » Dans cette perspective, la technologie numérique n'est pas monopolisée par les structures de pouvoir, mais peut être réarticulée, réinscrite dans de nouveaux contextes. *transmediale*, par exemple,

> considers technology as being more than the digital world and the cultural as being more than what emerges from within institutionalized fields of production. Accordingly, the activities of transmediale aim at fostering a critical understanding of contemporary culture and politics as saturated by media technologies (transmediale 2017).

Il devient, dans ce contexte, crucial d'approcher des technologies, de les ouvrir, de les diviser, d'en comprendre les composantes pour pouvoir, par la suite, les réassembler dans des pratiques artistiques nouvelles. À travers ce processus de création critique ou de critique créative, ces artistes et leur art « engage into reflective, aesthetic, and speculative positions in between art, culture, and technology [and] challenge us to rethink our everyday relationship to technology, old and new » (transmediale 2017). Cette relation critique est partagée, dans les grandes lignes du moins, par

plusieurs membres de la communauté artistique qui promeuvent les thèmes de la spéculation, de l'imprévisibilité, de la pensée nouvelle contre des structures sédimentées.

3.5 Précisions méthodologiques : sélection d'œuvres et limite du corpus artistique

Le point de départ de la sélection du corpus artistique est la transposition de la sensibilité critique des études de sécurité laquelle, on se souviendra, refuse d'attribuer un statut ontologique à la sécurité au profit d'une approche inductive. Ainsi plutôt que de chercher à assurer ou promouvoir la sécurité d'un objet, l'État par exemple, les études critiques de sécurité s'intéressent à la pratique et au discours de la sécurité en posant la question : que fait-on au nom de la sécurité ? Cette même sensibilité critique anime la constitution du corpus. Refusant d'attribuer un statut ontologique à l'art, je me tourne vers ce que l'on fait au nom de l'art numérique, de l'art de surveillance. La mise à l'avant-plan de la praxis qui traverse les études critiques de sécurité constitue un outre un point de convergence avec les études médiatiques et la théorie esthétique, où tant Couldry que Rancière appelle à l'adoption de cet angle d'analyse. C'est donc ce trait d'union que je mets en exergue et développe dans l'exploration de l'art et la sélection d'œuvres et qui m'amène à poser les questions : qui se revendique de l'art de surveillance ? Que fait-on au nom de l'art de surveillance ? Quelle forme la critique artistique prend-elle ? Que dit-on à son propos ? Où cet art circule-t-il ?

Deux constats empiriques, précédemment développés, ressortent de l'observation préliminaire d'une centaine d'œuvres et d'artistes. D'abord, de ces artistes se détache une communauté artistique qui se revendique de l'art numérique. Cette communauté partage des institutions et une sensibilité politique et esthétique pour la relation entre technologie-pouvoir-culture. Ensuite, la vive réaction de cette communauté aux révélations Snowden a pris la forme d'une production artistique abondante. Recentrer mon corpus autour de ces deux constats permet de borner mon champ d'analyse à un objet précis — la surveillance algorithmique des communications mondiales telles que mises au jour par Snowden —, à un temps précis — les années suivant les premières fuites publiées dans *The Guardian* en juin 2013 —, et à un contexte culturel commun — la communauté artistique comme public de Snowden.

Au premier regard, il peut paraître hasardeux de vouloir attribuer une présence commune à des artistes provenant de contextes culturels et nationaux distincts. Les États-Unis, le Royaume-

Uni et l'Allemagne diffèrent. Il faut reconnaître notamment une sensibilité particulière en Allemagne à l'endroit de la surveillance dont les souvenirs des intrusions de la Stasi dans le quotidien de millions de citoyens sont encore frais. Le degré de participation du BND, les services de renseignement allemands, aux efforts de la NSA, les allégations d'instruments de surveillance déployés dans l'Ambassade américaine à Berlin sise à quelques pas du Bundestag, et d'une surveillance ciblée dirigée contre la chancelière Merkel y ont suscité de vives controverses (Poitras et coll. 2013) qui diffèrent largement des débats légalistes sur la limite de la surveillance de la NSA à l'endroit des citoyens américains. Je suggère néanmoins qu'il est possible de parler d'un contexte partagé. D'une part, la communauté artistique se retrouve autour de lieux de circulation, de diffusion et de rencontre communs qui permettent d'établir une continuité dans le dialogue entre des artistes qui proviennent de milieux différents. D'autre part, Snowden présente des pratiques de surveillance qui, si elles demeurent dominées par les acteurs américains et britanniques, impliquent la participation d'agences du renseignement de pratiquement tous les États occidentaux. En outre, les révélations ont été portées au-devant du débat public par l'entremise de médias nationaux qui ont repris des exclusivités provenant principalement de trois grands journaux britannique, américain et allemand — *The Guardian*, *The Washington Post*, *Der Spiegel* — chacun donnant la tribune à quelques journalistes ayant eu un accès privilégié au lanceur d'alerte et à sa cache d'informations – respectivement Glenn Greenwald et Ewen MacAskill, Barton Gellman et Laura Poitras (voir notamment Poitras 2014). Ces trois traducteurs de Snowden ont ainsi pu contribuer à uniformiser le discours entourant les révélations.

Le corpus ainsi restreint, je m'intéresse à la façon dont l'art aborde le thème principal de la surveillance algorithmique des communications mondiales. Afin de conserver un niveau de fidélité envers les œuvres et artistes analysés et, en écho à la critique formulée par Holden, afin de contenir le poids de ma propre subjectivité, je laisse les œuvres parler d'elles-mêmes. Qu'ont à dire ces œuvres réalisées, aux dires de leurs auteurs, dans une perspective ou une démarche explicitement critique ? Quels thèmes ou sous-objets de la surveillance ces œuvres identifient-elles ? Quelles critiques y sont formulées ? Ainsi, plutôt que de chercher à refaire une nouvelle typologie de la résistance artistique catégorisée selon la forme de l'art ou de la contestation comme d'autres avant moi (Monahan, Phillips & Murakami Wood 2010; Brighenti 2010a; K. Barnard-Wills & Barnard-Wills 2012), je me penche sur le traitement de la surveillance par l'art.

Suivant les thèmes, objets et dynamiques de la surveillance abordés par les œuvres analysées, ces dernières sont ensuite regroupées sous l'un des trois grands piliers constitutifs d'une gouvernementalité. Pour Foucault, rappelle Mitchell Dean, une gouvernementalité est composée de technologies, de rationalités et de subjectivités qui s'allient afin de rendre le mode de gouvernance opératoire (Dean 2010). Reprenant cette conception du gouvernement, j'organise le corpus d'œuvres en regroupant celles qui permettent de visualiser, de politiser, et de résister chacune de ces trois composantes de la surveillance algorithmique, c'est-à-dire les infrastructures internationales des communications mondiales (technologies), l'opérationnalisation du savoir de sécurité (rationalités) et la participation numérique et la constitution du sujet (subjectivité). Cette division permet de structurer un vaste corpus d'œuvres tout en assurant une cohérence théorique avec la théorisation foucaldienne du pouvoir. Comme le rappelle Foucault, les tactiques de résistance sont inséparables des stratégies de pouvoir (Foucault 1976, 122-133). Les œuvres de la résistance numériques se lisent ainsi en miroir aux structures de pouvoir de la surveillance algorithmique des communications mondiales.

Enfin, je retiens les œuvres et les artistes dont la pertinence sociale semble avérée. Pour ce faire, je porte attention à leur notoriété dans la communauté comme en témoignent les lieux d'exposition des œuvres et l'importance de leur diffusion. Sans être restreint par les limites d'une analyse sociologique, reconnaître l'importance sociale de l'art permet d'éviter de sombrer dans l'excès de marginalité de certaines franges de l'art et de contourner le problème de l'isolement des œuvres qui viendrait miner la portée politique de l'esthétique comme le rappellent les théoriciens de la culture populaire (Rowley 2010). La pertinence sociale des œuvres vient en outre contre-balancer ma propre subjectivité dans la sélection du corpus. Certes, les œuvres retenues dépassent toutes la critique de l'individualisme qui entoure le droit à la vie privée et construisent ensemble un argument cohérent vers une résistance à la fois technologique, qui passe par la réappropriation des technologies numériques, et normative, promouvant la redéfinition du collectif. Une partie de cette sélection d'œuvres m'incombe, mais elle est doublement justifiée à la lumière des structures du pouvoir de la surveillance algorithmique des communications mondiales et de la pertinence sociale des œuvres qui s'imposent comme art phare dans leur communauté.

Ce corpus rencontre néanmoins des limites. D'une part, par sa définition même, il se penche sur la surveillance algorithmique des communications mondiales telles que révélée par Snowden. Or, il s'agit d'une parmi plusieurs autres pratiques de surveillance. En lien avec cette forme de

surveillance, le corpus met l'accent sur la capacité de collecte de mégadonnées et, par le fait même, dirige dans un premier temps toute la lumière vers la nature universelle et indiscriminée de la surveillance. S'il sera plus tard question de catégorisation sociale et de l'effet discriminatoire de la surveillance, ces thèmes ne sont pas abordés sous l'angle des communautés victimes de cette discrimination qui auraient pu mettre en perspective l'inégalité de traitement face à la visibilité et une revendication claire d'une présence égalitaire. D'autre part, en observant la réponse d'une communauté artistique transatlantique à des pratiques de surveillance des dispositifs de sécurité nord-américains et européens, le commentaire sur la résistance esthétique est fortement balisé par le contexte culturel occidental. Si je suggère des points de rapprochement possible dans le moment Snowden entre des artistes des deux continents, je ne prétends pas pouvoir exporter cette sensibilité critique au-delà de la sphère occidentale. Il est à ce titre intéressant de noter que des artistes provenant d'autres milieux politiques et culturels soulèvent des enjeux différents face à la surveillance. Le projet cubain *el paquete semanal* (Garcia Martinez 2017) et le projet *qaul.net* (Wachter & Jud 2018), réalisé en hommage aux manifestants du printemps arabe, par exemple, posent comme question centrale de la surveillance la censure de l'information et la répression des activistes, deux thèmes marginaux dans le corpus retenu.

3.6 Conclusion : la réappropriation de l'univers numérique est-elle possible ? À la croisée de la théorie esthétique et de la surveillance

Que nous enseigne l'art engagé de cette communauté dédiée à l'univers numérique, devenue un public de Snowden ? La réappropriation de l'univers numérique par les pratiques artistiques est-elle possible ?

Sur le plan disciplinaire, le savoir esthétique déstabilise le quasi-monopole du rationalisme des théories dominantes en RI. Le savoir esthétique dépasse cependant les frontières des RI pour s'inscrire dans la politique mondiale, espace de luttes et de conflits. Là, la pratique artistique déstabilise les structures de pouvoir et les subjectivités à travers lesquelles circule le pouvoir. Elle brouille et met au monde. « One of the key challenges ahead [for IR] consists of legitimising a greater variety of approaches to the study of world politics. Aesthetics is an important and necessary addition to our interpretative repertoire, » suggère Bleiker.

> To pinpoint the exact nature of this contribution is not easy, but it can probably be captured best by terms such as creativity and imagination. Aesthetic sources can offer us alternative

> insights into international relations; a type of reflective understanding that emerges not from systematically applying the technical skills of analysis which prevail in the social sciences, but from cultivating a more open-ended level of sensibility about the political. We might then be able to appreciate what we otherwise cannot even see: perspectives and people excluded from prevailing purviews, for instance, or the emotional nature and consequences of political events. … Aesthetics, in this sense, is about the ability to step back, reflect and see political conflict and dilemmas in new ways. This is why aesthetics refers not only to practices of art — from painting to music, poetry, photography and film — but also, and above all, to the type of insights and understandings they engender (Bleiker 2009, 2).

Si le tournant esthétique vise principalement à valider la pertinence de l'art dans la discipline, il faut aussi reconnaître sa pertinence au-delà des RI. Le tournant esthétique ne clôt pas le débat sur l'esthétique. Il laisse insuffisamment explorée la dimension esthétique de la politique. Contournant les spectacles et autres simulacres, le concept de visibilité réaffirme la dimension sensorielle de l'ordre social et politique. L'ordre social et politique détermine ce qui peut être vu et la façon dont on peut percevoir. Dans ce contexte, l'art permet de déstabiliser cette distribution de la visibilité. Traduit en terme rancièrien, la politique esthétique est cette pratique esthétique qui perturbe le partage du sensible et les hiérarchies et relations de pouvoir qui y sont associées. La pratique esthétique conteste l'univers sensible, cherchant à rendre perceptible ce qui ne fait pas partie de l'équation politique.

L'ambiguïté esthétique fait de l'art une avenue de contestation privilégiée. « [T]he arts offer another means to transcend our apparently secure state of existence » (Amoore 2006a, 268). Dénaturaliser, dé-objectiver, dé-ossifier constituent les mots-clés de cette résistance qui vise avant toute chose à rappeler l'immanence et la contingence du monde politique. Le monde politique est une construction tout humaine, rien d'autre que le produit de rencontres impromptues et non linéaires.

> The aesthetic realm, then, though not unproblematically or naturally politicizing, has a capacity to call us into question, to challenge our sense of invulnerability to the problems of the world, and to make us feel a certain discomfort. … it is in our encounters with one another that we are rendered undone, that the threads of our everyday lives can begin to unravel. … it is this moment of vulnerability and contingency, sought by artistic practices that intervene in everyday contexts, that conveys a sense that the apparent materiality of our lives may be less certain and secure (Amoore 2006a, 270).

L'esthétique est déstabilisante sans être grandiose. Il ébranle là les fondements des structures de pouvoir, sème ici le doute quant à la naturalité de l'ordre social. Du coup, l'esthétique bouscule l'ordre établi, crée des brèches temporaires qui laissent libre cours à l'imagination. Dans ce

contexte, « [t]he right question to ask, » dit Raley, « is not whether tactical media [as artistic practice] works or not, whether it succeeds or fails in spectacular fashion to effect structural transformation; rather, we should be asking to what extent it strengthens social relations » (Raley 2009, 28–29). L'esthétique perturbe la prétention du pouvoir à être intouchable en montrant sa fragilité, en s'intégrant dans un processus de définition instable et toujours à refaire et, ultimement en proposant des mondes alternatifs (Amoore 2006a, 264).

Ainsi, l'esthétique est à la fois déstabilisante et prometteuse. Déstabilisante, car elle remet en question la naturalité des structures de pouvoir. Prometteuse, car elle affirme la liberté comme qualité première du politique. Ici, la liberté ne doit pas être réduite à l'absence de contrainte ou la possibilité de choix, mais se comprend au sens où Hannah Arendt l'entendait : comme affirmation de la contingence ou, dans les mots de l'auteure, comme « freedom to call something into being which did not exist before, which was not given, not even as an object of cognition or imagination, and which therefore, strictly speaking, could not be known » (Arendt dans Kompridis 2014, xxvii). La liberté que le tournant esthétique recherche et promeut, c'est cette liberté de comprendre à nouveau ce qui semble déjà compris, de proposer de nouvelles solutions à ce qui semble déjà résolu, de ramener la pluralité et le dissensus là où un seul sens commun subsiste.

Afin de délimiter un corpus d'œuvres critique de la surveillance, je m'intéresse aux œuvres qui répondent aux révélations Snowden et constituent, en quelque sorte, un public du lanceur d'alerte participant avec lui à la définition et à la contestation de la surveillance de masse. Le public que je reconstitue pour la thèse est issu principalement de la tradition de l'art numérique engagé dans une exploration de la relation technologie-culture-pouvoir. Cette communauté — qui ne se veut pas exhaustive de la richesse de la création artistique abordant ce vaste thème — gravite autour des pôles que sont le festival *transmediale* de Berlin et les institutions *Rhizome* et *Eyebeam* de New York.

Dans le contexte de la surveillance, la pratique esthétique est une revendication d'un droit de regard sur l'univers numérique, contestant les mondes économique et sécuritaire. Plutôt que de se limiter aux débats actuels sur le devoir d'établir un compromis entre sécurité et liberté, ou de parler exclusivement de la protection de la vie privée (même s'il ne s'agit pas de nier sa pertinence),

la pratique esthétique de l'art de surveillance s'intéresse au régime de visibilité[15], aux composantes et structures de pouvoir qui disparaissent sous l'effet de la quotidienneté ou du secret d'État. L'art de surveillance pourra ainsi s'intéresser aux infrastructures matérielles de surveillance, au savoir issu de la rencontre entre les mégadonnées, les algorithmes et la rationalité du risque, et à la participation numérique et à l'impératif de visibilité qui soumet chaque individu à la surveillance algorithmique. En rendant perceptible ce qui ne l'est pas, l'art de surveillance crée l'événement politique, de nouvelles sensibilités, de nouvelles subjectivités.

[15] Il faut reconnaître au concept de partage du sensible proposé par Rancière la volonté d'étendre le registre des perceptions au-delà de l'œil. Avec le partage du sensible, l'ordre social dépasse le monde visible. Cela dit, l'utilisation du concept reste plus marginale. Par souci de cohérence avec la littérature existante, particulièrement dans le contexte de la surveillance où l'œil demeure la métaphore dominante (Gilliom and Monahan 2013), j'adopterai néanmoins le terme régime de visibilité.

4 Voir comme le réseau : infrastructures de surveillance et vulnérabilité du droit à la vie privée

> We know that the Internet has been turned into the greatest instrument of mass surveillance in the history of mankind. We know who's responsible for that, we know something about how the NSA does that. 98% of the world's data travels under the oceans. It's a phenomenon that seems everywhere and nowhere at the same time. … [T]he way that the Internet works is, it's not made out of cloud, it's not made up of some kind of weird mystical cyberspace, it's made out of infrastructures, it's made out of buildings, it's made out of routers and switches and it's made out of fiber-optic cables.
> Trevor Paglen[1]

Que les données numériques soient utilisées pour contrôler les mobilités, cela relève désormais du lieu commun. Insérées dans des rationalités de sécurité, les données servent à l'élaboration de catégories de risque, permettent d'assembler des profils in/dividuels, d'identifier des comportements suspects, et d'intercepter préemptivement les menaces imminentes. Mais les données circulent elles aussi, parcourant le globe à la vitesse de la lumière, franchissant des frontières et juridictions nationales. Cette circulation n'est pas innocente, avertit l'artiste britannique James Bridle : « [b]ecause the internet is everywhere, you can go anywhere—but because the internet is real, this also has consequences » (Bridle 2015e). Héritier d'une longue tradition esthétique critique cherchant à rendre visibles les infrastructures invisibles du pouvoir, Bridle explore dans son œuvre technologique Citizen Ex les conséquences de la mobilité internationales des données sur la surveillance algorithmique. « Every time you connect to the internet, you pass through time, space, and law, » explique-t-il.

> Information is sent out from your computer all over the world, and sent back from there. This information is stored and tracked in multiple locations, and used to make decisions about you, and determine your rights. These decisions are made by people, companies, countries and machines, in many countries and legal jurisdictions. Citizen Ex shows you where those places are (Bridle 2015f).

[1] (The Creators Project 2016)

Cette infrastructure, et la mobilité numérique qu'elle permet, modifient notre rapport à l'État, à la pratique de gouvernement et à la citoyenneté, « making us all more international, or super-national » (Bridle cité par Rutkin 2015).

Référence à la locution latine deus ex machina, le citoyen sorti — Citizen Ex — d'Internet est cœur de la réflexion de Bridle. En ce début de siècle marqué par les conflits mondiaux et la surveillance de masse, la citoyenneté constitue pour Bridle un enjeu-clé.

> Algorithmic Citizenship is both a potential threat and a possible solution to many of the issues that our allegiances and rights, guaranteed by traditional citizenship, face in the 21st Century. Used against us, it renders us effectively stateless and without protection, destabilising and destroying the legal protections which keep us from aggression, death, and invasions of all kinds. Properly accounted for, understood, and deployed in the service of citizens themselves, it may strengthen our ability to work and live together, to enact true democracies, and to protect the weak as well as the strong (Bridle 2015e).

Reprenant la définition proposée par Hannah Arendt, « citizenship is the right to have rights, » propose Bridle. « To tamper with [one's] citizenship is to endanger [one's] most fundamental rights. Without citizenship, we have no rights at all » (Bridle 2015e). La citoyenneté détermine nos droits à la mobilité, au travail, au soin, à la participation politique, etc. Elle constitue notre passeport dans un système d'États qui, malgré ses limites, n'a toujours pas montré son obsolescence.

Pour une majorité d'individus, connaître son identité nationale va de soi. Attribuée par le lien du sang ou de la terre, nous obtenons une citoyenneté à notre naissance, éventuellement une seconde selon nos circonstances de vie. L'espace numérique vient compliquer ce rapport à la citoyenneté. Même si Internet semble avoir relégué les frontières au passé, l'économie numérique sur laquelle est fondée la surveillance algorithmique demeure matérielle. L'infrastructure physique qui assure les communications mondiales est déployée inégalement à travers le monde et segmentée par les divisions internationales. Dans Citizen Ex, Bridle identifie deux principales conséquences de cette mobilité. À travers la mobilité des données, les infrastructures internationales de la communication mondiale soumettent les utilisateurs Internet à une multiplicité de juridictions nationales différentes. Celles-ci ne correspondent pas nécessairement à la citoyenneté des utilisateurs ni à celle des organisations et sites visités. Internet ne fait pas disparaître les frontières, mais transforme la façon dont elles sont traversées et contrôlées, et crée de possibles conflits de juridiction. La capacité à traverser les frontières numériques modifie notre rapport à la citoyenneté, nous soumettant à une multitude de cadres législatifs, d'obligations et de protections,

et marquant notre double numérique d'une citoyenneté, la citoyenneté algorithmique, possiblement différente de la nôtre. La mobilité des données influence ainsi la détermination de notre citoyenneté algorithmique, transformant les critères d'attribution et rendant cette citoyenneté fluctuante et éphémère. La citoyenneté algorithmique est fonction de la mobilité Internet, mesurée dans Citizen Ex, en pourcentage des sites visités. Bridle met en garde : « Your Algorithmic Citizenship is how you appear to the internet, as a collection of data extending across many nations, with a different citizenship and different rights in every place » (Bridle 2015f). « That means that fundamental rights around the right to privacy and the right to freedom of expression are being created by this algorithmic citizenship » (Bridle 2017). Marquée par les traces des infrastructures de communication, la mobilité des données fragilise le droit à la vie privée, protection contre la surveillance intrusive offerte par les États à leurs ressortissants.

L'univers numérique transforme la citoyenneté. Lue en parallèle aux débats entourant la déchéance de la citoyenneté, la citoyenneté algorithmique démontre la nature désormais éphémère du lien entre l'État et le citoyen. Dans le contexte des grandes plateformes Internet, la citoyenneté algorithmique constitue une forme de privatisation de la citoyenneté. Pour l'artiste, ces deux perspectives sont peu encourageantes. « To say today that you're a citizen of the internet is dangerous. It harks back to a utopianism about the internet which I shared » (Bridle 2017). Pour protéger les droits humains, qui s'étendent désormais au monde numérique (United Nations General Assembly 2016), pour son potentiel démocratique, la citoyenneté algorithmique doit être défendue. Car la citoyenneté algorithmique est porteuse d'espoir, suggère l'artiste.

> The idea of algorithmic citizenship that emerges from the digital could apply in useful ways… Algorithmic citizenship may potentially be a way of extending suffrage to people with interest in particular areas in interesting ways. It may enable new forms of participatory democracy and proportional representation and other democratic systems like that, which are not always necessarily implemented as effectively as they could be » (Bridle 2017).

À travers Citizen Ex, Bridle encourage une prise de conscience des nouvelles formes de pouvoir issues de l'infrastructure Internet et des contraintes à la vie privée que la surveillance algorithmique impose. « The promise of the internet as an open, free and borderless place, » propose-t-il, « relies on you being able to take advantage of certain tools that enhance your privacy » (Bridle cité par Rutkin 2015). Les infrastructures physiques d'Internet, dit Bridle, jouent un rôle important dans les structures de surveillance. Elle participe activement à la surveillance en filtrant les données et en établissant des niveaux de citoyenneté aux utilisateurs. Les infrastructures

de communication mondiale transforment ainsi l'univers numérique en espace strié (Amoore 2013, 112-113). À première vue, Internet apparaît comme un espace lisse où la mobilité est illimitée. Or, les infrastructures de communication parcellisent les territoires et individualisent chaque donnée, faisant d'Internet un espace de contrôle. La mobilité numérique n'est pas aussi fluide qu'il n'y paraît, réalité qui fait surface lorsque les sites Internet ne répondent pas, lorsque le temps de réponse du réseau est anormalement long, où que les serveurs refusent la connexion repérant à partir de l'adresse IP un risque d'hameçonnage. La mobilité des données sert aussi à identifier les individus suspects, à contrôler leurs comportements à l'extérieur du réseau.

La matérialité des infrastructures mondiales de communications et la transformation de l'univers numérique en espace de contrôle contestent la représentation traditionnelle éthérée et émancipatrice d'Internet. « [A]ll our metaphors are broken, » écrit Bridle.

> The network is not a space (notional, cyber or otherwise) and it's not time (while it is embedded in it at an odd angle) it is some other kind of dimension entirely. BUT meaning is emergent in the network, it is the apophatic silence at the heart of everything, that-which-can-be-pointed-to. And that is what the New Aesthetic, in part, is an attempt to do, maybe, possibly, contingently, to point at these things and go **but what does it mean?** (Bridle 2012; accentuation dans l'original)

Qu'est-ce que cela signifie de surfer sur Internet ? De traverser numériquement les frontières nationales ? De se voir attribuer une citoyenneté algorithmique ? De résister la surveillance algorithmique par le biais des arts et de l'esthétique ? Après un approfondissement des motivations esthétiques qui guident les pratiques de Bridle et de ses compères, j'explorerai plus en profondeur Citizen Ex. L'œuvre montre l'application et les limites du droit national dans le contexte d'Internet. Je m'intéresserai ensuite au projet IXmaps. Le projet cartographie la mobilité non linéaire des communications Internet afin de mieux comprendre la portée de la surveillance de la NSA et les contraintes qu'elle exerce sur le droit à la vie privée des citoyens canadiens. Après un long détour au cours duquel je détaillerai les pratiques de surveillance américaine et l'architecture légale qui les encadre, j'approfondirai les conséquences de ceux-ci sur les communications mondiales. La surveillance des communications mondiales n'est pas l'apanage des États-Unis. On fait plutôt face à une surveillance mondiale des communications bénéficiant des failles et des points de rencontre entre les pratiques de surveillance des agences de renseignement occidentales, les infrastructures mondiales de communication et le fractionnement des protections légales du droit à la vie privée. La surveillance d'Internet est un enchevêtrement entre exploitation et vulnérabilités.

4.1 In/visibilité : réappropriation technologique et regard esthétique sur les infrastructures de communication et de surveillance

Les représentations d'Internet comme un réseau immatériel et le secret des pratiques de surveillance rendent la striation de l'univers numérique difficilement perceptible. Or, pour Bridle, seule une meilleure connaissance des technologies (« system literacy ») peut accroître l'agentivité des individus soumis à un monde qu'ils comprennent mal (Jozuka 2015; Schwartz 2015). La démarche artistique qui le mène à visualiser les structures invisibles soutenant Internet devient un geste esthétique et politique permettant aux individus d'avoir un plus grand contrôle sur eux-mêmes et leur environnement. La démarche, que Bridle nomme New Aesthetic, se veut une réappropriation critique du système.

> [T]he New Aesthetic project is undertaken within its own medium: it is an attempt to "write" critically about the network in the vernacular of the network itself… Each image is a link, hardcoded or imaginative, to other aspects of a far greater system, just as every web page and every essay, and every line of text written or quoted therein, is a link to other words, thoughts and ideas. Again, in this the New Aesthetic reproduces the structure and disposition of the network itself, as a form of critique… It is deeply engaged with the politics and politicisation of networked technology, and seeks to explore, catalogue, categorise, connect and interrogate these things. Where many seem to read only incoherence and illegibility, the New Aesthetic articulates the deep coherence and multiplicity of connections and influences of the network itself… Without a concerted effort to raise the level of debate, we just loop over and over through the same fetishisations and reifications, while the real business of the world continues unexamined. Those who cannot understand technology are doomed to be consumed by it. … Technology is political. Everything is political. If you cannot perceive the politics, the politics are being done to you (Bridle 2013).

Visualiser les infrastructures permet de politiser le rôle des technologies dans les structures de pouvoir. En insistant sur la nature matérielle de l'univers numérique, Bridle conteste la naturalité des structures de pouvoir et la neutralité politique de la technologie. Le design, le déploiement et l'encadrement judiciaire des technologies créent des asymétries de pouvoir favorisant certains au détriment de d'autres. Visualiser les biais des technologies permet de contester ces asymétries et le technofétichisme ambiant. À l'inverse, les visualisations et réappropriations critiquent la technophobie qui rejette les technologies. En s'appropriant les technologies, Bridle joint l'émerveillement à la réflexion critique. Contre la recherche d'authenticité dans le retour au bois et le rétro, la symétrie de l'approche de Bridle, qui explore Internet à partir de ses fragments, rappelle la richesse et l'excitation du moment présent et des capacités offertes par les technologies numériques (Bridle 2012). Plutôt que de chercher à imposer un sens à Internet à partir de

conceptions du monde extérieures au réseau, le projet de l'artiste est immanent. Il cherche à découvrir le réseau, ces fonctionnalités et les effets concrets de l'utilisation des technologies. Il laisse le réseau généré son propre sens.

Comme l'observe Claire Richard, critique artistique pour le Nouvel Observateur, « Citizen Ex cherche surtout à donner à penser… pour se souvenir que "chaque fois que vous vous connectez à Internet, vous traversez du temps, de l'espace et des lois" » (Richard 2015). Bridle ne propose pas de réponse définitive. À travers une présentation alternative, inhabituelle des pratiques essentiellement invisibles, Citizen Ex invite le spectateur à réfléchir sur la mobilité des données induites par la géographie des infrastructures Internet, sur les formes de pouvoir et les opportunités qui en résultent. La nouvelle esthétique est

> an appeal to, and act of confidence in, the network itself, in the systems and people that comprise it, to follow their own ideas and intuitions, educate themselves and, outwith a hierarchical commentariat, come to their own conclusions. The onus is on the reader to explore further, just as and because the onus is on the individual in a truly networked politics. … we live in a world shaped and defined by computation, and it is one of the jobs of the critic and the artist to draw attention to the world as it truly is (Bridle 2013).

Quoique lui-même adopte une définition minimaliste de l'esthétique, « by which I meant simply, "what it looks like" » explique-t-il, et quoiqu'il dise ne pas être au fait des débats théoriques de l'esthétique (Bridle 2013), Bridle se situe néanmoins dans une riche tradition de l'esthétique critique. Depuis Walter Benjamin, cette tradition voit dans le renversement des images l'opportunité de révéler la véritable structure du monde, et susciter l'inconfort et un changement de comportement chez le spectateur (Debord 1996; Gracyk 2013; G. Graham 2005, 231; Azoulay 2011). Elle oppose, pour reprendre la terminologie classique, l'esthétisation du politique à la politisation de l'esthétique que l'historien de l'art Boris Groys résume ainsi :

> [t]he aesthicization of politics is what we would call branding, or design, which presents politics as a seductive spectacle. … Politics become a way to seduce people. On the other hand, the politicization of art is a way to get free of that and to act purely politically — beyond aesthetics, beyond art, beyond seduction, beyond spectacle (Groys cité par Azoulay 2011, 243).

Nonobstant la virulence des critiques à l'endroit de cette démarche (Rancière 2008) et la naïveté de Bridle, la démarche de l'artiste demeure pertinente lorsque la prétention à montrer le monde « as it truly is » laisse le pas à l'exploration des conséquences et significations des technologies. Dans une lecture rancièrienne de la nouvelle esthétique, la démonstration de la vérité

devient l'exploration spéculative du monde technopolitique. Ainsi l'objectif explicatif (Bridle 2017) de Citizen Ex ne devrait pas masquer l'élément spéculatif du projet (Bridle 2015e). D'autant plus que malgré les révélations de Snowden, le mystère demeure sur plusieurs pratiques de surveillance, et que des changements ont pu leur être apportés depuis. La perspective spéculative évite en outre les contradictions actuelles de la démarche de Bridle, notamment quant aux postulats épistémologiques et ontologiques, où l'émergence de sens rencontre maladroitement la révélation de la vérité (Andersen, Vuori & Mutlu 2015; Rancière 2008).

Citizen Ex n'est pas un vase clos. Sa démarche artistique n'est pas unique ni isolée, mais solidement ancrée dans un champ artistique. Comme le remarquerait d'ailleurs Bridle qui note l'importance de l'intertextualité, elle constitue un lien vers d'autres démarches artistiques, son œuvre, un lien vers d'autres œuvres, l'artiste, un lien vers un champ artistique plus vaste qui interroge les relations entre l'invisible et le visible. Ces œuvres et ces artistes se côtoient dans les galeries, se croisent dans les festivals, partagent des références théoriques et politiques, et des objectifs artistiques. La démarche de Bridle s'inscrit dans un riche champ de pratiques artistiques critiques qui situe géographiquement, historiquement et matériellement les structures de pouvoir en offrant un nouveau regard les infrastructures du pouvoir. Ce regard cherche à déstabiliser la compréhension du monde, à offrir une nouvelle perspective qui n'est pas pour autant une réponse définitive aux enjeux contemporains. Pour Trevor Paglen, artiste multimédia, photographe et sculpteur, qui a notamment participé à la réalisation du film de Laura Poitras Citizenfour, il faut réapprendre à voir le monde. Or, cet apprentissage n'est pas aisé, « because the world is always changing and because many of the things that shape the way that the world looks are, quite frankly, invisible. Or that we don't notice, or that we haven't trained ourselves to recognize » (Paglen cité par Johnson 2017). Cela demande un effort, une attention particulière à ce qui compose le monde et aux définitions utilisées pour le rendre intelligible.

Le défi est d'autant plus grand dans le contexte numérique où les métaphores qui permettent d'imaginer Internet — le réseau, le cyberespace, le nuage, l'autoroute de l'information — sont abstraites (Paglen cité par Johnson 2017). L'artiste Ingrid Burrington soulève la même problématique lorsqu'elle pose la question :

> When you *think about* or *use* the internet, what do you see? For a lot of people, the answer is that they see screens—browsers, software, laptops, phones. Maybe they see some hardware in the form of a wifi router. The internet is a network, but individual users mostly

> just get a glimpse of it, usually by peering into black mirrors. The most popular stock photography of internet infrastructure—data centers full of servers and cables—tends to make the physical internet feel clinical, distant, opaque (Burrington 2017).

Malgré sa présence dans le quotidien, l'univers numérique est pour l'essentiel invisible : un fantôme contemporain à la fois omniprésent et absent. « Because of its reliability and ubiquity, » écrit Tung-Hui Hu,

> the cloud is a particularly mute piece of infrastructure. It is just there, atmospheric and part of the environment… While the system of computer resources is comprised of millions of hard drives, servers, routers, fiber-optic cables, and networks, we call it "the cloud": a single, virtual, object (Hu 2015, ix).

Cette incapacité à penser l'infrastructure Internet, c'est-à-dire à penser Internet au-delà de la construction virtuelle et dématérialisée qu'est la nébuleuse nuagique, protège les parties contre le regard. Cette invisibilité masque les relations de pouvoir manifestes dans la géographie d'Internet, dans la division du travail et les pratiques de consommation. Il en va de même de la surveillance algorithmique. Elle n'est pas un produit spontané, mais le produit de décisions historiques, facilitées par les divisions nationales, le déploiement des infrastructures de communication, une technologie « dématérialisée » et des pratiques culturelles. Pourtant voir le tout et ses parties est difficile.

L'invisibilité peut être un instrument du pouvoir, comme le suggère le Critical Engineering Working Group (Oliver, Savicic & Vasiliev 2014), ou simplement le fruit d'un manque d'entraînement (Johnson 2017), d'un analphabétisme numérique pour reprendre le vocabulaire de Bridle (Bridle 2013), ou d'une trop grande familiarité (Amoore & Hall 2010) avec l'environnement. Dans tous les cas, cette incapacité à voir, intentionnelle ou non, est partie prenante des structures de pouvoir et empêche la remise en cause de cette normalité (Mirzoeff 2011). Dans cette optique, Paglen résume le projet critique de son art :

> to learn how to see the moment in history that you live in. Although I sometimes use tropes from documentary and use the kind of aesthetics of documentary, perhaps even, I'm actually trying to do something very different. I'm not trying to tell you something that's true. I'm not trying to do a true statement. What I'm trying to do is to activate your imagination. I'm trying to get you to ask questions about what it is that you think you're seeing, and to put you in the position where, perhaps, what you think you know about the world is destabilized (Paglen cité dans Johnson 2017).

Montrer l'invisible, exploiter les vulnérabilités, imaginer les formes possibles du pouvoir et de contre-pouvoir sont toutes des pratiques de contestation artistiques des infrastructures de

surveillance qui encouragent la critique et la recherche de sens. « The hidden geography of data is folded into a larger terrain of corporate and state power. I hoped that learning more about the former might offer some insight into how we perceive—and potentially challenge—the latter, » écrit Burrington (Burrington 2014b). Qu'est-ce qui émerge lorsque l'on rend visible et met côte à côte les infrastructures mondiales de communication et les pratiques de surveillance algorithmique ? Citizen Ex soulève le lien entre la citoyenneté, définie en terme juridique, et les infrastructures. Visualiser les infrastructures permet de politiser la place des infrastructures dans la détermination et l'application de nos droits. Pour Ben Murray, éditeur à The Space et commissionnaire de Citizen Ex,

> [t]his new interpretation of citizenship constitutes a radical shift away from historical precedent. It begs the question of exactly what a citizen is in a digital world, and how rights and obligations are constantly affected by such a shift. It also opens the door to a far murkier world of which, as the matrix grows about us, we should all be aware (Murray 2015).

Dans ce contexte de transformation, Citizen Ex montre la limite du droit pour assurer la protection des individus contre la surveillance. La protection légale contre la surveillance algorithmique, attribuée en fonction de la citoyenneté d'un individu, est remise en question par la mobilité transfrontalière dans l'univers numérique et l'éphémérité du statut de citoyenneté.

4.2 Persistantes frontières : citoyenneté et droit dans le contexte d'Internet

Conçu pour le festival Web We Want, organisé par le Southbank Centre de Londres dans le cadre des célébrations du 25e anniversaire de l'invention du World Wide Web, Citizen Ex se présente comme une application installée en extension à un navigateur Internet. L'extension compare la localisation géographique des serveurs Internet visités à celle du fureteur à travers les adresses de Protocole Internet (IP). En parallèle, elle enregistre tous les déplacements Internet afin de reconstituer, à partir du portrait global de la migration numérique, la citoyenneté algorithmique de l'utilisateur (Bridle 2015f). Citizen Ex rend ainsi visibles deux réalités : la mobilité internationale des données et les conséquences de cette mobilité sur les droits et la citoyenneté des utilisateurs.

Pour James Bridle, la circulation de nos données produites par la navigation Internet nous soumet non seulement à des cadres légaux différents dépendamment du territoire national où la mobilité virtuelle nous mène, elle participe aussi à la détermination de notre identité et, par

conséquent, aux droits et obligations qui nous sont associés. S'inspirant des travaux de John Cheney-Lippold, Bridle soutient que la détermination d'une identité algorithmique à travers notre comportement Internet, pratique d'abord commerciale, est reprise par les gouvernements afin de nous attribuer, en plus des catégories de genre, d'orientation sexuelle, de classe sociale, de race, d'intérêts, etc., une citoyenneté algorithmique (Cheney-Lippold 2011; Cheney-Lippold 2016). La mobilité d'Internet transforme notre rapport à la citoyenneté. La citoyenneté n'est plus attribuée par le droit du sang ou du sol, elle est construite au gré de notre circulation numérique et devient partielle et évolutive. Citizen Ex propose une façon de visualiser cette nouvelle citoyenneté « where your citizenship is a percentage based on the different places you visit » (Bridle 2017). Ainsi, un utilisateur Facebook deviendra progressivement Américain ou Irlandais, un utilisateur Google américain ou suédois. Le citoyen de Citizen Ex sera à divers degré américain, canadien, irlandais, français, etc. dépendamment de sa mobilité numérique et de l'emplacement des serveurs contactés. « National citizenship is normally seen as binary: You either are, or are not, a citizen of a country, » écrit John Cheney-Lippold.

> But Bridle's plug-in assigns you a percentage-based citizenship where you can be 54.8% Irish, 43.7% American, 1.49% German, and even 0.01% Estonian, as I currently am. I say "currently" because our algorithmic selves alter minute by minute and byte to byte depending on how we're using the internet. Last night, after chatting with friends living in England, you might have skewed British. This morning, chatting to your cousin in Spanish, Mexican (Cheney-Lippold 2017b).

Pour l'artiste, connaître le pourcentage de citoyenneté est primordial pour comprendre les pratiques de surveillance américaine. « Government surveillance agencies like the NSA and GCHQ use your Algorithmic Citizenship to decide whether to spy on you, » écrit Bridle.

> For example, the NSA is not allowed to spy on US citizens, so they use browsing data to assign a percentage score to everyone on the internet. If that score drops below 50% American, then they can record them: different laws apply to them, even if they don't know anything about them except how they behave online (Bridle 2015e).

La détermination du statut de citoyenneté de la personne surveillée est au cœur des pratiques et de la rationalité de surveillance. Cette distinction entre Américains et étrangers détermine la nature des protections légales offertes contre la surveillance et délimite le champ d'intervention du renseignement américain prioritairement orienté vers l'extérieur des frontières nationales. S'il est possible pour la NSA de surveiller des Américains, les contraintes seront beaucoup plus restrictives.

Si Citizen Ex se veut une réflexion sur la citoyenneté, la première information que révèle l'extension est géographique. À partir des informations IP, elle compare la position géographique de l'utilisateur à celle du site Internet visité. Ainsi, la première réalité que Citizen Ex rend visible est la grande mobilité d'un surfeur Internet. Le monde semble à portée de main. Citizen Ex attire également l'attention sur un deuxième phénomène : la dissociation entre la nationalité d'une organisation et la localisation réelle de son site Internet d'une part, et entre la nationalité d'une organisation et la juridiction nationale à laquelle son site Internet est soumis d'autre part. Ces dissociations éclairent deux réalités distinctes de la matérialité des infrastructures, propres à la gouvernance du réseau — la géographie du contenu Internet et l'administration des noms de domaine — et rappellent la persistance des frontières internationales et autres divisions territoriales dans la planète Internet.

Lorsqu'un utilisateur insère une adresse Internet dans la barre de navigation du fureteur, l'adresse est traduite dans une série de nombres. Pour le site google.com, par exemple, ce sera 74.125.226.31. Cette série de nombres, l'adresse de protocole Internet[2] (IP), permet aux ordinateurs de communiquer entre eux. Chaque poste d'accès à Internet est identifié par une adresse IP. Dans sa version classique[3], elle est composée d'une suite de quatre nombres de 0 à 255, séparés par des points pour une grande lisibilité. Chaque adresse IP est unique à un poste d'accès et est attribuée par la Société pour l'attribution des noms de domaine et des numéros sur Internet[4] (généralement connue sous l'acronyme ICANN) dans le cadre de la délivrance des fonctions de l'Autorité chargée de la gestion de l'adressage sur Internet[5] (IANA). L'ICANN remet des blocs d'adresses IP aux cinq Registres Internet régionaux qui sont eux responsables de les redistribuer, généralement en sous-blocs, aux différents réseaux locaux ou nationaux, par exemple aux gouvernements, universités et opérateurs de réseaux[6]. Chaque réseau se voit attribuer un numéro de système

[2] « internet protocol »

[3] Les adresses IP classiques, dites IPv4, étant à 99% attribuées, l'Autorité chargée de la gestion de l'adressage sur Internet (IANA) a développé un nouveau type d'adresse IP hexadécimale dite IPv6 (par exemple, 2001:db8:582::ae33) faisant passer de 4,3 milliards à 340 sextillions 3,4 x 10^{38} le nombre d'adresses IP. En date de 2014, seulement 1% des adresses IPv6 étaient attribuées

[4] Internet Corporation for Assigned Names and Numbers

[5] Internet Assigned Numbers Authority

[6] Malgré les imprécisions qui pourraient en résulter, j'emploie l'expression opérateur de réseaux pour identifier les entreprises responsables du fonctionnement des infrastructures primaires d'Internet, connues sous le terme de la dorsale Internet (« Internet backbone »). Le terme fournisseur de services fait référence aux entreprises offrant des services de courriels, des médias sociaux, etc. Cette division est approximative. Il peut arriver que certains opérateurs de réseaux comme Bell Canada ou Vidéotron offrent également des services Internet. Inversement, des fournisseurs de service comme Facebook et Google peuvent être propriétaires de réseaux privés et publics. La distinction permet

autonome (ASN) qui permet d'identifier l'administrateur des adresses IP (ICANN 2011b; ICANN 2015).

Internet, « the inter-network », est ainsi composé d'une multitude de réseaux partageant les mêmes protocoles et lié entre eux par les points d'échange Internet[7] (IX ou IXP), points de passage névralgiques des communications mondiales. Dans Tube, voyage journalistique au cœur des infrastructures Internet auquel fait référence Bridle dans son œuvre, Andrew Blum résume ainsi le fonctionnement d'Internet.

> When I enter an address into my browser, a thousand tiny processes are set in motion. But in the most fundamental terms, I'm asking a computer far away to send information to a computer close by, the one in front of me. Browsing the web, that typically means a short command—"send me that blog post!"—is volleyed back with a far larger trove, the blog post itself. Behind the URL—say, www.mapgeeks.com—is a self-addressed envelope with the instructions that connect any two computers. Every piece of "packet," of data traveling across the Internet is labeled with its destination, known as an "IP" address. Those addresses are grouped into the equivalent of postal codes, called "prefixes," given out by an international governing body, the Internet Assigned Numbers Authority. But the routes themselves aren't assigned by anyone at all. Instead, each router announces the existence of all the computers and all the other routers "behind" it… Those announcements are then passed around from router to router, like a good piece of gossip (Blum 2012, 29).

Par sa conception, Internet fonctionne ouvertement. Lors d'une communication d'un appareil à un autre, chaque réseau affiche publiquement les adresses IP auxquelles il donne accès et les diverses connexions qu'il entretient avec les autres réseaux[8]. Les communications, ou paquets de données[9] trouvent leur route aller-retour parce qu'elles partagent un protocole commun qui les identifie avec les coordonnées des ordinateurs en communication et des instructions sur le service demandé. Sans ces points de rencontre physiques et normatifs que sont les points d'échange et les protocoles, il y aurait plusieurs réseaux parallèles, mais pas d'Internet. Ces informations de protocole sont appelées des métadonnées, des informations sur les données, constituées par les informations nécessaires à la mobilité des communications. Ainsi, une commande de navigation Internet générera des métadonnées : l'adresse IP, le fournisseur de service Internet, des détails sur le matériel informatique[10], le système d'exploitation, la version du fureteur, la date et l'heure de la

néanmoins d'identifier deux structures différentes d'Internet : la mobilité des données et le stockage (l'immobilité) de données.

[7] « Internet exchange point »

[8] Toutes, ces informations sont enregistrées auprès d'ICANN et accessible publiquement par l'entremise du service WHOIS ou de services privés comme ipinfo.io ou who.is.

[9] « data packets »

[10] « hardware »

communication, les pages visitées et des données hébergées localement (MacAskill & Dance 2013). Ces métadonnées sont nécessaires à la mobilité des paquets de données et enregistrées par les fournisseurs de service, notamment, pour mesurer la performance ou l'utilisation de leurs services, et éventuellement à d'autres fins commerciales comme la publicité.

Les identifications de protocoles permettent de connaître la route d'une communication, c'est-à-dire les différents serveurs par lesquels la communication ou la requête est passée pour atteindre sa destination finale. Elles donnent également des renseignements géographiques. Chaque réseau qui se voit attribuer des adresses IP doit fournir des coordonnées. Partant du postulat selon lequel les réseaux conservent leurs serveurs à proximité, il devient donc possible de connaître approximativement la localisation géographique des postes d'accès Internet et donc de l'utilisateur ou du site Internet visité. Ces informations sont approximatives, d'une part, car les adresses IP sont généralement celles de serveurs des fournisseurs de service à partir desquels ils construisent des réseaux privés qui eux s'étendent jusqu'aux utilisateurs individuels. Ces réseaux privés ne sont pas affichés publiquement. Par conséquent, la localisation géographique d'un utilisateur individuel est celle du point de jonction entre le réseau privé et le réseau public Internet. D'autre part, plusieurs sites Internet d'importance sont hébergés par des réseaux de diffusion de contenu[11] (CDN). Ces réseaux sont composés de plusieurs serveurs pouvant être répartis à différents endroits. Or, seuls les fournisseurs des CDN sont enregistrés. Cela ne signifie pas pour autant que les serveurs de leurs CDN sont situés au même endroit.

Citizen Ex utilise les données publiques d'enregistrement fournies par les réseaux pour attribuer l'emplacement géographique d'un site Internet. En repérant, à travers l'adresse IP, l'emplacement géographique présumé des serveurs d'un site Internet, Citizen Ex permet, par exemple, de constater que les sites des quotidiens français Le Monde (lemonde.fr) et britannique The Guardian (theguardian.com) sont hébergés aux États-Unis. Citizen Ex est cependant restreint par l'imprécision des données publiques. Ainsi, si l'adresse IP du Guardian (151.101.45.111) indique que son site Internet est hébergé par Fastly, enregistrée à San Francisco, la compagnie, qui fournit également le New York Times, l'American Civil Liberty Union et le Gouvernement britannique (Fastly 2017a), n'a pas de serveur à San Francisco, les plus proches étant à San Jose, à près de 75 kilomètres de là (Fastly 2017b). Le même enjeu de précision survient lorsqu'il tente

[11] « content delivery network »

d'identifier l'emplacement de l'utilisateur. Ainsi, géographiquement à Montréal, mais sur un réseau de la compagnie ontarienne Cogent Communication, Citizen Ex me situe à North York en région torontoise.

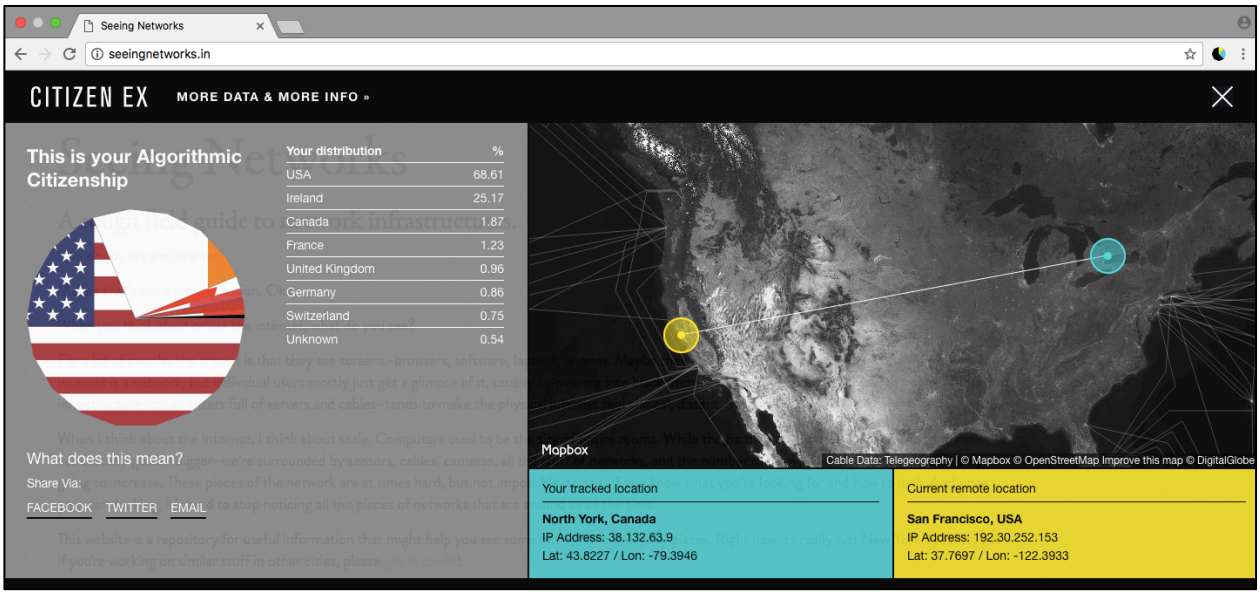


Figure 4.1 : La géographie IP de Citizen Ex de Montréal au site Internet Seeing Networks (in New York City) d'Ingrid Burrington, artiste basée à New York (source : capture d'écran)

Bridle est conscient des limites géographiques de l'adresse IP. Pour connaître un emplacement exact, certains sites Internet ou applications vont demander d'avoir accès aux données GPS d'un appareil ou encore à celles du signal wifi, ce que Citizen Ex ne fait pas. Mais pour l'artiste, la connexion IP demeure pertinente. « The way [Citizen Ex] sees you and the way it sees other websites is the way the internet sees you, every time you connect, » résume-t-il (Bridle 2015e). C'est généralement à travers l'adresse IP que les organisations vont attribuer une région aux visiteurs et charger la version appropriée de leurs sites Internet, que les publicistes vont cibler des produits locaux, que les chaînes de télévision vont autoriser — ou non — la diffusion d'un contenu, et que la NSA va déterminer la localisation d'un individu. Citizen Ex voit comme un réseau et montre la mobilité des utilisateurs Internet et de leurs données, et les dissociations géographiques et de citoyenneté qui existent entre une organisation et son site Internet.

Citizen Ex présente également une autre forme de dissociation : celle entre la nationalité d'une organisation et le cadre juridique auquel son site Internet est soumis. Il souligne la particularité de la gouvernance Internet qui accepte le décalage entre le monde numérique et les juridictions. Le système des noms de domaine, qui traduit l'adresse Internet en adresse IP, facilite

l'utilisation d'Internet, les noms étant plus facilement mémorisables que les séries de nombres. Les noms de domaine ont également une fonction de continuité. Un site Internet avec un nom de domaine conserve la même adresse même si le serveur qui l'héberge physiquement, et donc si son adresse IP, vient à changer. Comme pour les adresses IP, chaque nom de domaine est unique. Le système est aussi géré par l'ICANN, mais délégué en bloc à des administrateurs responsables. Ces blocs sont les domaines de premier niveau[12] (TLD), eux-mêmes divisés en deux catégories. Les domaines de premier niveau génériques[13] (gTLD), par exemple .com, .org, .net, sont des références plus ou moins approximatives à certains types d'organisation, alors que certains domaines, par exemple les .aero, .coop, .museum, .int, sont réservés à des entreprises du milieu aéronautique, à des coopératives, musées ou organisations internationales respectivement. Établis dans le but de conserver une représentation géographique sur Internet, il existe également plus de 250 domaines de premier niveau national[14] (ccTLD) associés à un pays, un territoire ou une géographie. Les .ca, .de, .jp, .fr, etc. sont attribués, à quelques exceptions près comme le .uk britannique[15], conformément au code des noms de pays de la norme internationale ISO 3166-1, reconnue par l'ONU (ICANN 2011a; ICANN 2015; ICANN 2017b). À travers ces noms de domaines, les organisations canadiennes, allemandes, japonaises et françaises respectivement peuvent s'identifier à leur pays d'origine.

Comme le soulève Bridle, la reconnaissance des ccTLD constitue un enjeu politique, notamment pour les communautés et territoires ayant des revendications autonomistes qui désirent avoir une représentation Internet. Les Catalans, les Écossais, les Gallois, pour ne nommer que ceux-là, ont fait face aux limitations de la norme ISO qui ne leur attribuent pas de code de premier niveau (Bridle 2015d; Organisation internationale de normalisation 2017). Inversement, alors que la norme ISO refuse de reconnaître certaines identités nationales, la reconnaissance du Territoire britannique de l'océan indien, qui couvre l'archipel des Chagos, dont l'île de Diego Garcia accueille une importante base militaire américaine, nie l'appropriation du territoire et la déportation des Chagossiens opérés par le gouvernement britannique (Bridle 2015b). Dans le même ordre d'idée, la norme ISO, basée sur l'alphabet latin, complique la présence des langues non latines sur

[12] « top-level domains »
[13] « generic TLD »
[14] « country-code TLD »
[15] En vertu de la norme internationale, le code du pays aurait dû être .gb.

Internet (Bridle 2015a). Plusieurs de ces enjeux ont été abordés par l'ICANN, mais ils illustrent bien la dimension politique de la gouvernance d'Internet.

En plus de la question de la reconnaissance nationale et des vestiges coloniaux qui transparaissent dans l'attribution des droits de présence ou des droits de visibilité Internet, l'administration des noms de domaines est également politique, donnant lieu à des conflits de juridiction entre le code législatif auquel est soumise une organisation et celui auquel est soumis son site Internet. Comme pour les adresses IP, la gestion des noms de domaines est confiée à des entreprises, gouvernements ou universitaires. Chacun est responsable des noms relevant de leur bloc de domaines. La gestion des noms de domaines de premier niveau relève de l'organisation responsable. Il prend en charge l'attribution des noms de domaines et la gestion des registres pour assurer l'unicité des noms contre les tentatives de piratage de sites. Il doit également veiller à ce que le contenu du site Internet respecte la législation nationale qui chapeaute l'organisation, notamment à protéger les droits de propriété intellectuelle. S'il ne peut pas nécessairement effacer le contenu d'un site Internet, le serveur qui contient physiquement les données pouvant être situé à l'extérieur du territoire de l'administrateur de domaine, il peut néanmoins révoquer le nom de domaine rendant le site introuvable, à moins de connaître l'adresse IP du serveur qui l'héberge.

La gouvernance du système des noms de domaine ramène à l'avant-scène l'importance des juridictions nationales. Celle-ci est accentuée par les dissociations existantes entre la nationalité des organisations et l'administration de leur site Internet. S'ils ne sont pas directement associés à un territoire national par leurs noms, les gTLD ne sont pas pour autant extérieurs au droit national. Un nom de domaine générique est en effet soumis au droit national auquel l'organisation responsable est elle-même soumise. Ainsi, le gTLD .com, administré par la compagnie américaine Verisign, est soumis à la législation américaine. L'ICANN est elle-même incorporée en tant qu'organisation sans but lucratif en vertu du droit américain, alimentant les demandes pour universaliser la gestion d'Internet (ICANN 2017a; Yu 2003, 6). En principe, chaque organisation responsable des ccTLD doit être située dans le pays qu'il représente, soumettant les ccTLD à la loi locale. Si plusieurs responsables de ccTLD réservent leur domaine à des organisations basées sur leur territoire, le potentiel de profit associé aux noms de domaines a encouragé plusieurs organisations à les vendre, à l'image des .io, .is (Islande), .be (Belgique), .in (Inde), .tv (Tuvalu) et autres .cc (Îles Coco), sans égard à la nationalité de l'organisation, encourageant les dissociations de nationalité.

Discutant du cas du ccTLD .ly attribué à la Libye, Citizen Ex rappelle la pertinence de ce cadre législatif local pour la présence Internet (Bridle 2015c). Bridle rapporte ainsi le cas de Violet Blue, journaliste et blogueuse américaine écrivant sur le thème de la sexualité. En 2009, Violet Blue a lancé le service de réduction de liens vbly (vb.ly), similaire aux services bitly (bit.ly) et owly (ow.ly). Toutefois, contrairement aux autres services qui refusent de raccourcir les sites avec un « contenu offensant » notamment à caractère pornographique, vb.ly ne filtrait pas les sites Internet dont les liens étaient raccourcis. vb.ly se présentait ainsi comme « the Internet's first and only sex-positive URL shortener » (Needleman 2009). Or, le service opérait sans égard à la loi régissant le domaine .ly. Malgré les contestations contre la censure imposée à l'égard de leur service, vb.ly fut fermé par les autorités responsables du domaine .ly, la pornographie étant interdite en vertu de la législation libyenne. Dans un autre exemple rappelant l'importance des législations nationales, Bridle rapporte que le site Internet de la compagnie libyenne Lybian Spider (lybianspider.com) fut fermé en mars 2011, au cœur de l'intervention de l'OTAN contre Kadhafi, par son fournisseur de service américain, Softlayer. Le domaine .com étant sous juridiction américaine, le gouvernement américain a demandé au fournisseur de déconnecter les communications de l'entreprise libyenne (Bridle 2015c).

Pour Bridle, visualiser les structures d'Internet ramène le politique à l'avant-scène.

> We often think about the internet as something remote, distant, and ephemeral, and use terms like "the cloud" to describe it. But in fact, the internet is very real, and very solid: a world-wide infrastructure of computers, cables, routers—and people. And that infrastructure means its connected to real places, with real territory, real citizens, and real politics (Bridle 2015h).

Citizen Ex rappelle la persistance des frontières dans l'univers numérique et soulève la relation étroite entre gouvernance, frontière, espace et infrastructure. Internet est politique. Il rend visible ou masque l'existence de certaines communautés, crée des conflits de juridiction, soumet les utilisateurs à plusieurs cadres législatifs. Citizen Ex met l'accent dans ce premier temps sur les dissociations géographiques et de nationalité qui résultent de la structure d'Internet et des écarts de droits, d'obligations et de protections qui résultent de ces dissociations. Cette chose « très réelle, et très solide » qu'est l'infrastructure Internet demande d'être déployée dans un espace tout aussi réel : enfouie sous la terre, au fond des mers ou regroupée dans des centres de données.

Même si, pour l'artiste, l'Internet n'est pas un espace — « The network is not a space (notional, cyber or otherwise) and it's not time (while it is embedded in it at an odd angle) it is

some other kind of dimension entirely, » écrit-il (Bridle 2012) —, la spatialité et la matérialité demeurent centrales, supports essentiels tant à Internet qu'à Citizen Ex. D'une part, Bridle conclut chaque section du site Internet du projet avec une photo montrant les traces de la présence physique des infrastructures de communication dans l'environnement. D'autre part, la carte du monde sur laquelle s'affiche la mobilité numérique est traversée de fines lignes blanches. Celles-ci représentent les câbles sous-marins de fibre optique, dorsale des communications mondiales[16]. La surveillance des données de masse menée par la NSA est marquée par ces écarts de droits et la géographie de ces infrastructures. Le déploiement des infrastructures de communication confère à la NSA et ses consœurs qui ont des accès privilégiés aux câbles sous-marins de fibre optique, aux points d'échange Internet ou aux centres de données des avantages importants ou des occasions de surveillance que Bridle laisse aux autres le soin d'explorer.

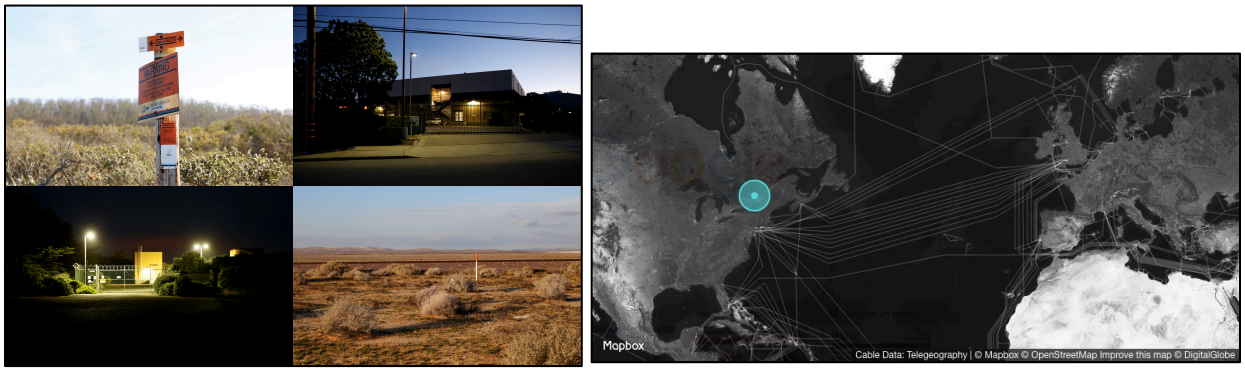


Figure 4.2 : Traces
Mosaïque des infrastructures de communication au quotidien et de la matérialité dans Citizen Ex (source : Bridle 2015f)

4.3 Spatialité, matérialité : exploitation des infrastructures de communication mondiale et de la mobilité non linéaire des données

Contrairement à la représentation de la mobilité qui est faite dans Citizen Ex, la circulation des données ne suit pas la plus courte ligne droite. Une communication ne suit pas une logique géographique, mais saute d'un réseau à un autre jusqu'à atteindre la destination finale, selon une logique de marché, conformément aux ententes commerciales entre les opérateurs. Certes, la circulation des données mène l'utilisateur aux quatre coins du monde, parfois même sur des territoires ne correspondant pas à la nationalité de l'organisation avec laquelle il communique. Cette mobilité et les dissociations géographiques et de nationalités affectent les droits auxquels l'utilisateur est soumis, dit Bridle. Elle facilite notamment la surveillance. Elle permet aux agences

[16] « Internet backbone »

de renseignement d'intercepter et de copier les signaux et données à partir d'endroits stratégiques, généralement les serveurs des fournisseurs de service ou des points d'accès des opérateurs de réseau.

Citizen Ex identifie le lieu d'origine et la destination d'une communication entre lesquels il tire un trait droit. La mobilité Internet n'est pourtant pas linéaire. Cette mobilité dépend des opérateurs réseau et des infrastructures connectant les différentes régions. Au gré des ententes négociées, les compagnies se partagent les différentes couches d'Internet affectant les routes prises par les communications. « Multiple networks run through the same wire, even though they are owned and operated by independent organizations, » explique Blum.

> The networks *carry* networks. One company might own the actual fiber-optic cables, while another operates the light signals pulsing over that fiber, and a third owns (or more like rents) the bandwidth encoded in that light. China Telecom, for example, operates a robust North American network—not as a result of driving bulldozers across the continent, but by leasing strands of existing fiber, or even just wavelengths of light with a shared fiber (Blum 2012, 19).

Une communication Internet ne voyage donc pas en ligne droite à travers les nuages. Elle transite de réseau en réseau jusqu'à atteindre sa destination finale. Une visite sur le site Internet de Citizen Ex à partir du réseau Vidéotron à Montréal constitue un voyage de plusieurs milliers de kilomètres jusqu'à Provo, Utah, où le site est hébergé sur les serveurs de la compagnie Bluehost. Le détail de la route explique qu'au passage, la communication aura transité par le 60 rue Hudson, New York, d'où elle sera connectée, à travers les réseaux de Tata Communications, au réseau de Qwest (Century Link). Celui-ci l'acheminera de New York à l'Ouest américain jusqu'aux serveurs de Bluehost à Provo. Passant à travers les infrastructures américaines, cette communication risque d'être interceptée au passage par la NSA.

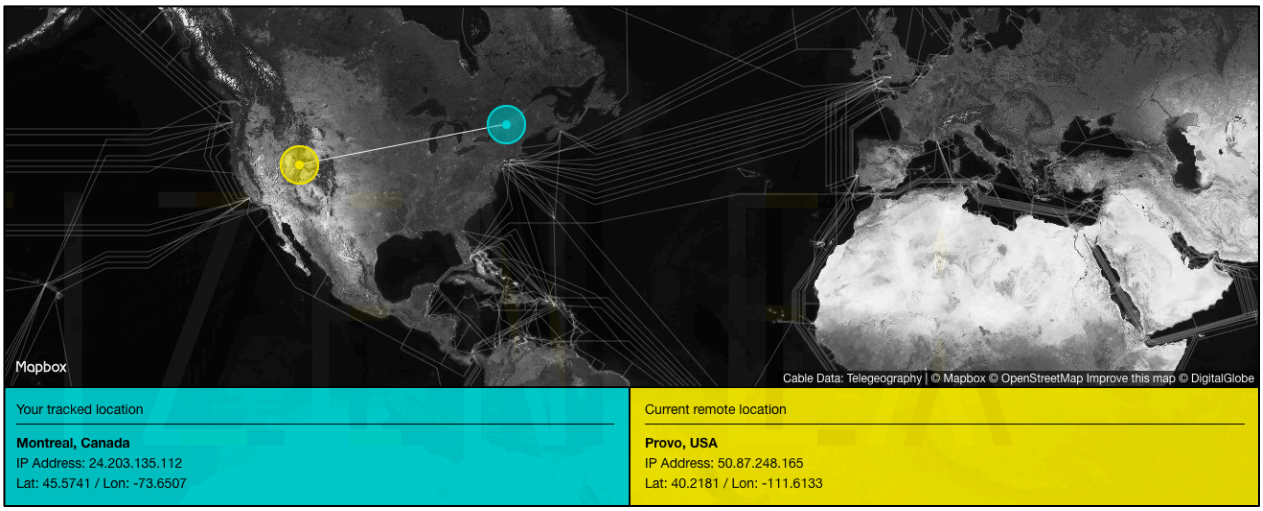
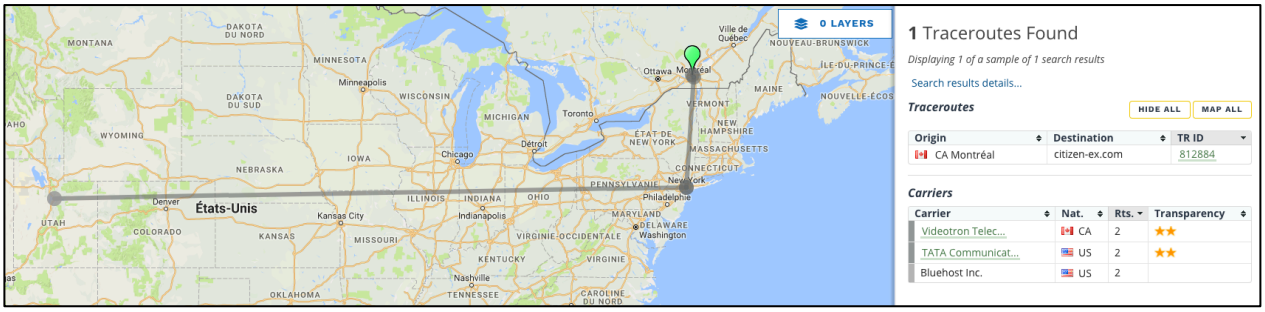


Figure 4.3 : De Montréal à Citizen Ex
vue par Citizen Ex de James Bridle (Source : capture d'écran)



Traceroute details: ID 812884 created on 2017-07-11 15:31:13.582024-04
Origin: Submitted by Simon Hogue from H2M
Destination: citizen-ex.com [50.87.248.165]

Hop	IP Address		Min. Latency	Carrier	Geolocation	Geoprecision	Hostname	Flag
1	24.203.135.0		12	VIDEOTRON - Videotron Telecom Ltee	Montréal QC	Maxmind	24.203.135.0	Flag This IP
2	216.113.126.222		14	VIDEOTRON - Videotron Telecom Ltee	Montreal QC	Maxmind	216.113.126.222	Flag This IP
3	64.86.226.58		18	TATA Communications	New York NY	building level	if-5-2.tcore2.N0V-New-York.as6453.net	Flag This IP
4	216.6.90.21		19	TATA Communications	New York NY	building level	if-2-2.tcore1.N0V-New-York.as6453.net	Flag This IP
5	63.235.41.97		19	Qwest		Maxmind	63-235-41-97.dia.static.qwest.net	Flag This IP
7	63.232.104.62		64	Qwest		Maxmind	63-232-104-62.dia.static.qwest.net	Flag This IP
8	162.144.240.159		64	BLUEHOST-AS-2 - Bluehost Inc.	Canberra 01	Maxmind	162-144-240-159.unifiedlayer.com	Flag This IP
9	162.144.240.15		64	BLUEHOST-AS-2 - Bluehost Inc.	Provo UT	Maxmind	162-144-240-15.unifiedlayer.com	Flag This IP
10	50.87.248.165		64	BLUEHOST-AS-2 - Bluehost Inc.	Provo UT	Maxmind	box1165.bluehost.com	Flag This IP

Figure 4.4 : De Montréal à Citizen Ex, bis
Une route non linéaire[17] *(source : capture d'écran et IXmaps 2016, Traceroute 812884)*

[17] Selon le site de localisation des adresses IP Maxmind.com, la géolocalisation du serveur 162.144.240.159 de Bluehost à Canberra en Australie est une erreur. Il serait plutôt situé à Provo, Utah avec les autres serveurs de la

L'imprévisibilité des routes ne signifie pas pour autant qu'elles soient aléatoires. Internet est plus centralisé qu'il n'y paraît. Projet conjoint de l'Université de Toronto et de l'Ontario College of Art and Design, mené par le professeur Andrew Clement, IXmaps cartographie le chemin réel emprunté par la communication Internet et identifie les lieux suspectés d'interception de la NSA. En levant le voile sur le mystère du fonctionnement Internet, IXmaps montre les conséquences politiques du déploiement des infrastructures Internet.

La mobilité numérique qui se fait par sauts de réseau en réseau nécessite des lieux de rencontre, les points d'échange Internet, pour assurer l'interconnectabilité entre les réseaux. Ces lieux de rencontre et les infrastructures auxquelles ils donnent accès structurent la circulation des données, sans toutefois assigner une route précise. « I hope we're dispelling some of the myths that get in the way, that affect the understanding, in particular the idea that the Internet is a cloud, an ethereal space that doesn't have any borders, » explique Clement.

> In fact, the Internet consists centrally of a few very important points — Internet Exchange points, and other switching centers. These are in big buildings in center cities and who owns those and the deals that are made there are what basically drives the Internet routing (The New Transparency 2013).

Le nombre restreint de ces points nodaux, la position oligopolistique de quelques joueurs majeurs des télécommunications, et les accords commerciaux entre ces joueurs favorisent la concentration des capacités matérielles d'Internet entre quelques mains. Comme l'explique Hu par rapport au réseau américain,

> the structure of the US Internet is bifurcated. On a logical level, we see communication patterns that may resemble a distributed network—although the fact that cloud computing concentrates our files into the data centers of a few underlying service providers, such as Google and Amazon Web Services, complicates this theory. This seemingly distributed network is built, however, on top of a layer that can only be centripetal in nature, whether approached from the question of access—one or two broadband companies per population center, such as Comcast and the telephone monopoly; the market dominance of a handful of

compagnie. Cela est d'ailleurs plus cohérent avec les infrastructures de Qwest (Century Link) situées dans le centre, centre-ouest des Etats-Unis (Bloomberg 2017). Plus généralement, la démarche de géolocaliation d'IXmaps comporte imprécisions et approximations. La localisation exacte d'un serveur est un secret d'entreprise. Certaines informations permettent néanmoins de deviner sa position : l'adresse IP d'une part, et le nom du serveur hôte (« host name ») d'autre part. Si certains noms sont indéchiffrables, certaines compagnies incluent des indices géographiques. Dans l'exemple ci-dessus, TATA Communications précise New York dans le nom du serveur hôte. Cogent Communications, quant à elle, nomme souvent ses serveurs avec le code de l'aéroport de la région (jfk pour New York, iad pour Washington-Dulles et le nord de la Virginie, etc.) (McCann 2011). Il est en outre possible d'estimer les lieux spécifiques des interconnections entre les réseaux en croisant les réseaux révélés par IXmaps aux informations sur le pairage des réseaux (voir peeringdb.com par exemple).

> wireless carriers, such as Verizon and AT&T—or from the level of infrastructure, where six telecommunications companies control the vast majority of the routes. And so the introduction of interoperable protocols such as Internet Protocol, or IP, is like the situation of railroad barons: when they began to widely adopt standard gauge after 1863, interoperability between their networks only increased their concentration of power (Hu 2015, 7).

Un parallèle peut être tiré entre les réseaux canadiens et américains, à la différence près que le réseau canadien n'est pas entièrement autonome. Dans son rapport sur la transparence des opérateurs de services Internet canadiens au sujet de la confidentialité des données, l'équipe d'IXmaps identifie une douzaine d'opérateurs Internet (par exemple, AT&T, Cogent, Level3, TATA) et de détaillants principaux (par exemple, Bell, Cogeco, Rogers, Videotron, etc.) qui se partagent le marché canadien (Clement & Obar 2015, 3). Les opérateurs de la dorsale Internet qui opèrent au Canada sont pour la plupart des compagnies américaines (AT&T, Comcast, Sprint, Verizon) ou internationales (AboveNet, Cogent, Hurricane, Level-3, Limelight, Savvis, Tata and TeliaSonera). Parce que la mobilité des données ne suit pas une logique géographique, mais commerciale, les communications, même canadiennes, passent souvent par les États-Unis, avant de revenir au Canada (Clement & Obar 2015, 14). Cela est particulièrement vrai lorsque les fournisseurs empruntent les réseaux des opérateurs étrangers. L'équipe d'IXmaps appelle un routage boomerang ce type de communication qui circule à travers un pays tiers, bien que l'origine et la destination soient dans le même pays.

Au Canada, près de 25 % des communications nationales circuleraient par les États-Unis (IXmaps 2017b), soumettant les données canadiennes au droit américain. Ainsi, une communication nationale, voire locale, par exemple d'un utilisateur basé à Montréal vers le site Internet de la coopérative financière québécoise Desjardins (desjardins.com) hébergé à Montréal, peut transiter par les États-Unis. Au passage, la communication passera par le point d'échange Internet PAIX-NYC de la compagnie Equinix sis au 111 8th Avenue, New York, bâtiment suspecté par l'équipe d'IXmaps d'héberger un poste d'interception de la NSA. Par le routage boomerang, une communication toute québécoise pourra être surveillée par le gouvernement américain qui interceptera les informations bancaires du communicateur.

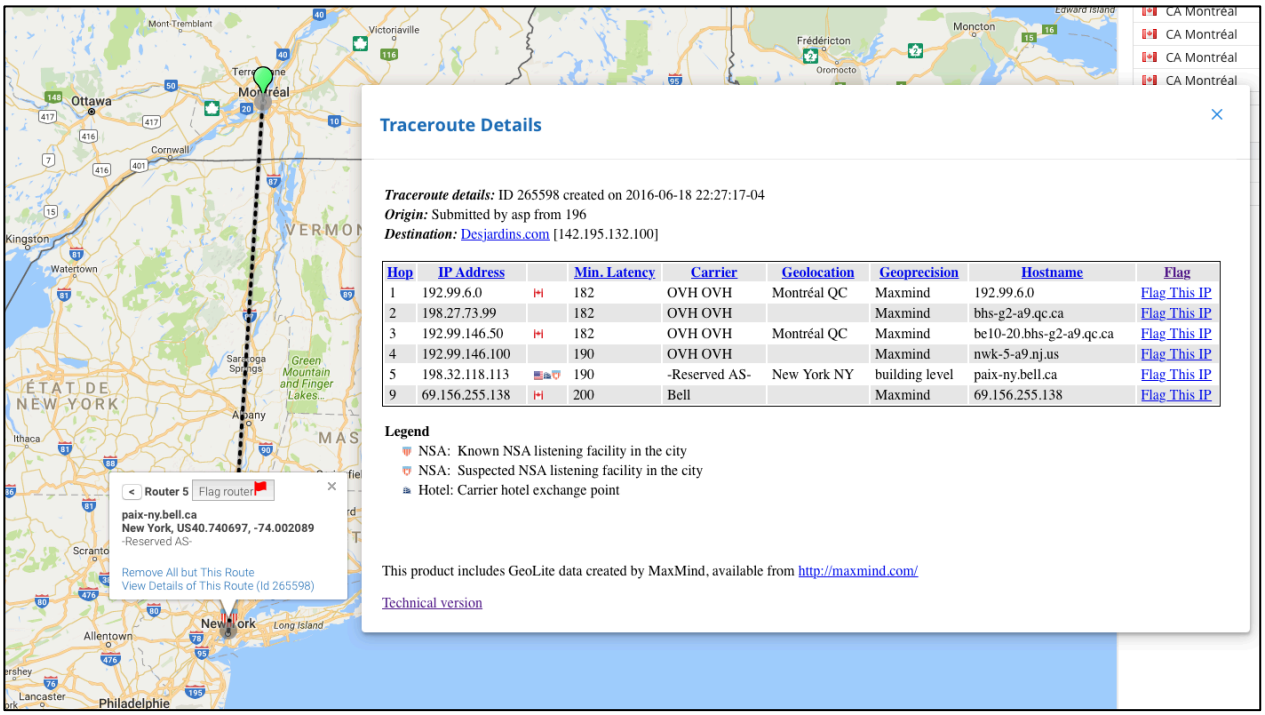


Figure 4.5 : IXmaps : De Montréal à Desjardins
le routage boomerang, exemple d'une visite sur le site Desjardins.com à partir de Montréal (source : IXmaps 2016, Traceroute 265598)

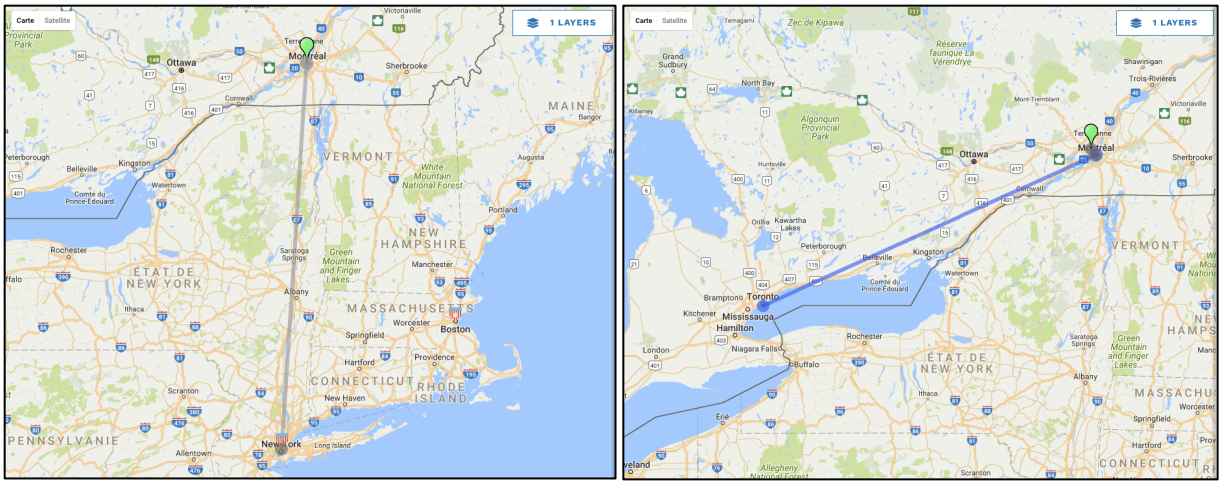


Figure 4.6 : De Montréal à Desjardins.com, bis
l'imprévisibilité des routes Internet (source : IXmaps 2016, Traceroutes 265598 & 790024)

En raison du caractère particulier des ententes entre les acteurs de l'économie numérique, il est difficile de prévoir la route que prendra une communication Internet, celle-ci pouvant aussi bien transiter par les États-Unis que rester au Canada. Ainsi, les routes prises par deux communications générées par deux opérateurs (OVH et Vidéotron respectivement) dont l'origine est Montréal vers le site de Desjardins diffèrent considérablement, l'une transitant par New York,

l'autre par Toronto. Au-delà, des centaines de kilomètres parcourus par la communication, c'est le franchissement d'une frontière internationale qui importe. Pendant le court laps de temps durant lequel les données transitent par les États-Unis, elles deviennent sujettes au droit américain et à la surveillance de la NSA. Le routage boomerang, écrit IXmaps,

> challenges privacy and threatens "network sovereignty," understood as national sovereignty in the internet context. Sometimes termed cyber-sovereignty, this term refers to the ability of a nation-state, or other geographically defined political governance entity, to exercise effective control over critical internet infrastructure within its jurisdictional region. Pursued within a human rights framework, network sovereignty can help protect privacy, as well as achieve routing efficiencies and economic benefits (IXmaps 2017b).

À travers le routage boomerang, les communications canadiennes perdent les protections offertes par la Charte canadienne des droits et libertés. « These communications lose legal and constitutional protection when they leave their home country. At the same time, they are exposed to foreign surveillance and jurisdiction » (IXmaps 2017b). Les États-Unis n'offrent en effet pas de protection légale pour les citoyens étrangers.

4.4 Être ou ne pas être américain : l'architecture légale de la surveillance de l'autre

Dans le contexte de la NSA, « collect it all » n'est pas une phrase creuse. Un ancien cadre du renseignement américain explique : « Rather than look for a single needle in the haystack, his [Former NSA director 2005–2014 General Keith B. Alexander] approach was, 'Let's collect the whole haystack,' 'Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it' » (Nakashima & Warrick 2013). Le mot d'ordre de l'ancien directeur de la NSA guide le déploiement d'un vaste éventail de programmes de surveillance et de partenariats avec des organisations publiques et privées permettant d'acquérir des millions de données de communication d'individus à travers le monde. Dans le documentaire prime *Citizenfour*, Snowden décrit ainsi les activités de l'agence : « the NSA specifically targets the communications of everyone. It ingests them by default. It collects them in its system, and it filters them, and it analyzes them, and it measures them, and it stores them » (Snowden cité par Poitras 2014). La NSA procède à la collecte et au stockage d'un gigantesque bassin d'informations. Des documents du programme BOUNDLESS INFORMANT, programme permettant l'analyse des métadonnées collectées par l'agence, montrent par exemple qu'en un mois à partir du 8 mars 2013, l'unité Global Access

Operations avait amassé 97 milliards de données de communication par courriel et 124 milliards de données de communication par téléphone de partout à travers le monde (Greenwald 2014, 92-93). La NSA, en partenariat avec le Government Communications Headquarters, dit être capable d'accéder à 40 milliards de données de contenu par jour grâce au programme britannique TEMPORA (NSA 2012d, 2).

Officiellement, le mandat de la NSA est double. Il vise la défense des réseaux américains et la surveillance des réseaux étrangers dans une perspective de sécurité nationale :

> [p]ursuant to EO [Executive Order] 12333, NSA is authorized to collect, process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions, and to provide signals intelligence support for the conduct of military operations. The executive order, however, prohibits the collection, retention, or dissemination of information about U.S. persons except pursuant to procedures established by the head of the agency and approved by the Attorney General (NSA 2016).

Dans cette optique, la NSA mène une panoplie de programmes établis sur une architecture législative complexe. Le site Snowden digital surveillance archive (snowdenarchive.cjfe.org) en répertorie plus d'une centaine, l'importante majorité menée par la NSA. Dans son projet Code Names of the Surveillance State, Trevor Paglen identifie plus de 4000 noms de codes utilisés par les programmes de surveillance occidentaux (Paglen 2017a). PROJECT BULLRUN, par exemple, vise le décryptage des communications chiffrées. EGOSTICAL GIRAFFE est un programme de piratage et de dé-anonymisation du réseau TOR. MUSCULAR permet de pénétrer sur les réseaux privés de Google et Yahoo! (Greenwald 2014, 94). RAINFALL, AURORAGOLD, et MYSTIC visent la téléphonie cellulaire (Gellman & Soltani 2014; Gallagher 2014). FOXACID permet d'infecter et de prendre le contrôle d'un ordinateur à distance (J. Ball, Schneier & Greenwald 2013). Ces programmes sont fondés sur différents articles de loi ou éléments législatifs déterminant les autorisations et la portée des pratiques de la NSA en fonction de trois critères : la citoyenneté de la personne surveillée, sa localisation, et la localisation du site de surveillance ou la technique de collecte de données. D'après cette architecture, la surveillance de citoyens américains sur le territoire américain est plus contraignante que la surveillance d'étrangers (MacAskill & Dance 2013; Nakashima & Soltani 2014).

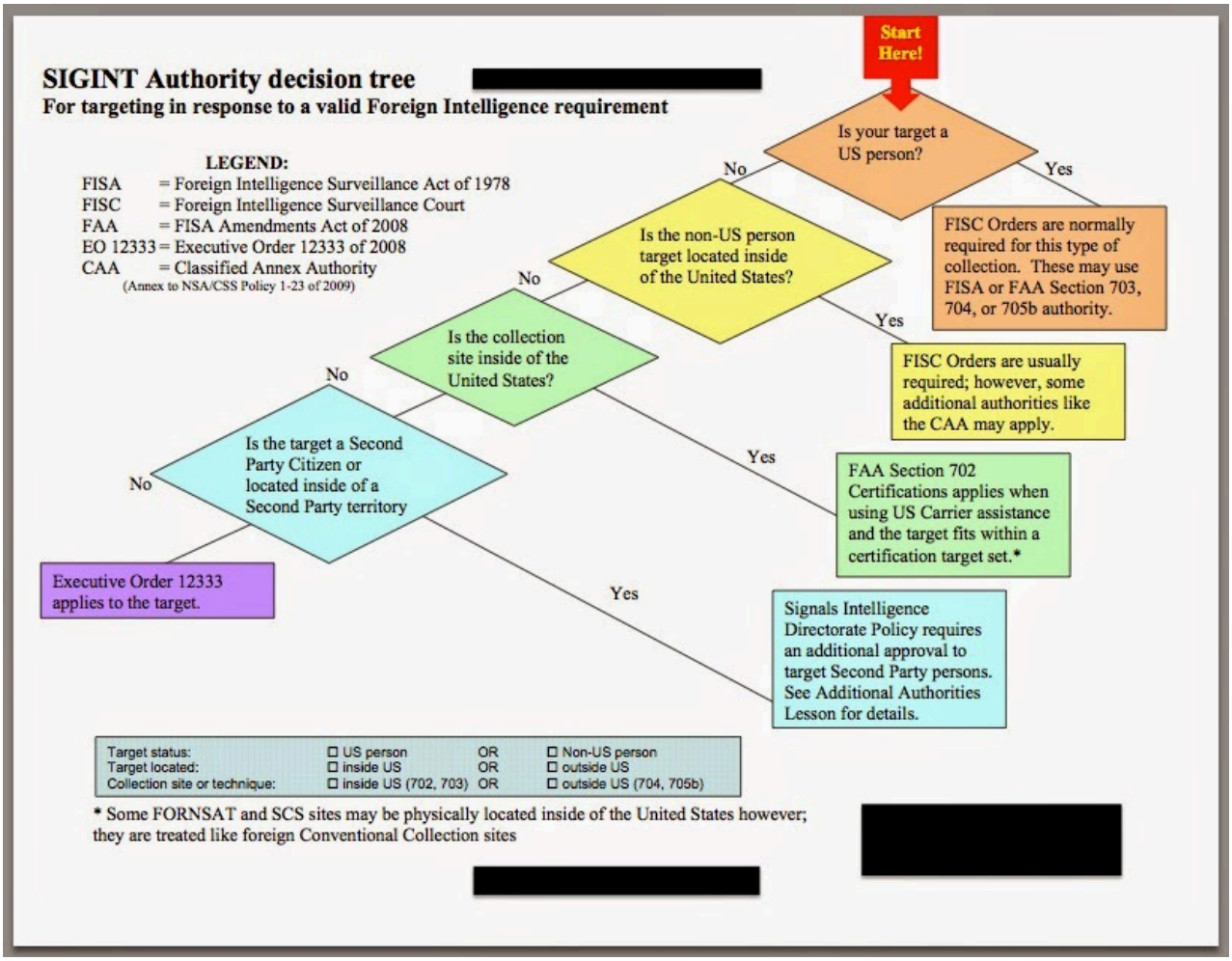


Figure 4.7 : L'architecture légale de la surveillance de la NSA
(source : Nakashima & Soltani 2014)

De tous les programmes de la NSA, trois ont retenu davantage l'attention. La collecte de métadonnées de téléphonie a été le premier mis au jour par Snowden lorsque The Guardian publia l'ordre de la Foreign Intelligence Surveillance Court obligeant Verizon à remettre au renseignement américain ses registres téléphoniques contenant les métadonnées des communications incluant celles d'Américains (Greenwald 2013a; Nakashima 2013). Parce qu'il permettait de collecter des données d'Américains, ce programme a été largement discuté aux États-Unis. Il a été en partie abrogé en juin 2015 lorsque l'US Freedom Act est venu réformer le Patriot Act de 2001 sur lequel il était fondé (Roberts, Jacobs & Ackerman 2015). Deux autres programmes, établis en vertu de l'article 702 du Foreign Intelligence Surveillance Amendment Act de 2008, permettent la collecte des métadonnées et du contenu des communications Internet, incluant la téléphonie sur protocole Internet. PRISM permet la collecte de données à partir des serveurs des

fournisseurs de services Internet (The Guardian 2013b, 3). Les divers programmes regroupés sous le terme de surveillance en amont (« upstream ») permettent de collecter des données à partir d'opérateurs de réseaux « as flows past … ***cable, switch network, and/or routers made possible by the partnerships involving NSA and commercial telecommunications companies*** » (The Guardian 2013b, 3; 2015, 3).

Concrètement, la surveillance des communications Internet, tant à travers le programme PRISM qu'à travers la collecte en amont, est initiée par l'identification d'une personne et d'une installation informatique[18], c'est-à-dire un numéro de téléphone, une adresse courriel, un compte ou un identifiant Internet[19], qu'elle est soupçonnée d'utiliser. Dans la terminologie officielle, la NSA ciblera[20] un individu en surveillant son installation informatique, processus désigné par l'expression assigner un sélecteur[21]. La NSA ciblera un individu en assignant un sélecteur. Un sélecteur identifie uniquement une installation informatique. Il ne peut pas s'agir d'un nom d'individu ou d'un mot-clé. À partir de là, la NSA peut légalement contraindre un fournisseur de services, par l'entreprise du FBI puisque celui-ci est situé sur le territoire américain, ou un opérateur de réseaux à lui remettre toutes les communications adressées ou provenant[22] du sélecteur identifié qui se retrouvent dans ses bases de données ou qui transitent par ses réseaux. Dans le cas de la collecte en amont, l'opérateur de réseaux remettait également toutes communications mentionnant[23] le sélecteur (PCLOB 2014, 32-41). En vertu des modifications apportées aux pratiques de surveillance de la NSA suite aux demandes formulées par la Foreign Intelligence Surveillance Court, la collecte de données de communication mentionnant un sélecteur est interrompue depuis mai 2017 afin d'assurer la reconduction de programme au-delà de décembre 2017 (Froomkin 2017; ODNI 2017a). Si la surveillance en amont soulève le plus d'interrogations légales, le programme PRISM générait, selon des données de 2011, 91 % des communications Internet collectées par la NSA (PCLOB 2014, 33).

L'identification des communications est effectuée par l'entreprise privée qui les transfère ensuite vers les centres de données de la NSA. Celle-ci filtre, minimise selon le vocable officiel,

[18] « technical facility »
[19] « electronic communications emails/addresses/identifiers »
[20] « to target »
[21] « to task a selector »
[22] « to and from »
[23] « about »

alors les données, retirant par exemple ce qu'elle appelle le « high volume, low value traffic », c'est-à-dire les communications lourdes en données, mais dont le contenu d'information de sécurité est faible, par exemple le téléchargement de pair-à-pair (« P2P downloads ») utilisé dans l'échange de fichiers de musique ou de films (GCHQ 2012, 2). La NSA filtre également les communications nationales entre Américains ou entre personnes situées sur le territoire national. Les procédures de minimisation visent principalement à garantir le respect du droit à la vie privée des Américains dans le contexte d'une collecte de données de masse. Selon le libellé officiel de la loi américaine, ces procedures

> are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information (PCLOB 2014, 50).

Une fois les données minimisées, les agents de surveillance peuvent interroger[24] les bases de données pour trouver des informations spécifiques. L'interrogation se fait à partir de programme comme XKEYSCORE (Greenwald 2013b) qui cherche, parmi les données disponibles, des mots-clés — par exemple une adresse IP, de courriel, le nom d'une personne, ou des termes plus généraux comme la prolifération nucléaire (PCLOB 2014).

En principe, la législation américaine protège les citoyens américains, ou plus spécifiquement les personnes américaines (« US persons ») — les citoyens, résidents permanents, les associations composées d'un nombre significatif de citoyens ou résidents permanents américains, et les entreprises enregistrées aux États-Unis — contre la surveillance de la NSA. La loi américaine est ainsi établie pour arbitrer la volonté d'obtenir des informations pertinentes à la défense des intérêts nationaux et le droit à la vie privée des citoyens américains, le proverbial compromis entre liberté et sécurité. Encadrant les activités du renseignement extérieur (« foreign intelligence »), l'ordre exécutif 12333 fait référence à plusieurs reprises aux besoins d'information et de protection des libertés civiles individuelles. D'un même souffle, il est stipulé que

> Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. …

[24] « query »

> The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law (ODNI 1981, Preamble & § 1.1b).

Toutefois, comme le relève John Cheney-Lippold, les mesures de protection offertes par la loi américaine sont souvent ambiguës et incohérentes avec les pratiques de surveillance du renseignement américain (Cheney-Lippold 2016, 1726).

Pierre angulaire de ces protections, le 4e amendement de la constitution des États-Unis protège officiellement la vie privée des citoyens américains contre les fouilles excessives perpétrées par leur gouvernement :

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (cité par Landau 2013, 55).

Pensé à l'origine pour protéger contre les fouilles des maisons, des commerces ou du courrier, le 4e amendement est mis à mal une première fois par l'apparition du téléphone et l'écoute électronique. D'abord autorisées, les écoutes électroniques sont interdites en 1967 dans le jugement de la Cour suprême *Katz v. United States* qui renverse une précédente décision datant de 1928. D'abord appliquée à la police et au contexte criminel, l'interdiction est étendue aux écoutes pour des raisons de sécurité nationale 5 ans plus tard. Dans la foulée du scandale du Watergate, un comité spécial du Sénat est mis sur pied en 1975 pour enquêter sur les pratiques de surveillance du gouvernement. La Commission Church, du nom de son président le sénateur Frank Church, met à jour 40 ans de surveillance excessive ciblant l'opposition politique. Des centaines de milliers de lettres de journalistes, de juges de la Cour suprême, d'employés du congrès et de l'administration aussi bien que celles de citoyens participant au mouvement pour la paix auraient ainsi été ouvertes par le renseignement, sur ordre du gouvernement au nom de la sécurité nationale, sans supervision judiciaire, et en contravention d'avec leurs droits constitutionnels (McCutcheon 2013, 726-727; Landau 2013, 55).

Suite à ce rapport, le congrès adopte le Foreign Intelligence Surveillance Act de 1978 (FISA) encadrant les pratiques de surveillance du renseignement américain. En vertu de FISA, le gouvernement est autorisé à faire de l'écoute électronique s'il possède une « probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign

power » (Cheney-Lippold 2016), excluant formellement la surveillance d'un citoyen américain à moins d'avoir des preuves d'espionnage à son endroit. Prenant acte de la difficulté de connaître avec certitude l'utilisateur d'un poste téléphonique, FISA offre ainsi une marge de manœuvre au renseignement lui permettant de cibler sans mandat des appareils situés à l'extérieur des frontières des États-Unis dont l'utilisateur est probablement une puissance étrangère ou un de ses agents. FISA compense cette flexibilité en restreignant la surveillance aux agents d'une puissance étrangère. Pour les cas nécessitant la surveillance à l'intérieur du territoire américain ou la surveillance d'un Américain suspecté de travailler pour une puissance étrangère, une cour spéciale est créée, la Foreign Intelligence Surveillance Court (FISC), responsable d'évaluer, d'autoriser ou de refuser les demandes de mandat pour procéder à l'écoute électronique. Dans les années qui suivent, répétant la logique du compromis entre liberté et sécurité, le gouvernement étend la législation interdisant l'écoute électronique des téléphones aux communications électroniques, avant d'obliger les opérateurs de réseaux à mettre en place des infrastructures permettant aux autorités d'accéder à leurs données (McCutcheon 2013, 726).

Le Patriot Act de 2001 puis le FISA Amendment Act de 2008 (FAA) viennent cependant modifier de façon importante la portée de la surveillance électronique. Pendant 15 ans jusqu'à sa révision en 2015, le Patriot Act garantit un accès privilégié aux métadonnées téléphoniques en définissant les métadonnées des registres commerciaux dont le propriétaire n'est pas l'individu, mais l'entreprise. Ainsi, la législation américaine ne considère pas la collecte des métadonnées, par opposition à la collecte de contenu, comme une forme d'écoute électronique. Elle n'est donc pas soumise aux mêmes restrictions. À l'origine, les nouveaux pouvoirs autorisant la collecte de registres commerciaux devaient permettre la collecte d'information sur une base individuelle. La loi est rapidement ré-interprétée « to justify requests for domestic telephone metadata delivered in bulk » (Landau 2013, 56). Cette interprétation généreuse n'est plus de mise. La révision du Patriot Act, remplacé le 1er juin 2015 par l'US Freedom Act, interdit la collecte de masse de ces métadonnées ainsi que d'autres informations issues de registres commerciaux (Roberts, Jacobs & Ackerman 2015).

Le FAA, en particulier l'article 702, étend la portée de la surveillance de la NSA. Dans son Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, le Privacy and Civil Liberties Oversight Board (PCLOB), organisation indépendante et bipartisane issue de l'exécutif, résume ainsi :

> Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information (PCLOB 2014, 20).

L'article 702 du FAA apporte des changements importants à FISA. Il autorise désormais le renseignement à surveiller tout individu étranger, plus uniquement les agents de puissances étrangères, situé à l'extérieur du territoire américain. Cette surveillance se fait à partir d'installations situées sur le territoire américain, plutôt que de restreindre la NSA à des activités extérieures, dans le but d'obtenir des informations pertinentes à la sécurité nationale et à la conduite des affaires étrangères des États-Unis. En contrepartie, l'article 702 du FAA oblige la NSA à obtenir un mandat avant de procéder à ses opérations de surveillance. Comme le révèle toutefois Snowden, ces mandats ne sont pas individuels, c'est-à-dire qu'ils ne s'adressent pas à la surveillance d'un individu précis dans le cadre d'une enquête spécifique, mais autorisent la collecte de toutes données en provenance ou à destination d'un sélecteur (Greenwald & Ball 2013). Comme le rapporte le PCLOB,

> [t]here is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the "traditional" FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information (PCLOB 2014, 6).

Les mandats émis en vertu de l'article 702 du FAA ne visent pas des individus, mais des catégories d'informations pertinentes pour la sécurité nationale américaine dont le renseignement estime qu'elles seront probablement transmises par certaines installations informatiques.

Par rapport à FISA, le FAA étend la surveillance ainsi à toute installation liée à une personne étrangère dont il est raisonnable de croire qu'elle est située à l'extérieur des États-Unis et qu'elle puisse fournir des informations pertinentes. La nécessité de cibler une puissance étrangère ou un de ses agents devient pertinente uniquement pour la surveillance à l'intérieur des frontières américaines ou de citoyens américains hors des frontières (Office of General Counsel 2008, 3). Toutefois, à cause de la nature particulière des communications électroniques, la localisation et la citoyenneté d'un individu peuvent parfois être difficiles à identifier. Comme le remarque Cheney-Lippold,

> According to publicly available legal documents, a United States person is, tautologically, anyone who can prove his or her U.S. personhood through a state-authenticated artifact of citizenship, green card, or articles of incorporation. Conversely, a non–United States person is anyone unable to provide such documentation. But conventional proof of citizenship status through documentation is nonviable in a digitally networked world (Cheney-Lippold 2016, 1727).

La NSA fait face à deux enjeux : la forte probabilité, vu les stratégies de collecte, d'amasser des données provenant d'Américains et la difficulté d'identifier la nationalité d'un individu. Sur Internet, un individu ne circule pas avec son passeport ou sa carte d'identité, marqueur traditionnel de la citoyenneté. Face à ces difficultés, la NSA a établi des procédures de détermination qui permettent de statuer sur la citoyenneté et la localisation d'un individu tout en respectant les protections légales offertes aux citoyens américains. Dans « Exhibit B: Minimization procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended », daté de 2017, le procureur général américain Jeff Sessions précise la définition d'un Américain :

> (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.
>
> (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person (Sessions 2017, 3).

Lorsque la citoyenneté d'individu ciblé est inconnue, sa localisation, identifiable notamment par l'indicatif régional de son numéro de téléphone ou son adresse IP, sert de repère. En d'autres mots, lorsque l'expéditeur est inconnu, l'endroit d'émission de la communication fait acte du statut de citoyenneté de l'individu. Dans le document complémentaire, « Exhibit A: Procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended », datant de 2009 et non caviardé, l'ancien procureur général Eric Holder écrit :

> In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person (Holder 2009, 4).

Ainsi, la NSA considère toute communication dont l'origine et l'expéditeur sont inconnus comme émanant d'un étranger, autorisant par le fait même la surveillance électronique. Similairement, toute communication provenant de l'étranger et dont l'expéditeur est inconnu est considérée comme émanant d'un étranger, autorisant également la surveillance. Inversement, toute communication provenant des États-Unis et dont l'expéditeur est inconnu est considérée comme émanant d'un citoyen, interdisant la surveillance, sauf si cette communication est faite avec un étranger ou dirigée vers l'étranger. Si le FAA interdit le ciblage inversé (« reversed targeting »), c'est-à-dire la surveillance d'étranger dans le but d'intercepter les communications d'Américains, la NSA est cependant autorisée à intercepter toute communication dont une des deux fins est extérieure aux États-Unis, dans la mesure où la cible n'est pas américaine. Dans de tels cas, la surveillance d'Américains est dite fortuite (« incidental »). Dans le contexte de la collecte de données de masse des personnes étrangères, la NSA juge qu'il est techniquement impossible de séparer les données des Américains de celles des autres. En contrepartie, des procédures de minimisation assurent la suppression des informations concernant des Américains et le caviardage de l'identité de l'Américain surveillé. Elle est néanmoins autorisée à regarder, à conserver et à utiliser les informations si celles-ci sont jugées pertinentes (Greenwald & Ball 2013; Greenwald 2014, 74; Cheney-Lippold 2016, 1727-1728).

Si le FAA donne de la souplesse à la NSA en laissant à l'analyste le soin de déterminer la citoyenneté et la localisation d'un individu, il est néanmoins tenu de le faire avec diligence. Ainsi, il doit justifier sa décision avec les informations disponibles. Afin de limiter la collecte de communications de citoyens américains, les procédures de ciblage de 2009 précisent que la « NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons » (Holder 2009, 3), une sorte de bottin téléphonique et numérique géant permettant d'identifier les citoyens américains. La NSA ne se limite cependant pas à cette forme de validation. Selon les informations divulguées en 2013 par Barton Gellman et Laura Poitras dans le Washington Post, la procédure de détermination autorise la surveillance lorsqu'il existe « at least 51 percent

confidence in a target's "foreignness" » (Gellman & Poitras 2013). Cette interprétation du processus de détermination est cependant contestée par les autorités américaines. Le PCLOB, qui a pu réviser les procédures et les documents classés, valide la version officielle. Selon le PCLOB, la détermination du statut d'étranger (« foreignness ») ne se fait pas selon un standard de probabilité. « If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting, » écrit le PCLOB (PCLOB 2014, 44). S'il ne dévoile pas les détails des procédures de détermination, il rapporte les statistiques du Département de la justice selon lesquelles en 2013 les analystes de la NSA se trompèrent sur seulement 0,4 % des cas évalués comme preuve de la pertinence des procédures (PCLOB 2014, 44).

Les changements apportés à la structure légale de la surveillance par le FAA sont importants diminuant le niveau de preuve nécessaire pour autoriser la surveillance d'étranger. « [W]here previously the NSA needed individual authorisations, and confirmation that all parties were outside the USA, » écrivent Glenn Greenwald et Ewen MacAskill, « they now need only reasonable suspicion that one of the parties was outside the country at the time of the records were collected by the NSA » (Greenwald & MacAskill 2013). Les procédures de détermination du statut et de la provenance d'une communication garantissent un large rayon d'action à la NSA. Par la bande, ce sont aussi les Américains qui se retrouvent davantage sous surveillance. Jamel Jaffer, vice-directeur légal à l'American Civil Liberty Union (ACLU), voit même dans l'extension de la portée de la surveillance électronique à la suite du FAA la preuve de la volonté des autorités américaines d'étendre leur pouvoir de surveillance sur les Américains comme sur les étrangers.

> The principal purpose of the 2008 law was to make it possible for the government to collect *Americans*' international communications—and to collect those communications without reference to whether any party to those communications was doing anything illegal. And a lot of the government's advocacy is meant to obscure this fact, but it's a crucial one: The government doesn't need to "target" Americans in order to collect huge volumes of their communications (cité par Greenwald 2014, 127).

Pourtant, les efforts déployés pour se conformer au cadre légal de la surveillance démontrent l'importance que l'agence accorde à sa constitutionnalité. Comme la NSA enseigne à ses nouvelles recrues :

> The best way to protect ourselves and our SIGINT [signal intelligence] is to play by the rules. No matter how inconvenient the rules may seem, if we fail to adhere to them, the next set of rules will be far stricter. There are very few things that we cannot accomplish with the existing rules, using the authorities we have and those authorities we can receive (Clapper 2009, 83–84).

La NSA n'agit pas sans égard à la loi, mais exploite les failles et les ambiguïtés au risque de procéder à des interprétations créatives de ses pouvoirs et obligations. Bien que le PCLOB évalue favorablement la constitutionnalité des pratiques de surveillance de la NSA menées en vertu de l'article 702 du FAA, il ne demeure pas moins sceptique quant à la légalité de certains aspects.

> Outside of this fundamental core [— acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court—approved targeting rules and multiple layers of oversight —], certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected (PCLOB 2014, 9).

En outre, la distinction faite entre la collecte de données et l'interrogation des données promue par la NSA est une interprétation de la surveillance contestée en cour, notamment par l'Electronic Frontier Foundation et l'ACLU. Dans une déclaration en cour, faite dans le cadre de la poursuite intentée par l'ACLU contre le gouvernement américain (ACLU v. Clapper), Theresa Shea, directrice du Signals Intelligence Directorate de la NSA, défendait les pratiques de l'agence sur la base de cette distinction.

> only a very small percentage of the total data collected is ever reviewed by intelligence analysts … [a]lthough bulk metadata are consolidated and preserved by the NSA pursuant to Section 215 [of the Patriot Act authorizing the collection of telephony metadata], the vast majority of that information is never seen by any person (cité par Aradau & Blanke 2015, 4-5).

Comme le remarquent Claudia Aradau et Tobias Blanke, « the assumption is that there is no surveillance where data in not 'seen' by a human being » (Aradau & Blanke 2015, 5). Quoique la déclaration de Shea ait été faite en référence au programme de collecte de métadonnées de téléphonie, la même logique peut être généralisée aux autres programmes de surveillance. La NSA ne considère pas la collecte d'information comme une forme de surveillance. Elle n'est donc pas inconstitutionnelle. Cette distinction néglige toutefois l'ampleur du travail mis en œuvre par

l'agence pour accéder à cette masse d'information. Décrivant le fonctionnement de la surveillance en amont, le PCLOB explique :

> Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the "Internet backbone." The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702—tasked selectors on the Internet backbone, *Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection* (PCLOB 2014, 36-37; je souligne).

Dans la logique de la NSA, puisque le travail de filtre a été mené par les entreprises privées et les données analysées et rejetées n'ont pas été collectée, il n'y a pas de surveillance, d'autant plus que toutes ces informations n'ont pas toutes été, ni ne seront scrutées par des analystes. Le chiffre de 26,5 millions de transactions Internet collectées en 2011 par la surveillance en amont est trompeur. D'une part, parce qu'au ratio précédemment présenté et selon lequel le programme PRISM génère 91 % des communications Internet de la NSA, cela signifie que la NSA aurait collecté en 2011 267,9 millions de transactions Internet grâce au programme PRISM. En combinant les deux types de surveillance, la NSA aurait collecté près de 300 millions de transactions Internet. D'autre part, il faut se rappeler que toutes ces données ont été interceptées sur les réseaux ou fouillées dans les serveurs une première, puis une deuxième fois pour identifier les données à transmettre vers les centres de données de la NSA. Ce travail n'est pas à ignorer. D'ailleurs, l'argument officiel voulant que le travail d'accès aux communications et les filtres successifs ne constituent pas une forme de surveillance tant que les données ne sont pas dirigées vers les centres de données de la NSA et que ces données ne sont pas interrogées vit mal au côté des objectifs internes. « Why can't we collect all the signals, all the time? » avait demandé le directeur de la NSA Keith Alexander durant une visite des installations de l'agence de renseignement GCHQ, partenaire de la NSA (MacAskill et coll. 2013). L'interception et le filtrage des données de masse sont indissociables de la pratique de surveillance actuelle. Elles constituent les premières étapes sans lesquelles la suite de la recherche d'information serait impossible.

S'il a été fait grand bruit de la surveillance d'Américains par la NSA et de la complaisance de la FISC (Greenwald 2014, 128-129) qui violent ainsi le droit à la vie privée des Américains, ces

critiques ignorent l'effet de la surveillance américaine sur le droit à la vie privée des autres citoyens de la planète. Pour le gouvernement américain, surveiller les étrangers semble être incontestablement légitime : « Foreign persons outside the U.S. —fair game, » est-il écrit dans un guide destiné aux étudiants de l'école de cryptologie de la NSA (Clapper 2009, 50). Les pratiques de surveillance américaines fragilisent le droit à la vie privée non seulement pour les Américains, mais pour l'ensemble du monde. L'arbre ne doit pas cacher la forêt. Les mesures de protection légales de la vie privée qui contraignent le travail de la NSA ne protègent que les citoyens américains. Malgré les nombreuses failles qui ont été observées, certaines mesures d'atténuation existent pour les Américains auxquelles les « autres » n'ont pas droit. Marieke de Goede rappelle :

> The limits to the privacy debate … are partly related to the specific American legal definition of privacy that applies only to citizens, not to foreigners. But the limits to privacy are more profoundly revealed through the notion that 20 million database queries per month can be deemed just and legitimate, with breaches defined narrowly as queries that are imprecise or too broad. This raises questions concerning the notions of suspicion and data analysis deployed within contemporary data-led security, and their relation to existing (legal) codifications of privacy (de Goede 2014, 100-101).

Les discussions autour du cadre légal américain ne doivent pas masquer la signification de la surveillance américaine pour le reste de la planète qui n'est pas protégée le 4e amendement de la constitution américaine. Il est vrai qu'en principe certaines protections et autres recours sont offerts par la constitution américaine aux étrangers. En outre, les citoyens des États partenaires du Five Eyes, une entente de coopération au niveau du renseignement entre les cinq grands pays anglo-saxons — Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni — sont par convention protégés de la surveillance américaine. « The NSA does NOT target its 2nd party partners [les États du Five Eyes], nor request that 2nd parties do anything that is inherently illegal for NSA to do, » précisant du même souffle que « [w]e can, and often do, target the signals of most 3rd party foreign partners, » est-il écrit dans un document rendu public par Der Spiegel (Poitras et coll. 2013). Cependant, les trois pages consacrées à l'analyse du traitement des étrangers dans le rapport du PCLOB, sur les 191 pages qui le composent, en disent long sur la place secondaire des étrangers dans les considérations légales du gouvernement américain. Pourtant, octroyer des niveaux de protection légale distincts pour les citoyens et les étrangers ne va pas de soi. Susan Landau rappelle, par exemple, que la Cour européenne des droits de l'homme « recognizes the right of liberty and security for each person regardless of citizenship » (Landau 2013, 58), d'autant plus que le droit à la vie privée a été reconnu par l'ONU. La portée et l'efficacité de la surveillance de

la NSA combinées au fractionnement des protections légales associées au droit à la vie privée en près de 200 territoires nationaux et citoyennetés nationales obligent à remettre en question les termes du débat actuel qui oppose la surveillance à la vie privée. Les pratiques du renseignement américain ne garantissent ni liberté ni sécurité pour des milliards de non-Américains.

4.5 Spatialité, matérialité (bis) : exploitation mondiale des infrastructures de communications et la limite de la protection légale du droit à la vie privée

En visualisant la mobilité numérique, IXmaps promeut, afin d'accroître la confidentialité des données et la protection de la vie privée, la souveraineté Internet canadienne. Le projet rend visible la fragilité des protections légales contre la surveillance dans le contexte de l'imprévisibilité de la circulation des données et de la préséance des États-Unis dans l'économie numérique. En d'autres mots, le projet montre l'étroite relation entre les infrastructures matérielles et l'architecture juridique de la surveillance. Toutefois, à partir du moment où l'enjeu ne porte plus uniquement sur les communications nationales, la souveraineté du réseau national perd de sa pertinence. L'utopie associée à Internet est précisément la possibilité de communiquer avec l'ensemble du monde, au-delà des frontières nationales. La critique d'IXmaps quant à la disparition des protections légales du droit à la vie privée dépasse alors la question du routage boomerang et devient pertinente pour l'ensemble des communications mondiales.

Compte tenu de la logique économique de la mobilité Internet, toutes les communications, peu importe leur origine et leur destination, risquent de passer par les États-Unis, sans parler des risques liés aux services d'infonuagique offerts par les géants américains tels que Google, Apple, Amazon et Microsoft qui sont sous juridiction américaine et dont les serveurs sont dispersés à travers le monde et encouragent la mobilité internationale des données. Comme le remarquent Ellen Nakashima et Ashkan Soltani du Washington Post :

> today, emails, calls and other communications cross U.S. borders and are often stored beyond them. Companies like Google and Yahoo have "mirror" servers around the world that hold customers' data. That means Americans' data are often stored both in the United States and abroad simultaneously, subject to two different legal and oversight regimes. Surveillance on U.S. soil requires court permission and an individual warrant for each target. Surveillance abroad requires a warrant for U.S. persons, but if collection is coming from a data center overseas, large volumes of Americans' communications may be picked up as "incidental" to collection on a foreign target (Nakashima & Soltani 2014).

Si la situation est inquiétante pour les Américains, elle l'est d'autant plus pour les étrangers qui ne bénéficient pas des mêmes protections légales. L'imprévisibilité de la route des communications Internet, la capacité de transit des infrastructures américaines et la participation des entreprises américaines aux efforts de surveillance de la NSA ont pour conséquence qu'une communication, qu'elle soit ou non destinée aux États-Unis, puisse très bien venir à transiter par les infrastructures du pays ou être enregistrée sur un des serveurs hébergés dans le pays.

La NSA a compris et exploite le potentiel offert par la position stratégique des États-Unis dans les infrastructures Internet. La NSA écrit ainsi dans le document de présentation du programme PRISM rendu public par Snowden : « Much of the world's communications flow through the U.S. A target's phone call, e-mail or chat will take **cheapest** path, **not the physically most direct** path — you can't always predict the path. Your target's communications could easily be flowing into and through the U.S. » (The Guardian 2013b, 2). Cette exploitation est rendue possible par la participation des entreprises privées. Selon un document produit par le Office of General Counsel de la NSA résumant le FAA et rendu public par Snowden,

> [o]ne of the primary purposes in enacting the FAA was *the creation of a new way for the US Government to compel providers of electronic communications services to assist the Government* in acquiring foreign intelligence information concerning non-US persons located outside the United States (Office of General Counsel 2008, 3; je souligne).

Des différents programmes, ce sont les entreprises privées qui fournissent la part du lion des données collectées par la NSA. 80 % de toutes les données de la NSA proviennent des partenariats avec le privé (2015, 5). Menés par le département des Special Sources Operations (SSO), le « crown jewel » de la NSA selon les mots de Snowden (Snowden cité par Greenwald 2014, 102), les partenariats avec les concepteurs de matériel informatique, les opérateurs et fournisseurs de service sont essentiel à la poursuite des activités de surveillance de la NSA. La NSA se targue d'avoir établi des « alliances with over 80 Major Global Corporations supporting both missions [defending networks in the US and monitoring networks abroad] » (NSA Strategic Partnerships cité par Greenwald 2014, 102; Poitras et coll. 2013). AT&T, Verizon, Qwest, HP, Qualcomm, IBM, Oracle, Intel, Cisco, Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple ont toutes été identifiées dans divers documents de Snowden (Greenwald 2014, 102; The Guardian 2013b, 6). L'agence a ainsi consacré un budget de près de 480 et 380 millions de dollars américains en 2010 et 2011 respectivement, quoiqu'il soit difficile de savoir quelle

somme a été directement versée aux entreprises (2015, 24). En parallèle aux incitatifs pécuniaires, la NSA s'en remet également aux incitatifs légaux pour obtenir la coopération des compagnies. Le gouvernement négocie notamment avec les opérateurs de réseaux étrangers désireux d'exploiter un réseau aux États-Unis des procédures d'accès aux données en échange de permis d'exploitation (Timberg & Nakashima 2013).

La NSA a ainsi conclu une série de partenariats avec les grands opérateurs et fournisseurs de services Internet, dont AT&T (programmes FAIRVIEW et BLARNEY) et Verizon (programme STORMBREW) (Angwin et coll. 2015; Greenwald 2014, 103; 2015), afin d'établir, à même leurs infrastructures, des centres d'interception permettant d'accéder aux données qui y circulent. Déjà au milieu des années 2000, Mark Klein, un ancien employé d'AT&T, révélait que la compagnie avait installé, dans leurs bureaux du 611 rue Folsom à San Francisco, un diviseur permettant de copier vers les serveurs de la NSA les données circulant sur leurs infrastructures (Kravets 2013; Angwin et coll. 2015). La NSA aurait déployé des technologies similaires dans plusieurs autres villes américaines. Selon les données répertoriées par IXmaps, qui se base notamment sur les documents de Snowden et d'autres informations divulguées par Jacob Appelbaum, la NSA serait présente dans près de 20 villes américaines (2012b; IXmaps 2017b; IXmaps 2017a).

Avec de telles infrastructures, la NSA est en mesure d'intercepter des communications qui ne sont pas destinées aux États-Unis ni par la nationalité de l'organisation ni par la localisation des serveurs hébergeant le site visité. Ainsi, IXmaps permet de voir que la NSA interceptera une communication de Montréal vers le site Internet de la BBC hébergé à Londres (IXmaps 2016, Traceroute 144914). Similairement, une communication de Montréal vers l'Amérique du Sud voyagera presque inévitablement à travers les milliers de kilomètres de fibre optique qui traversent les États-Unis, passant, comme dans le cas de la connexion au site Internet de l'Universidade de São Paulo (usp.br), à travers les centres d'interception de la NSA en Floride.

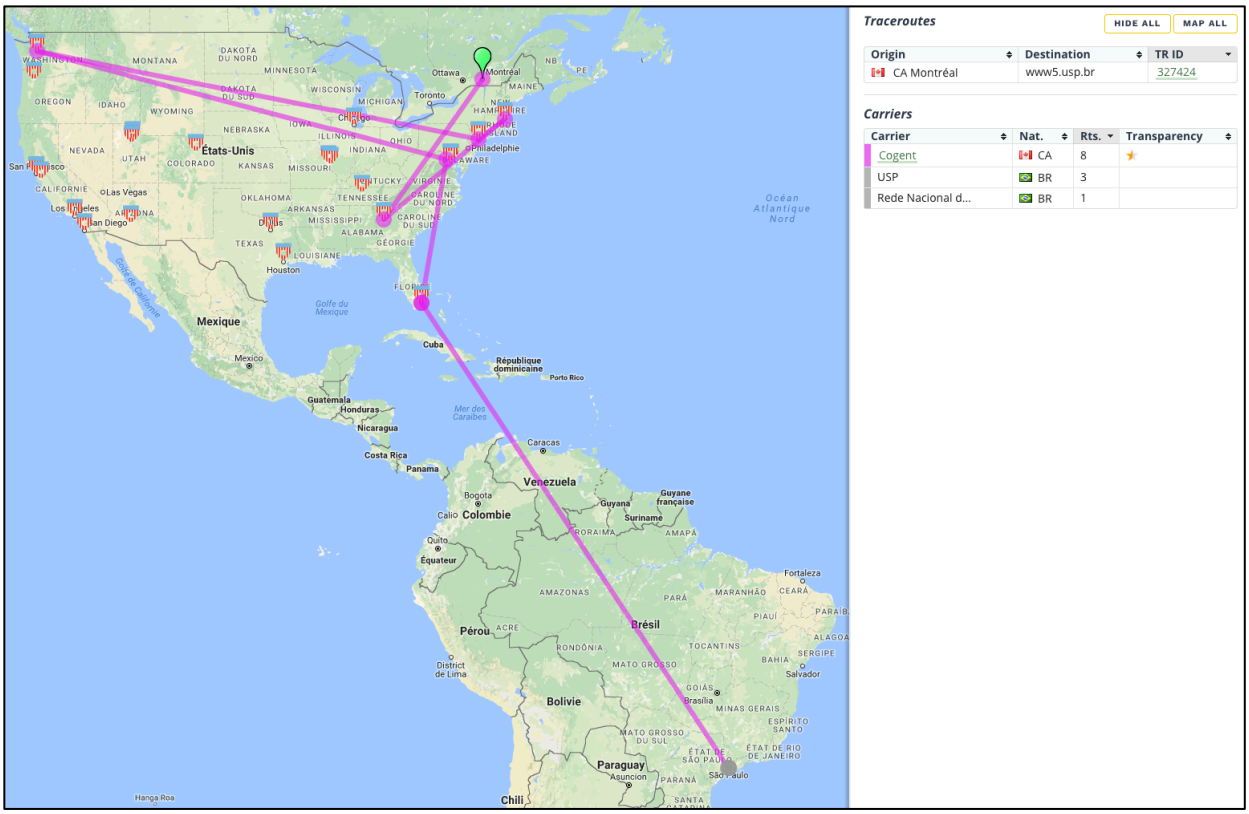


Figure 4.8 : De Montréal vers le monde
(source : IXmaps 2016, Traceroute 327424)

Le déploiement des infrastructures de communication mondiale, la répartition des points d'échange Internet et la distribution des câbles sous-marins de fibre optique, vecteurs de la centralisation d'Internet, forcent des millions de communications à transiter par les États-Unis. Si les routes que chaque communication emprunte sont difficilement prévisibles, elles ne sont pas pour autant aléatoires. Par exemple, trois régions accueillent la quasi-totalité des points d'atterrissage[25] des câbles sous-marins de fibre optique sur la côte est de l'Amérique du Nord (TeleGeography 2017b). Deux sont situées la grande région de New York, à Long Island et le long de la côte du New Jersey, d'où partent la majorité des câbles à destination de l'Europe. Une communication des Amériques vers l'Europe passera probablement par la région new-yorkaise, à travers un des grands points d'échange Internet de Manhattan comme le 60 rue Hudson (Mendelsohn 2011), avant de traverser l'Atlantique à travers les câbles sous-marins jusqu'à Telehouse à Londres avant de rejoindre le continent. La route qui relie New York et Londres est la plus importante route intercontinentale de communication au monde, la majeure partie de ces

[25] « landing points »

communications transitant par le 60 rue Hudson et Telehouse North sis de chaque côté de l'Atlantique (Blum 2012, 202). La région de Miami, la plus importante plaque tournante en Amérique du Nord devant New York et Londres, est un autre point d'atterrissage important pour les câbles sous-marins de fibre optique, connectant cette fois l'Amérique du Nord au reste des Amériques (TeleGeography 2017a). Ces trois régions et les principaux points d'échange Internet par lesquels transitent les communications nord-américaines et mondiales créent des goulots d'étranglement[26] qui facilitent la surveillance de la NSA. Compte tenu du volume de données circulant dans les grands points de passage Internet américains, IXmaps avance que « [l]ocating interception facilities in as few as 18 cities is sufficient to capture nearly 100% of internet communications originating within or passing through the U.S. » (IXmaps 2017b).

IXmaps situe spatialement et géographiquement cette surveillance avec les yeux du réseau, en projetant sur un planisphère Google les adresses IP que traversent les communications. Trevor Paglen poursuit une entreprise similaire en observant les composantes matérielles de la surveillance. Ainsi, il capture dans une série de photos des câbles sous-marins reposant sur le fond marin au large de Miami et les plages servant de point d'atterrissage des câbles sous-marins. Derrière ces scènes familières reposent des infrastructures essentielles de la surveillance. « On the surface these photographs appear as straightforward images of the sea, while in fact, Paglen points to the vast infrastructure of the surveillance state » (Altman Siegel 2015). « A scene at a beach is a scene of mass surveillance, » ajoute l'artiste (The Creators Project 2016).

[26] « choke point »

Figure 4.9 : Capturer les infrastructures de surveillance
Bahamas Internet Cable System (BICS-1), NSA/GCHQ-Tapped Undersea Cable, Atlantic Ocean, 2015 (source : Packard 2015); NSA-Tapped Fiber Optic Cable Landing Site, Keawaula, Hawaii, United States, 2016 (source : Paglen 2016)

Comme ces photos occupant les marges de Citizen Ex, Paglen rappelle qu'il est impossible de comprendre Internet sans s'attarder à sa matérialité et à son déploiement dans l'espace. L'artiste nous transporte ainsi sur les plages de New York, Miami, Los Angeles et Hawaï, mais aussi au large, au fond des mers et au-delà du territoire américain. En jouxtant aux photos de plages et de câbles des photos des stations d'interception de la NSA dans la région de Frankfort en Allemagne et en Cornouailles au Royaume-Uni, Paglen montre que la surveillance des communications mondiales ne se limite pas au territoire américain. La présence de la NSA est mondiale. L'agence entretient des collaborations avec des partenaires privés et publics, essentiellement d'autres agences de renseignement, avec lesquels elle poursuit son entreprise de surveillance des communications mondiales.

Figure 4.10 : Capturer les infrastructures de surveillance, bis
NSA Surveillance Base, Egelsbach, Germany, 2015 (source : Paglen 2015); National Security Agency Surveillance Base, Bude, Cornwall, UK, 2014 (source : Paglen 2014b)

Le choix d'Egelsbach et Bude n'est certainement pas un hasard. Située à proximité de Frankfort, Egelsbach rappelle l'importance de la présence américaine en Allemagne et des opérations de surveillance menées à partir du territoire allemand. Certes, le rôle spécifique d'Egelsbach dans les opérations de la NSA demeure nébuleux, contrairement à ceux du Consulat général des États-Unis à Frankfort, de l'European Technical Center de Wiesbaden ou de l'European Center for Cryptology de Griesheim qui, selon les informations révélées par Snowden et publiées dans le Spiegel, ont notamment servi à la surveillance de la chancelière allemande Angela Merkel, de support aux opérations de drones et à l'interception des communications transitant par l'Allemagne. Egelsbach rappelle néanmoins l'ombre américaine en Allemagne, la NSA à elle seule y possédant plus d'une douzaine de points d'interception (Spiegel 2014). « According to insiders familiar with the German portion of the NSA program, the main interest is in a number of large Internet hubs in western and southern Germany, » écrivent Laura Poitras et coll. dans le Spiegel.

> The secret NSA documents show that Frankfurt plays an important role in the global network, and the city is named as a central base in the country. From there, the NSA has access to Internet connections that run not only to countries like Mali or Syria, but also to ones in Eastern Europe (Poitras et coll. 2013).

Frankfort accueille le Deutscher Commercial Internet Exchange (DE-CIX), le plus important point d'échange Internet au monde en termes du volume de bande passante Internet, connectant plus de 700 réseaux en un seul espace physique (Blum 2012, 112-113; DE-CIX 2017). C'est sans grande surprise que le site attire l'attention de la NSA qui, une fois à l'extérieur des États-Unis, n'est pas tenue par les contraintes légales du FAA, mais agit avec la liberté que lui confère l'ordre

exécutif 12333. Mais Frankfort attire aussi l'attention du BND, l'agence de renseignement allemande.

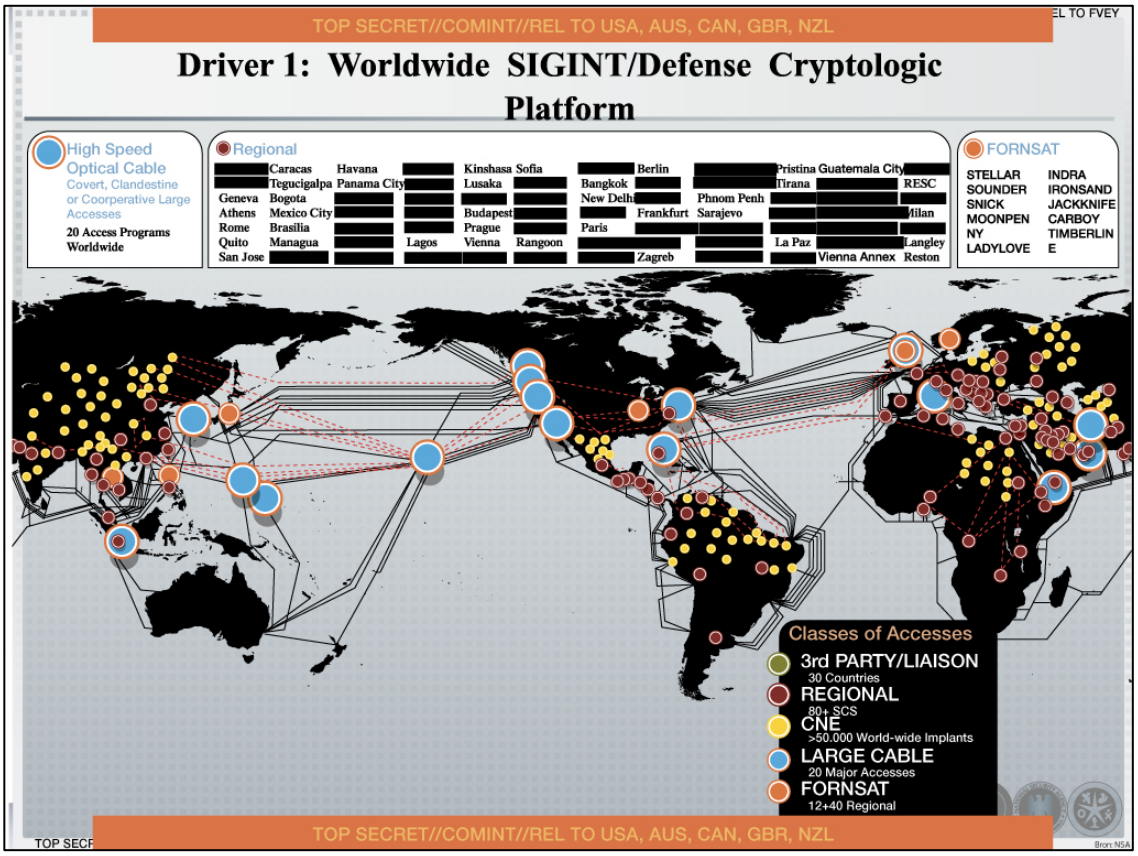


Figure 4.11 : Présence mondiale de la NSA
Notons les 30 pays tiers et les États partenaires du Five Eyes qui ne sont pas représentés (source : NSA 2012a)

La surveillance est une entreprise collaborative. Malgré la force centripète qu'exercent les États-Unis sur les communications mondiales, Internet n'est pas un complot américain. Sa géographie dépasse les États-Unis, et la surveillance des communications mondiales n'est pas l'apanage de la NSA. La NSA avait en 2012 des partenariats avec 30 pays tiers (« 3rd Party/Liaison »), dénomination qui exclut les membres du Five Eyes anglo-saxon — Australie, Canada, États-Unis, Nouvelle-Zélande, Royaume-Uni (voir aussi Greenwald 2014, 123). Cette collaboration permet de contourner certaines contraintes légales. Même si la NSA nie demander l'aide de ses partenaires pour contourner ses obligations constitutionnelles telles que la surveillance d'Américains, Zigmunt Bauman et coll. proposaient le contraire.

> The bulk collection of data and the visualization through networks makes it impossible to be certain about the difference between nationals and foreigners. Legality requirements threaten the functioning of the system and so they presume that the law must adjust, not the

> system. To avoid this "complication," transnational networking between different services has enabled a blurring of the boundaries of domestic and foreign jurisdiction. It seems that the different services in charge of their own national security, working through the gathering and exchange of information, ask other security services to perform some of their tasks, bypassing limitations on foreign intelligence by using "a citizen privacy shopping" to exchange surveillance of their own citizen with another service. In this way, what is national and what is foreign becomes mostly irrelevant for transnationally organized operations (Bauman et coll. 2014, 125).

Une lettre du 21 février 2011 écrite par le directeur adjoint de l'Intelligence Defence Signals Directorate de l'Australie et adressée à la NSA reproduite dans le livre *No Place to Hide* de Glenn Greenwald semble confirmer cette interprétation. Il est écrit : « [w]e would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities — in particular Australians involved with AQAP » (cité par Greenwald 2014, 122). La lettre semble effectivement demander à la NSA de surveiller des citoyens australiens jugés suspects.

La collaboration internationale permet également de profiter des accès privilégiés des autres partenaires. La BND participe à la surveillance de DE-CIX à Frankfort. La DGSE française a installé des intercepteurs à Djibouti pour surveiller les nombreux câbles sous-marins connectant l'Asie et l'Afrique. Djibouti est le point d'atterrissage de plusieurs câbles sous-marins et plusieurs autres passent au large du pays par le détroit de Bab-el-Manded. La FRA suédoise surveille les communications entre les pays baltes et la Russie (Bauman et coll. 2014, 122). Le Centre de la sécurité des communications canadien mène un programme de surveillance dirigé vers les autorités brésiliennes en plus de faire profiter la NSA de ses « unique geographic access to areas unavailable to the U.S. » (Greenwald 2014, 121).

Le plus important partenaire international de la NSA demeure toutefois le GCHQ britannique. Avec la transformation des infrastructures de communication mondiale, soutenue à 99 % par le réseau de fibres optiques (Reuters 2013) et le rôle de plaque tournante de la Grande-Bretagne, c'est désormais à partir de sondes Internet installées sur les câbles, plutôt que par la surveillance des tours microonde et des satellites de communication, que la majorité de la surveillance britannique est menée (MacAskill et coll. 2013). À ce titre, GCHQ mène notamment le programme TEMPORA décrit par Snowden comme « the largest programme of suspicionless surveillance in human history » (cité par MacAskill et coll. 2013). TEMPORA est un programme de surveillance en amont, « attaching intercept probes to transatlantic fibre-optic cables where they

land on British shores carrying data to western Europe from telephone exchanges and internet servers in north America » (MacAskill et coll. 2013). Le programme génère, selon un document de la NSA, 40 milliards de données par jour (NSA 2012d, 2).

À l'instar de la NSA, GCHQ a conclu des partenariats avec des entreprises privées. Au moins sept opérateurs de réseau assurent l'accès aux données circulant sur leurs infrastructures. Publiant des documents de Snowden, le quotidien allemand Süddeutsche Zeitung rapportait des détails sur une de ces collaborations. Identifiée sous le nom GERONTIC, GCHQ aurait accès aux câbles sous-marins et autres infrastructures de Cable & Wireless — racheté par Vodafone en 2012. Un document daté de juillet 2009 précisait que ce partenariat garantissait l'accès à 29 des 63 câbles interceptés par GCHQ et fournissait 70 % de toutes les données collectées par l'agence (Obermaier et coll. 2014). Toutefois, contrairement à la surveillance menée par la NSA en vertu de l'article 702 du FAA, GCHQ ne semble pas déléguer aux opérateurs de réseaux la tâche de filtrer les communications. L'architecture légale britannique est moins contraignante que celle qui encadre les pratiques de la NSA. Selon un document de la NSA résumant le programme, TEMPORA fonctionne plutôt comme une mémoire tampon du contenu Internet circulant par le biais des câbles de fibre optique permettant d'emmagasiner pour une période de 3 jours l'ensemble du contenu (contenu web, courriels, discussions Internet [chat], réseaux privés virtuels [VPN], voix sur IP [VoIP]), et pour une période de 30 jours les métadonnées liées. Pendant cette période, les analystes britanniques et américains, puisque le programme est partagé avec ces derniers, ont accès aux informations qu'ils peuvent ensuite transférer dans des bases de données à plus long terme si l'information est jugée pertinente (NSA 2012d; GCHQ 2012).

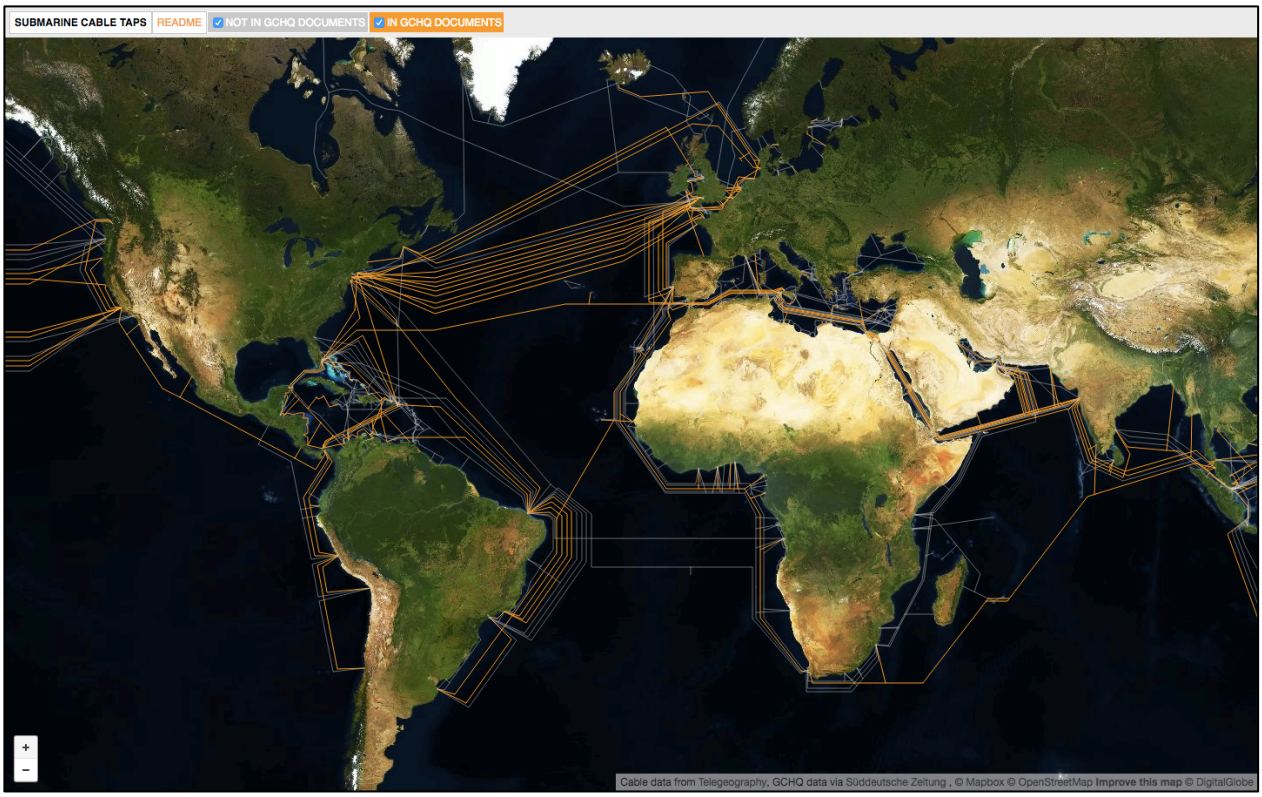


Figure 4.12 : Submarine Cable Taps d'Ingrid Burrington
une visualisation des 63 câbles sous-marins interceptés par GCHQ (en orange) (source : Burrington 2014a)

La base de Cheltenham à Bude, en Cornouailles, photographiée par Paglen, est un symbole contemporain de la coopération entre les deux pays. Construite à proximité de points d'atterrissage de plusieurs câbles sous-marins, Cheltenham a été désignée pour opérer le programme TEMPORA (MacAskill et coll. 2013). Située à l'extrême pointe ouest de l'île britannique, la Cornouaille est depuis le début un point de passage clé pour les infrastructures de télécommunication transatlantiques (Blum 2012, 202-204). Le village de Bude est le lieu d'émergence du premier câble sous-marin de fibre optique, le TAT-8, reliant les États-Unis à l'Europe, en passant par la Grande-Bretagne, désormais remplacé par le TAT-14, propriété des plus grandes entreprises de télécommunication mondiale (BT, Verizon, Deutsche Telekom, Orange, Sprint, AT&T, Belgacom, etc.). Par ces connexions avec l'Amérique du Nord, mais aussi l'Afrique et l'Asie, Bude, et la Cornouaille est un lieu névralgique de la communication mondiale et de la surveillance de sécurité (TeleGeography 2017b). Grâce à la présence des infrastructures mondiales de communication et des ententes signées par GCHQ avec les entreprises propriétaires, Bude rejoint Menwith Hill, base d'opération du célèbre programme ECHELON. Paglen n'a pas pris sa photographie au hasard. En plus de symboliser la coopération anglo-américaine, la base de Cheltenham est un symbole de

l'enchevêtrement entre les pratiques de surveillance des agences de renseignement occidentales, les infrastructures internationales de la communication mondiale, la parcellisation des architectures judiciaires encadrant la surveillance et assurant la protection légale du droit à la vie privée. La surveillance mondiale des communications est le résultat précaire de ces rencontres.

4.6 Conclusion : Une surveillance mondialisée, des citoyens mis à nu

Paglen vise probablement juste lorsqu'il dit que « the Internet has been turned into the greatest instrument of mass surveillance in the history of mankind » (The Creators Project 2016). Le jeu des superlatifs ne fait qu'aider à donner un sens à l'ensemble des efforts déployés pour intercepter les communications mondiales. En même temps, restreindre l'analyse à la NSA, de la même manière que restreindre la question du droit à la vie privée aux citoyens américains, est trompeur. La surveillance des données de masse est devenue une entreprise mondiale, du moins occidentale. À ce titre, représenter le réseau mondial de câbles sous-marin avec le style renaissance comme l'a fait la firme de consultant TeleGeography, dont les cartes interactives font autorité, est révélateur.

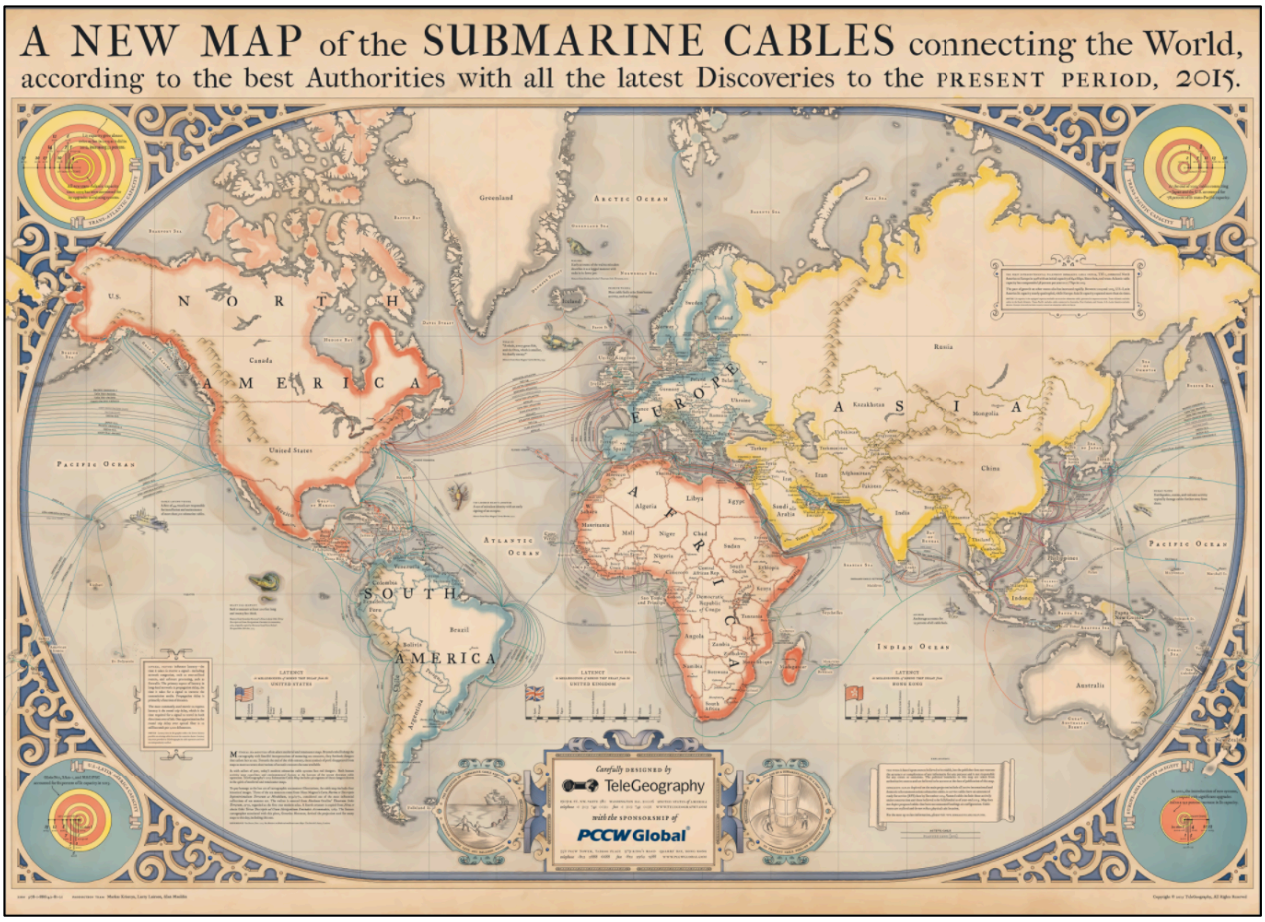


Figure 4.13 : Le contrôle des routes de communication et la constitution d'empires (source : TeleGeography 2017c)

Réalisée en hommage au cartographe Gerardus Mercator, la version 2015 de la carte de TeleGeography reproduit l'esthétique de la période de la renaissance européenne et, avec celui-ci, elle reproduit le bagage politique, indissociable de la production du monde sensible de l'époque des Découvertes et de la naissance des Empires européens. La carte rappelle les dynamiques de pouvoir associées au contrôle des lignes de communication. Conçue en 1569, la projection Mercator visait à faciliter la navigation pour les flottes européennes. En ce sens, elle était un instrument de pouvoir. En situant l'Europe au centre du monde et les deux tiers des parties submergées dans l'hémisphère nord, la carte relègue visuellement le reste du monde au second rang. Mais cette relégation n'est pas que visuelle. Elle ne cherche pas à assurer une reproduction juste du globe, mais à permettre aux empires maritimes européens naissants d'étendre leur emprise sur le reste du monde (Campbell 2013, 224-225). Aujourd'hui, la carte rappelle, involontairement, que le contrôle des routes de communications Internet constitue toujours un élément-clé de la

constitution d'empires, primant les intérêts des États occidentaux sur ceux des autres (Edwards 2015).

Penser la surveillance comme une entreprise occidentale, voire mondiale, ne signifie pas pour autant qu'elle soit singulière ni sans accrocs. D'une part, les entreprises collaborant avec la NSA et ses consœurs conservent un contrôle sur les données qu'elles leur transmettent. En vertu de l'article 702 du FAA, ce sont elles qui manipulent les données et les transmettent à la NSA. Comme la NSA le rappelle dans un document explicatif du portfolio d'entreprise des SSO,

> Because of partner relations and legal authorities, SSO Corporate sites are often controlled by the partner, who filters the communications before sending to NSA. Because we go through partners and do not typically have direct access to the systems, it can take some time for OCTAVE/UTT/Cadence tasking to be updated at site (anywhere from weekly for some BLARNEY accesses to a few hours for STORMBREW) (2015, 5).

La NSA n'est pas le seul maître à bord. Le gouvernement américain a réagi fortement aux intentions de fournisseurs de service de chiffrer leurs données (Nakashima 2014), rendant plus difficile la lecture de données collectées en amont et par le programme d'intrusion sur les réseaux privés de Yahoo ! et Google, quoique cela n'aurait pas nécessairement d'effet sur le programme PRISM. De la même façon, les partenariats entre les agences de renseignement ne sont pas toujours sans vague. Bauman et coll. remarquent par exemple que les révélations Snowden ont refroidi la coopération interagence.

> Trust between the services—which was limited, but nevertheless existed in the name of the struggle against terrorism—largely disappeared when it became clear that spying on politicians, industrial espionage, data mining of the personal information of large populations in order to profile the evolution of consumer choices, and even political opinions about future elections, have been used by NSA analysts. This included spying on the populations of the countries with which they were allied and with whom they collaborated in the "five eyes plus" network. There has thus been a realization on the part of some partners of the NSA that collaboration in support of the national security of the United States has compromised their own national security and interests, and with their own "involuntary" complicity (Bauman et coll. 2014, 127).

Si les agences de renseignement principalement occidentales ont ensemble pu créer un bassin commun d'informations — et contourner les législations nationales en demandant à un partenaire de surveiller certains citoyens (Greenwald 2014, 122), cet échange d'informations ne constitue pas un accès automatique ou sans filtre, et encore moins un accès également partagé, la NSA conservant la main haute sur les opérations. La taille de la NSA y est pour quelque chose. La

NSA emploie, incluant les entrepreneurs privés, de 12 à 16 fois plus d'employés que les autres agences de renseignement et se voit remettre un budget 6 fois plus élevé que celui de GCHQ et jusqu'à 12 fois ceux des consœurs française et allemande (Bauman et coll. 2014, 126-127). Il faut néanmoins reconnaître que malgré le pouvoir d'attraction de la NSA, la surveillance mondiale des données, portée par la NSA, n'est pas un système hiérarchique structuré à la Big Brother. Dans son photoreportage sur les infrastructures matérielles du nuage Internet, l'artiste Ingrid Burrington conclut :

> Mass surveillance in the United States is a complex public-private partnership, and the data-industrial complex is but one of its sprawling pieces. Beneath headlines about the spooks of the surveillance state are normal, nonspooky humans in normal, nonspooky places—engineers working at colocation centers used by defense contractors, county economic development offices looking to expand the local tax base, real estate companies looking to get into a new market, energy companies that welcome the profits born of an industry that uses more electricity than some small nations (Burrington 2014b).

La surveillance mondialisée n'est ni unique ni issue d'un régime pouvant réécrire le droit et l'Histoire à sa guise. Cependant, elle n'est pas sans conséquence, rendant pratiquement caduc le système de protection légale assurant le droit à la vie privée des individus à travers le monde. Comme le montre IXmaps, l'imprévisibilité des routes Internet et la portée de l'entreprise mondiale de surveillance des données rendent difficilement imaginable qu'une communication puisse transiter sans être interceptée quelque part en chemin par la NSA ou par une autre agence de renseignement.

Similairement, Citizen Ex rappelle la limite du droit national et de la citoyenneté dans le contexte des communications mondiales. La détermination du statut de citoyenneté de la personne par le renseignement américain, et par le fait même de l'autorisation de surveillance, est emblématique de l'écart existant entre l'apparente universalité d'Internet et le fractionnement international de son fonctionnement. Malgré les représentations d'Internet, du réseau et du nuage, les structures liées au système d'État, comme les frontières et la citoyenneté, se transforment, mais demeurent bien vivantes. Pour Tung-Hui Hu, le monde numérique ne remplace pas les anciennes structures du pouvoir étatique. Au contraire, elle s'y greffe en y intégrant des formes plus souples de pouvoir.

> Rather than considering sovereign power a historical exception or aberration within a whole sale shift to the systems of control, I suggest that it has mutated and been given new life inside the cloud … the cloud grafts control onto an older structure of sovereign power, much

> as fiber-optic networks are layered or grafted onto older networks. I term this new hybrid form the "sovereignty of data" (Hu 2015, xvi).

Certes, en approfondissant les procédures de surveillance, Citizen Ex apparaît imprécis. La détermination du statut de citoyenneté ne s'exprime pas en pourcentage et dépend de beaucoup plus de variables que les sites Internet visités. Bridle est néanmoins juste lorsqu'il soulève que la distinction entre nationaux et étrangers sur laquelle se fonde la surveillance et le droit à la vie privée n'est plus si nette. Le faible taux d'erreur des analystes de la NSA ne doit pas masquer la transformation qui accompagne la notion de citoyenneté. La citoyenneté algorithmique est une citoyenneté mesurée, flexible et temporaire. La citoyenneté n'est plus définitive. En ce sens, le travail esthétique de Bridle ne doit pas être pris au pied de la lettre. Le projet est, pour reprendre les mots de l'artiste, « just one illustration of how this [algorithmic citizenship] might be done » (Bridle 2015e). Mais en se faisant, Bridle s'aventure sur le même terrain que la NSA et des dispositifs de sécurité américain et occidentaux : celui de l'incertain et de la spéculation. Or la transformation de cette incertitude en contenu opératoire est précisément ce qui est important, l'espace du politique. Une source du Guardian expliquait la rationalité de la surveillance britannique :

> Essentially, we have a process that allows us to select a small number of needles in a haystack. We are not looking at every piece of straw. There are certain triggers that allow you to discard or not examine a lot of data so you are just looking at needles. If you had the impression we are reading millions of emails, we are not. There is no intention in this whole programme to use it for looking at UK domestic traffic — British people talking to each other (MacAskill et coll. 2013).

Même si les agences de renseignement s'intéressent uniquement à quelques aiguilles, leur accès à la botte de foin, l'impossibilité de savoir quelles aiguilles sont retenues et la façon dont celles-ci sont analysées et interprétées montrent les limites des protections légales du droit à la vie privée attribuées sur la base d'une citoyenneté fixe et permanente dans un univers de plus en plus marqué par l'ambiguïté et la fluidité. Citizen Ex permet non seulement de voir, mais est une œuvre spéculative qui invite à penser comme le réseau. Elle imagine comment les données de masses peuvent devenir opératoires à des fins de sécurité.

5 Le surveillant émancipé : opérationnalisation des données et spéculation sécuritaire dans l'âge d'or de la surveillance numérique

Ces histoires de frontières à traverser et de distribution des rôles à brouiller rencontrent en effet l'actualité de l'art contemporain où toutes les compétences artistiques spécifiques tendent à sortir de leur domaine propre et à échanger leurs places et leurs pouvoirs. … [Il faut] concevoir [ce mélange des genres] comme une nouvelle scène de l'égalité où des performances hétérogènes se traduisent les unes dans les autres. Car dans toutes ces performances il s'agit de lier ce que l'on sait avec ce que l'on ignore, d'être à la fois des performers déployant leurs compétences et des spectateurs observant ce que ces compétences peuvent produire dans un contexte nouveau, auprès d'autres spectateurs. Les artistes, comme les chercheurs, construisent la scène où la manifestation et l'effet de leurs compétences sont exposés, rendus incertains dans les termes de l'idiome nouveau qui traduit une nouvelle aventure intellectuelle. L'effet de l'idiome ne peut être anticipé. Il demande des spectateurs qui jouent le rôle d'interprètes actifs, qui élaborent leur propre traduction pour s'approprier l'« histoire » et en faire leur propre histoire. Une communauté émancipée est une communauté de conteurs et de traducteurs.
Jacques Rancière[1]

Comment transforme-t-on des données numériques en savoir permettant de préempter un attentat terroriste ? Les infrastructures matérielles et légales des télécommunications mondiales font en sorte de miner les protections légales du droit à la vie privée consenties par les États à leurs citoyens et qui, en principe, circonscrivent les pratiques de surveillance du renseignement occidental. Ces infrastructures facilitent l'accès physique aux données lorsque les agences de renseignement réussissent à contrôler certains points de circulation cruciaux, notamment les points d'échange Internet et les points d'atterrissage des câbles sous-marins de fibre optique. Le contrôle de ces infrastructures-clés sur le territoire américain par la NSA, mais aussi à travers le monde par l'entremise de ses opérations extérieures ou par ses collaborations avec des pays alliés, lui assure un accès aux données mondiales qui, s'il n'est pas illimité, n'en demeure pas moins colossal. L'équivalent d'une Bibliothèque du Congrès américain est ingéré par la NSA toutes les 14,4

[1] (Rancière 2008, 28-29)

secondes selon un document datant de 2006, sans compter les autres millions de données filtrées pour identifier les sélecteurs et non collectées qui ne sont donc pas « surveillées » (Gellman 2013).

L'accès à toutes ces données génère ses propres enjeux. D'abord, ces masses de données doivent être stockées dans des bases de données. Cela demande une production toujours croissante d'espace de stockage, d'où la construction, au coût de deux milliards de dollars, du Utah Data Center à Bluffdale, en Utah, dont la superficie est évaluée à un plus de 90 000 mètres carrés et la capacité de stockage est estimée en yottaoctet (10^{24} octets) (Bamford 2012). À ce défi matériel s'ajoute celui du catalogage des données qui doit être suffisamment précis et cohérent pour permettre aux analystes de les récupérer lors de leurs recherches. Divers programmes et filtres sont ainsi mis en œuvre pour écarter les données sans valeur stratégiques qu'il s'agisse des téléchargements de pair à pair qui engorgent les bases de données, des carnets d'adresses sans propriétaire qui ne permettent pas de reconstruire avec précision les réseaux de suspects ou encore la pornographie dans les vidéos Webcam (Gellman & Soltani 2013a; Ackerman & Ball 2014; NSA 2012d).

Plus généralement, le renseignement doit réussir à transformer des données diversifiées provenant de courriels, d'appels téléphoniques, de l'utilisation des réseaux sociaux, de navigation Internet, de transactions numériques, etc. en savoir de sécurité. Les données doivent être filtrées, notamment pour repérer les sélecteurs. Elles doivent également être filtrées et catégorisées pour séparer les données ne fournissant pas d'informations valables de celles devant attirer l'attention des analystes. Ces données filtrées par le dispositif de sécurité sont jugées suffisamment pertinentes pour justifier le déploiement et l'extension des technologies et pratiques de surveillance et pour justifier des interventions de sécurité. En réponse aux révélations Snowden, le directeur de la NSA du moment, le général Keith Alexander, a ainsi défendu les programmes de surveillance sur la base que les informations obtenues auraient servi à prévenir 54 complots terroristes, quoique ce nombre ait été contesté (Landau 2013, 59-60). Les informations collectées par les opérations de la NSA servent également de support aux opérations militaires américaines, notamment aux missions d'assassinat ciblé exécutées par les drones (Currier & Maass 2015). Sans grande ambiguïté, le général Michael Hayden, ancien directeur de la CIA et de la NSA, déclarait pendant un symposium organisé par la John Hopkins University : « [w]e kill people based on metadata » (Naughton 2016). Aux yeux des acteurs de la sécurité, la pertinence des données de masse pour le savoir et les pratiques de sécurité ne fait pas de doute.

Le processus de filtrage et de sélection des données suggère toutefois un moment de passage entre l'existence de données numériques et leur transformation en savoir de sécurité qui invite à approfondir la signification sociale des données dans cette époque que la NSA qualifie de « golden age of SIGINT » (Risen & Poitras 2013). Comme le relèvent Louise Amoore et Marieke de Goede, cette perception positive des données de masse par le renseignement occidental est fondée sur la rationalité voulant qu'elles contiennent des informations permettant de prévoir des actions futures. « In the aftermath of 9/11, the Madrid and London bombings, political authorities in the West have pursued the idea that knowledge about future risk is *always already present* in the data, if only information on transactions patterns can be effectively integrated and mined » (Amoore & de Goede 2008b, 174). À la question « how do we thwart a terrorist who has not yet been identified? », le dispositif de sécurité propose de relier les points, « joining [the] dots that should have been connected before 9/11 » (Department of Homeland Security cité dans Amoore 2011, 26). Cette approche vis-à-vis des données de masse demande l'opérationnalisation de données produites dans des espaces et des temps différents et dans des contextes qui ne sont pas ceux de la sécurité en informations de sécurité (Amoore 2011). Comprendre cette opérationnalisation demande un accès à la production de savoir de la NSA et du renseignement occidental, savoir qui demeure pour l'essentiel secret, protégé par les scellés du système de classification de sécurité. L'œuvre Secret Power de Simon Denny offre un accès partiel, néanmoins provocateur, à l'opérationnalisation du savoir de la NSA. En insistant sur la cartographie de l'organisation, l'œuvre ouvre la porte à l'exploration des concepts de géopolitique et de souveraineté, notamment à travers la reterritorialisation de la menace à l'ère numérique où la fixité du territoire cède le pas à la mobilité des réseaux et la fluidité des données. La recherche d'une menace à la fois omniprésente et invisible pousse à la sécurisation de tous les espaces sociaux.

5.1 Percer la culture du dispositif de sécurité américain

Dans l'exposition Secret Power, Simon Denny, représentant la Nouvelle-Zélande à la Biennale de Venise de 2015, propose une incursion à l'intérieur de la culture organisationnelle de la NSA et ses consœurs du Five Eyes pour comprendre la façon dont ces agences rationalisent le savoir de sécurité (Leonard 2017). Si une telle incursion est généralement impossible vu le secret les entourant, les révélations de Snowden offrent un aperçu à l'intérieur de cet espace clos. La production visuelle de la NSA qui apparaît sur les diapositives PowerPoint et qui accompagne le

texte des révélations sont, pour l'artiste, autant d'artefacts du savoir de sécurité des agences de renseignement occidentales donnant accès au monde tel qu'elles le définissent. En organisant une exposition autour de ces documents, Denny explore « the culture within technology organizations and state technology organizations and how sovereignty and geopolitics is imaged today, » explique l'artiste (Te Papa 2016c). L'artiste met aussi en lumière les effets de l'acte de révélation de Snowden. Le geste du lanceur d'alerte a transformé les diapositives de la NSA en artefacts culturels de la façon dont le public conçoit Internet et les pressions qu'exerce la surveillance numérique sur les concepts de géopolitique, de souveraineté et de vie privée. Pour Denny :

> the Snowden slides … turned into some of the most culturally important material of the current age. I think it changed the way a lot of people thought about sovereignty in the world and the way a lot of people felt about privacy and the way that they were vulnerable online, or not. I think one of the reasons why I made this project is to highlight the fact that those images that were designed within that organisation became an icon for all those issues around sovereignty and privacy and access and visibility (Te Papa 2016a).

Installée dans la Bibliothèque Marcienne à Venise et dans l'aéroport international Marco Polo de Venise, l'œuvre de Denny propose de retourner à « l'iconographie du pouvoir » produite par la NSA pour réfléchir à la définition de la souveraineté et de la géopolitique en forçant le contact entre l'espace et le contenu de l'exposition. Comme l'explique Robert Leonard, le commissaire du pavillon néo-zélandais,

> *Secret Power* is site specific, exploring La Biennale Arte di Venezia, the Library, and the Airport as media. Denny hints at geopolitical imperatives that cross-reference and distinguish these frames. Completed in 1588, the Library represents the Republic of Venice as a wealthy world power during the Renaissance. Established in 1895, La Biennale is premised on a model of national representation that seems obsolete today, in a time of cosmopolitan global art. Completed soon after 9/11, the Airport represents a new era of global security (Leonard 2017).

La rencontre forcée entre ces représentations contemporaines, un espace légataire d'une conception désuète du savoir, un événement artistique fondé sur une division contestée du monde, et une infrastructure actuelle du dispositif de sécurité, offre une occasion particulièrement riche pour explorer la relation actuelle entre savoir et pouvoir promue par la NSA.

Le spectateur qui arrive dans la Cité des Doges par la voie des airs découvrira d'abord la partie de l'œuvre située dans l'aéroport Marco Polo. Là, Denny a installé sur les murs et les planchers du hall d'arrivée de l'aéroport des reproductions de certaines œuvres de la Renaissance qui habille la Bibliothèque Marcienne. En même temps que l'artiste juxtapose des peintures et

cartes anciennes, symboles de la puissance de la République vénitienne, aux « restricted spaces, surveillance spaces, and interrogation spaces » (Leonard 2017) de l'appareil moderne de sécurité de la ville qui assure sa connectivité avec les autres pôles du monde et la mobilité nécessaire à son industrie touristique, Denny rappelle qu'un aéroport occupe des fonctions qui ne sont pas uniquement utilitaires ou sécuritaires, mais aussi commerciales vendant ses aires d'affichage à des fins de publicité (McGarry 2015). L'artiste rappelle ainsi le lien entre l'aéroport et les mondes économiques et sécuritaires, thème largement documenté ailleurs (voir Salter 2008b; Fuller 2003; Adey 2006).

Le cœur du projet de Denny se trouve toutefois à la Bibliothèque Marcienne, construction de la Renaissance, où il occupe le grand salon. Le spectateur y pénètre à partir du vestibule où sont exposées deux cartes anciennes des 15^{e} et 16^{e} siècles. Une fois dans le grand salon, le spectateur franchit une porte vitrée imitant les entrées standardisées des bâtiments institutionnels contemporains symbolisant un des objectifs de l'artiste avec son œuvre : l'entrée dans la culture organisationnelle du renseignement occidental. Dans le grand salon, Denny a installé huit baies de serveurs et autant de stations de travail qu'il utilise comme vitrines transformant, le temps de la Biennale, le salon de la bibliothèque en centre de données. Y sont exposées diverses études de cas de la culture visuelle de la NSA, reprenant des cartes et des icônes associées à divers programmes, certaines sculptées à l'aide d'imprimantes en trois dimensions. L'artiste a ainsi recréé l'aigle à tête blanche, symbole de la souveraineté américaine, tenant le monde dans ses serres, sceau officiel des Special Sources Operations (SSO) de la NSA, la tête robotique de la série culte Terminator du programme TREASUREMAP, et le magicien de MYSTIC, programme de surveillance des téléphones cellulaires, pour ne nommer que ceux-là. Les représentations visuelles qui apparaissent dans les diapositives de la NSA donnent accès à la conception de la souveraineté et de la géopolitique de l'organisation grâce, notamment, à une riche production de cartes. Denny souligne également les allusions au jeu et à la magie qui se retrouve dans le document du GCHQ « The Art of Deception: Training for Online Covert Operations » et aux nombreuses références à la culture populaire qui meublent les diapositives. Cette insistance sur les liens et appropriations avec la culture populaire se veut critique (Thackara 2015). La réutilisation ou l'adaptation de représentations issues de la culture populaire rend candides des pratiques souveraines et exceptionnelles à la frontière du droit, de la vie et de la mort.

Secret Power n'est pas que visuel, Denny travaillant sur l'environnement de l'exposition pour contester la surveillance numérique. Ainsi, en plus des références visuelles aux activités de la NSA, le matériel informatique utilisé provenant des compagnies CISCO et HP fait écho aux opérations de piratage de l'agence, les Tailored Access Operations, qui profitent des failles de sécurité de certain matériel pour pénétrer sur les appareils électroniques des cibles du renseignement et accéder à leur contenu (Appelbaum, Horchert & Stöcker 2013; NSA 2008; Herrick 2015). Pour l'artiste, la symbolique entourant ce matériel piraté dépasse toutefois l'action ciblée. Il représente, plus largement, la vulnérabilité et l'absence de certitude quant à la protection de la vie privée des utilisateurs des technologies numériques. « These had become hacked and that's a hardware metaphor within the context of how we feel after the Snowden revelations, » explique Denny. « We realised that what we were doing online before, which we assumed was private, was actually much more public » (Denny cité dans Herrick 2015). L'expérience de Secret Power est également auditive. Le bourdonnement incessant des systèmes de ventilation des serveurs invoque la composante matérielle et temporelle de la surveillance numérique, rappelant, à travers le travail des serveurs qui procèdent au traitement continu des données collectées, la permanence de la surveillance (Click 2015).

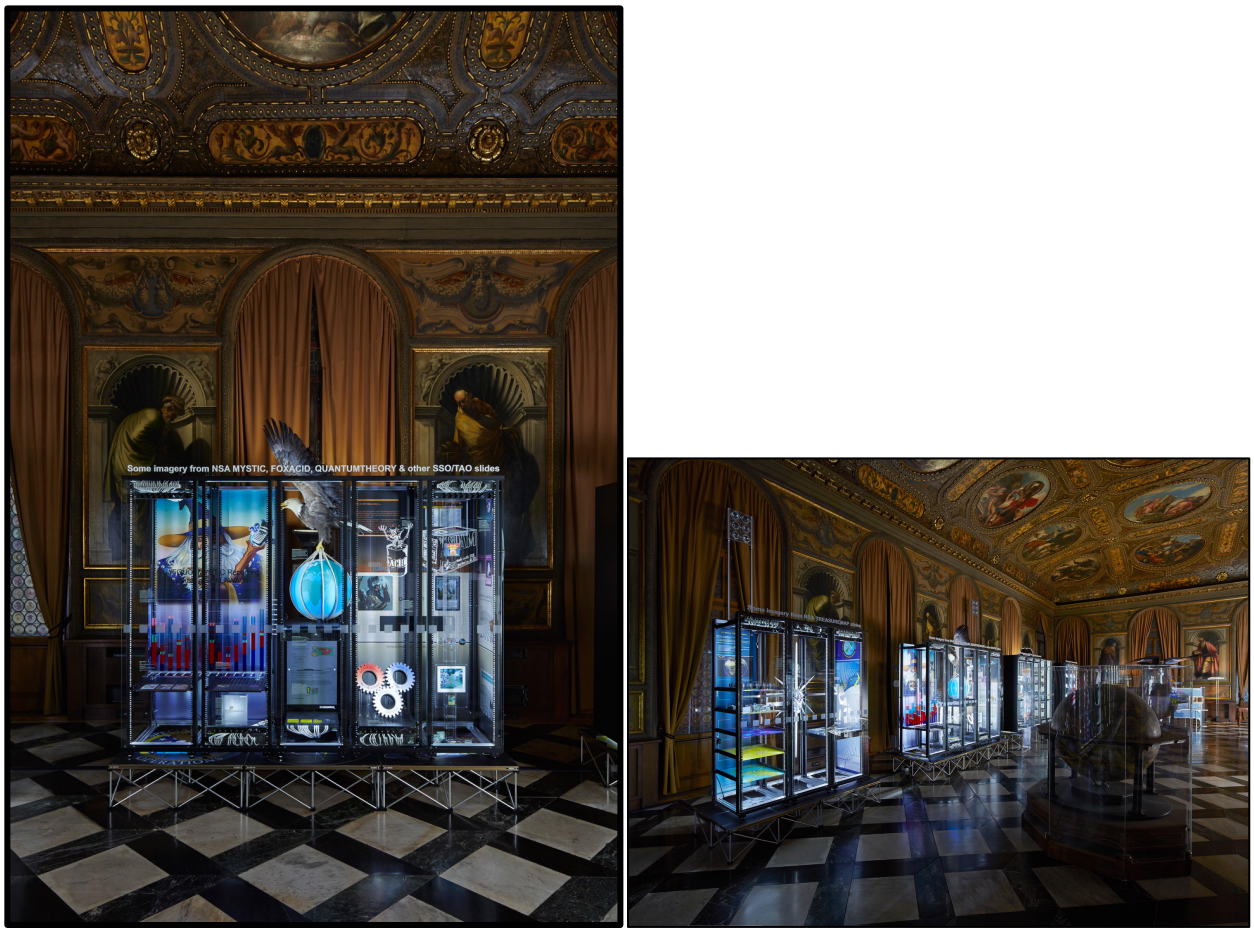


Figure 5.1 : Secret Power à la Biennale de Venise 2015
rencontre entre les iconographies du pouvoir (source : Leonard 2017)

Secret Power se veut ainsi une expérience immersive au cœur de la culture du renseignement occidental où l'artiste « uses space to isolate aspects of the media culture rather than mapping them » (Angelotti 2015). Il permet au visiteur de voir et ressentir son fonctionnement et la production de savoir qui en émane plutôt que d'expliquer ce qu'il expose. « Paradoxically, » suggère le commissaire du projet, « [Denny] places himself and us (as artist and viewers) in positions oddly analogous to these agencies, as we trawl through data and metadata, engaging in analytics, pattern recognition, and profiling, trying to make sense of things » (Leonard 2017). Si Denny invite à réfléchir sur nombre de questions, il se garde toutefois d'offrir des réponses toutes faites aux enjeux de géopolitique et de souveraineté soulevés par la surveillance numérique de la NSA. « Faire la critique, c'est rendre difficiles les gestes trop faciles », proposait Foucault (Foucault 1994a) ; Denny interpelle le spectateur, l'incite à se questionner sur les pratiques de surveillance et leurs conséquences sociales. Comme il le dit en entrevue avec un journaliste néo-zélandais,

> I think critique can get a lot of different interpretations. Critique to some people can be someone saying, "fuck you, I think it's bad" or whatever. But my notion of what great critique is is more like "let's look at what this means and let's look at how it operates." It's not rejection of the value system that it's looking at, necessarily. It's a careful look at it. I don't want to say the NSA is bad or all intelligence is bad. That's not what I'm trying to do with the work (Manhire 2016).

Dans la même entrevue, il prend d'ailleurs ses distances face à la position plus ouvertement dénonciatrice du journaliste d'enquête Nicki Hagger, conseiller technique pour la réalisation du projet, et dont le livre Secret Power, paru en 1996, sur les liens entretenus par la Nouvelle-Zélande avec les opérations du renseignement américain donne son titre à l'œuvre de Denny. Pour l'artiste, le projet est avant tout exploratoire et réflexif : « [an] inquiry into the current iconography of geopolitical power being framed within an obsolete one » (Leonard 2017).

5.2 Déstabilisation esthétique : sortir l'iconographie du pouvoir de son environnement naturel

Pour Denny, les documents révélés par Snowden sont parmi les plus importants documents culturels du moment. L'espace et la fonction sociale du musée permettent de reconnaître leur importance en les exposant « alongside other things that we revere » (Te Papa 2016a). Le geste de Denny est résolument politique et critique, même si la critique ne se veut pas un rejet catégorique et explicite de la surveillance numérique de la NSA. En isolant ces artefacts dans les vitrines de la Bibliothèque Marcienne, Denny utilise le pouvoir institutionnel du musée pour préserver les documents Snowden. À l'instar de la démarche d'Ai Weiwei et Jacob Appelbaum (Poitras 2015), il les préserve contre la censure, s'assurant que le savoir secret qu'ils contiennent ne sera pas confisqué par l'institution détroussée. Pour paraphraser Christine Sylvester, on pourrait dire que la Biennale de Venise participe dans ce contexte à un « pillage » d'artefacts culturels, d'un retrait de ces artefacts de leur environnement habituel, au nom de l'accès à l'information et du droit de savoir en démocratie. Le musée, plus que le système de classification de sécurité, est à même de garantir la conservation et l'accessibilité de cet héritage culturel (Sylvester 2013, 209-212).

Cette démarche esthétique et muséale cherche à donner accès au bagage culturel habitant l'iconographie du pouvoir. En ce sens, elle s'apparente à celle de la géopolitique critique qui interroge les constructions spatiales de la sécurité. Comme explique David Grondin,

> [c]ritical geopolitics is an attempt to critically think how geographical and political security are rendered in policy discourses on matters that speak of war, peace, diplomacy, security,

> foreign policy, etc. … It is because of the 'symbolism that is part of the discourses of politics and [that] has significance precisely because of the stories that are thus told' that a critical geopolitics becomes so essential (Dalby 2007a). It allows one to both make sense of how space, power, political identity (the nation), and geographical categories (like the global) interact with one another and reflect on the knowledge (geopolitics) produced by these relations (Grondin 2010b).

Au côté des documents officiels, rapports de centre de recherche et autres forums d'experts, la géopolitique critique porte également attention aux productions issues de la culture populaire et les arts. La place du cinéma dans la construction et la diffusion de l'espace de sécurité a fait l'objet d'un intérêt particulier, explorant par exemple la représentation de l'exceptionnalisme américain ou la légitimation du soldat (Crampton & Power 2005; Carter & Dodds 2011; Lawrence & McGarrahan 2008; Dittmer 2011). Mais, d'autres médias populaires ont également été mis à l'examen : photographie, périodique, caricature, publicité, jeux vidéo ont tous été analysés en partant du postulat que « geopolitics [is] a social and cultural process by which leaders and ordinary citizens make sense of the world » (Hughes 2007, 983). Le projet de Denny n'est pas différent. Reproduisant à la pièce des documents institutionnels, il propose une exploration visuelle et immersive dans la culture de sécurité.

Denny construit son œuvre comme une incursion physique et sémiotique dans la culture institutionnelle de la NSA. Il présente ainsi un texte de sécurité que le spectateur est invité à lire et à analyser. Ce texte, même s'il est essentiellement visuel, recréé à partir des images et cartes des diapositives PowerPoint de la NSA, n'est pas moins significatif qu'un discours officiel. Comme le souligne Trevor Paglen dans le cadre de son projet Symbology (Paglen 2017b), dans lequel l'artiste explore la culture militaire à travers les symboles et insignes des unités et projets secrets du Département américain de la Défense, les productions visuelles officielles et officieuses issues de ce monde secret permettent de comprendre de quelle façon les militaires répondent aux questions de l'identification de groupe dans le contexte du secret (Van Tomme 2009). Loin d'être aléatoires, les symboles utilisés sur ces insignes forment un langage : « [i]f you could begin to learn its grammar, you could get a glimpse into the secret world itself » (Paglen 2008, 3–4). Comme pour les insignes, suggère Denny, les représentations visuelles qui accompagnent les diapositives de la NSA constituent un langage propre.

> The images contain different kinds of information than the text. They give us a hand in understanding more about the culture — the office culture, let's say — behind the surveillance programs, and therefore the kinds of interests and values of the people working

> on them. They are an insight into the environment the programs are maintained and proliferated within (Denny cité par Gallagher 2015a).

Décoder ce langage permet d'accéder au savoir interne de l'organisation : à leur définition de l'espace, de la géopolitique, de la souveraineté et, plus généralement, à leur production de savoir de sécurité.

L'œuvre de Denny ne se limite pas à cette présentation textuelle. En créant une adéquation évidente entre le contexte de l'exposition et celui du texte exposé, Secret Power utilise également les dimensions temporelles et spatiales pour favoriser le regard critique du spectateur. Denny imite avec des objets contemporains les pratiques des musées qui scellent dans des cryptes un savoir passé assurant aux générations futures la possibilité de revenir sur une époque révolue. Il isole les représentations et pratiques de surveillance numérique de la NSA, accentuant certains thèmes, tels que la souveraineté et la géopolitique, et éclairant certaines de ses apparentes contradictions. Sa référence à la série *Terminator*, représentation populaire des dangers associés à la militarisation de l'intelligence artificielle, suggère ainsi un futur sombre, déterminé par la technologie et à l'extérieur du temps humain, du temps de traitement de l'information par le cerveau humain, mais peut-être aussi du temps où l'humain ne sera lui-même qu'histoire (Te Papa 2016b).

Par cet exercice, Denny invite les spectateurs à se projeter dans le futur et à regarder le présent comme ils regardent les artefacts des siècles passés. Faute de pouvoir proposer une généalogie de ces pratiques de surveillance, l'artiste semble proposer l'obsolescence et l'archaïsme pour ancrer la contingence dans la réflexion sur la production du savoir de sécurité de la NSA. Denny entretient ainsi une proximité d'esprit avec l'approche théorique et artistique de l'archéologie des médias qui invite à repenser l'histoire des médias afin de contester les prétentions à la nouveauté et à mieux contextualiser le développement des technologies, notions souvent écartées par l'étude des nouveaux médias (Huhtamo & Parikka 2011b; Parikka 2012). L'histoire des médias, rappelle-t-on, n'est pas téléologique ni linéaire. Les médias tels qu'ils existent au moment présent sont le résultat de soubresauts, d'essais et de reculs : une accumulation de sédiments qui rappelle la nécessité de s'intéresser à la relation entre le développement des technologies et l'univers social, entre « the discursive and the material manifestations of culture » (Huhtamo & Parikka 2011a, 3). Les médias n'existent pas indépendamment du monde extérieur, ils ne s'imposent pas uniquement pour leur valeur utilitaire ou leur efficacité (Feenberg 1999). Des raisons culturelles, économiques et politiques contribuent à la prédominance ou à la disparition de

certains médias. Si les nouveaux médias transforment certains aspects de la société actuelle, le déterminisme et l'euphorie technologique menacent la réflexion critique et nuancée sur l'état de nos sociétés. Malgré cet intérêt marqué pour l'histoire, l'archéologie des médias est donc, dans la tradition foucaldienne, avant tout tournée vers le moment actuel et cherche à comprendre et à réexpliquer d'une manière non linéaire ni progressive les conditions d'existence du présent (Parikka 2012, 1-18).

Secret Power est une occasion de penser la production de savoir et les constructions géopolitiques dans une perspective culturelle, historique et contextuelle, plutôt que positiviste, linéaire et progressive, à l'image de la démarche de l'archéologie des médias. Si elle ne cherche pas à réécrire une histoire alternative du savoir tel qu'il existe aujourd'hui, l'œuvre invite néanmoins à lire la production contemporaine de savoirs de la NSA avec les yeux de l'archéologue. Cette production de savoir, suggère Secret Power, n'est pas le développement naturel ou évident d'anciens savoirs incomplets ou faillibles ni l'aboutissement logique ou téléologique de la sécurité, mais le résultat contingent de savoir, la rencontre intentionnelle et fortuite de technologies, pratiques et stratégies de sécurité. Accentuant l'idée de rencontre, Denny présentait en parallèle à Secret Power l'exposition Innovator's Dilemma au MoMA PS1 de New York, institution partenaire du célèbre musée d'art contemporain, dans laquelle il explorait les pratiques culturelles de Silicon Valley et le rôle des technologies dans la détermination d'une culture médiatique mondiale (Thackara 2015; voir aussi Leonard 2017). Les projets se parlent : les deux cultures institutionnelles partagent les mêmes fantasmes du pouvoir des données. Denny y invite le spectateur à observer le savoir contemporain de la NSA non pas comme la finalité de la sécurité, mais comme un produit de son époque que les générations futures regarderont probablement avec les mêmes yeux à la fois amusés et condescendants avec lequel nous regardons les anciennes représentations du monde et iconographie du pouvoir désormais obsolètes qui meublent la Bibliothèque Marcienne.

Denny mise sur la dissociation entre la Biblitohèque Marcienne et la surveillance numérique pour nourrir cette réflexion culturelle et historique sur la production contemporaine de savoir de sécurité. Terminée dans la deuxième moitié du 16^{e} siècle, la Bibliothèque Marcienne est une œuvre de la Renaissance de l'architecte Jacopo Sansovino. La Bibliothèque s'est vue attribuer une fonction politique dès son origine, construite, avec un retard d'un siècle, pour héberger la collection d'ouvrages que le cardinal grec Bessarion avait léguée à la ville en 1468. Devant la

menace à l'héritage grec ancien que représentait la prise de Constantinople par les Ottomans, le cardinal regroupa une collection de plus de 1100 objets qu'il remit à la ville. Le geste se voulait, en plus d'un acte de préservation, une marque de reconnaissance pour l'accueil que Venise offrait aux Grecs fuyant les Ottomans et un hommage à la puissance culturelle de la ville et à son opposition aux ennemis de Byzance (Monfasani 1982; R. A. Burke 1982). Face au Palais des Doges sur la place Saint-Marc, l'emplacement de la Bibliothèque dans le cœur politique, religieux et culturel de la ville réaffirme sa centralité et le vecteur de pouvoir qu'elle représente. Le grand salon où est exposée l'œuvre de Denny est décoré de peintures des grands maîtres de l'École de Venise, les Titien, Le Tintoret, et Véronèse, source d'influence culturelle importante à une époque de grande production artistique, non loin d'ailleurs de l'esprit des pavillons nationaux de la Biennale elle-même où chaque pays peut promouvoir sa culture et son identité nationale à travers sa production artistique (Merson 2017, 49-51). Ces peintures, représentant la philosophie et la sagesse, sont une « allegory for the benefits of acquiring knowledge » (Leonard 2017). La Bibliothèque abrite également des cartes du monde connu de l'époque, produits et instruments de la puissance maritime de Venise. Ainsi, en tant que « state-produced house for knowledge, » la Bibliothèque offre, pour l'artiste, un espace de prédilection pour tenir « a conversation about visual languages within intelligence communities » (Denny cité par Herrick 2015).

Pour qui cherche à décoder l'iconographie du pouvoir de l'époque, la Bibliothèque est beaucoup plus qu'une allégorie. Dans une série de seize tableaux, elle dépeint sur ses murs, avec des représentations de Platon et Aristote, les canons de la philosophie occidentale à la Renaissance. Au côté de ceux-ci se retrouvent les valeurs chrétiennes essentielles, la foi et la charité, mais aussi Prométhée, le titan à la source du savoir humain, symbole de la naissance de l'homme et de sa sortie de l'état de nature selon le récit raconté par Protagoras à Socrate (Platon 1967 320c-322d). La présence de Prométhée sur les murs de la Bibliothèque n'est pas fortuite. La Renaissance italienne marque la naissance de l'homme moderne et les balbutiements de l'État dorénavant maîtres de leurs destins face aux forces divines et aux revendications temporelles de Rome. Prométhée affirme l'existence autonome de Venise. Mais alors que le titan vola aux dieux le don du feu et des arts pour les remettre aux humains, celui d'administrer les cités demeura entre les mains de Zeus. Les œuvres du plafond de la Bibliothèque compensent cette lacune. Y sont peints les détails de ce que constituaient à l'époque les arts, sciences et vertus essentiels au progrès des sociétés. Ainsi sont mises côte à côte des représentations de l'histoire naturelle, de l'agriculture et

de la chasse ; des mathématiques, de la géométrie et de l'astrologie ; de la vertu (Machiavelli 1994), de l'honneur et de la gloire ; des arts, du commerce et de la richesse ; du gouvernement, de l'Église et de l'armée (voir le détail des œuvres couvrant le grand salon de la Bibliothèque Marcienne dans Leonard 2017).

Les représentations habillant la Bibliothèque Marcienne constituent un guide détaillé de l'iconographie du pouvoir de la Renaissance vénitienne. Denny semble suggérer que les documents rendus publics par Snowden offrent des informations similaires sur notre époque. Ceux-ci donnent un accès privilégié pour comprendre la façon dont la NSA définit et opérationnalise les concepts de géopolitique et de souveraineté et plus largement la production de savoir de sécurité. Comme le suggère la figure de Prométhée, l'époque actuelle marque un moment de transformation géopolitique.

5.3 Lire la production du savoir géopolitique : la cartographie et la création du territoire

Le rapport à l'espace est au cœur de l'œuvre de Denny, celui-ci consacrant une vitrine à la production de cartes et du savoir spatial. Dans celle-ci, l'artiste expose une reconstitution sur verre de plusieurs cartes présentes dans les diapositives révélées par Snowden qu'il oppose aux cartes médiévales présentes dans la Bibliothèque. « Some of the way I was framing the way to look at this material, » explique-t-il, « is about how we imagine space today and what is a contemporary image of the world » (Te Papa 2016a). Cette mise en exergue n'est pas incohérente avec les concepts de géopolitique et de souveraineté qu'il tente d'éclairer, les deux faisant référence au territoire. Mais, si la cartographie est généralement interprétée comme une science factuelle et les cartes, comme un exercice de précision (Neocleous 2003, 417), l'artiste rejette ce postulat positiviste. Comme l'écrit Tess Thackara dans sa critique de l'œuvre, « [b]oth maps and vitrines (and the vaunted, stately architecture of the library itself) demand the reverence that comes with knowledge and power, and yet at their core, Denny suggests, are abstractions and fantasy » (Thackara 2015). Similairement, Kevin McGarry relève l'importance de la cartographie dans le projet : « Denny's twinned project plumbs mapmaking as a form of data visualization that began in ancient times, which to this day maintains a duality between faithfully charting the world as we have explored it and romantically projecting fantasies of elsewhere » (McGarry 2015). Les deux critiques reconnaissent l'objectif de dé-essentialisation des représentations de l'espace que se

donne l'artiste. Le terme fantaisie doit toutefois être lu avec prudence. Il ne s'agit pas de suggérer une déconnexion complète d'avec la réalité, ou un acte créatif pur, mais comme le propose Jacques Lévy qu'une carte communique d'abord une idée, « [u]ne idée qui n'est géographique que dans la mesure où elle correspond à une spatialité, mais qui demeure une idée, intégrable dans le cadre d'une pensée du social qui, elle, ne peut se limite à sa dimension spatiale » (Lévy 2008, 32-33). Une carte est le produit d'une vision du monde, elle n'est pas une reproduction du monde. Denny joue avec les incongruités entre les reproductions anciennes et contemporaines du monde pour illustrer cette réalité.

Figure 5.2 : Production de savoir géopolitique à travers les cartes
À gauche : « Various Maps Depictions from Snowden-Leaked Slides » (détail) par Simon Denny (source : Leonard 2017).
À droite : Carte de Fra Mauro (1460) : représentation moderne et cosmologique du monde. Fidèle à son époque, le sud est représenté en haut de la carte. (source : Falchetta 2006)

En plus des livres et peintures qu'elle abrite, la Bibliothèque Marcienne sert de dépositoire de cartes et de globes anciens. Un des artefacts les plus célèbres est la carte du monde de Fra Mauro, carte monumentale de deux mètres de diamètre datant de 1460. Cette carte est reconnue notamment pour sa taille et l'ampleur de son détail, la carte contenant près de 3000 inscriptions (P. D. A. Harvey 2015, 106), pour être la première représentation européenne du Japon (Leonard 2017), et pour représenter la circumnavigation de l'Afrique jusqu'à l'océan indien avant qu'elle ne soit effectuée par un explorateur européen contrairement à la géographie ptoléméenne dominante à

l'époque qui faisait de cet océan une mer intérieure (Olshin 2014, 839). Pour réaliser sa carte, le moine-cartographe vénitien compara les références géographiques établies à une multitude de sources différentes provenant de voyageurs et de commerçants, dont les récits de l'explorateur vénitien Marco Polo, afin d'en faire une carte précise et utile pour les navigateurs. Une copie de la carte, aujourd'hui perdue, aurait d'ailleurs été commandée par le roi Alfonso V du Portugal, dont le pays était en pleine exploration du continent africain. Pour sa méthodologie et sa précision, l'historien Piero Falchetta, conservateur à la Bibliothèque Marcienne, voit dans cette carte une œuvre expérimentale à cheval entre les représentations médiévales et modernes de l'espace (Nuti 2008, 170; P. D. A. Harvey 2015, 106-107).

Le cartographe demeure ancré dans la conception médiévale de l'espace selon laquelle le monde naturel et divin ne forme qu'une seule image (P. D. A. Harvey 2015, 106). Ainsi, la sphère terrestre se retrouve-t-elle au cœur des multiples sphères célestes qui composent la cosmologie chrétienne de l'époque et que l'on peut observer dans les quatre coins de la carte (Vogel 2011, 85-87). Comme l'écrivent Christian Vandermotten et Julien Vandeburie, cette « territorialité cosmologique rend compte jusqu'à la Renaissance des prétentions universalistes et du discours idéologique de l'Église » (Vandermotten & Vandeburie 2005, 117). Cette cosmologie est généralement représentée par des cartes en T, à l'instar du Rudimentum Novitiorum (Brandis 1475a) réalisé quinze ans après la carte de Fra Mauro. La terre, disque plat, est divisée en trois, représentant l'occupation du monde par les fils de Noé. L'est est situé en haut de la carte où se retrouve l'Asie et Jérusalem, route vers le paradis qui trône au sommet, le sud et l'Afrique sont à droite, et le nord et l'Europe à gauche. Les régions et duchés y sont représentés, mais leur exactitude géographique demeure approximative (Vandermotten & Vandeburie 2005, 117-122).

Figure 5.3 : Rudimentum Novitiorum
cartographie ecclésiastique (Brandis 1475b)

Fra Mauro brise avec une partie de cette tradition ecclésiastique, bien qu'il soit lui-même issu de l'Église. Il incorpore à sa carte les considérations des commerçants et explorateurs en tentant une représentation juste des territoires afin de faciliter la mobilité. Il écrit, en outre, sa carte en italien vénitien plutôt qu'en latin, rompant avec l'universalité de l'Église et affirmant la puissance de la République de Venise comme territoire particulier (P. D. A. Harvey 2015, 106). En ce sens, la carte de Fra Mauro constitue « a testament to the power, wealth and knowledge of its Venetian homeland » (Gow 2007, 235). Mais cette volonté instrumentale qui guide Fra Mauro dans sa représentation spatiale du monde connu au tournant de la Renaissance demeure indissociable du cadre de pensée qui domine le rapport à l'espace au milieu du 15e siècle : la cosmologie des sphères que Fra Mauro ne conteste pas. Fra Mauro écrit ainsi au bas de sa carte :

> This work, created for the perusal of our illustrious signori, is not as complete as it should be, as it is quite impossible for the human intellect to comprehend this cosmography or map of the world in its entirety without some kind of celestial demonstration; it serves merely to impart a taste of knowledge rather than to satiate a thirst for it (cité par Vogel 2011, 84).

La connaissance de la géographie terrestre reste dépendante du savoir théologique. Dans ce contexte, la théologie ne constitue pas un frein à la réalisation d'une cartographie moderne qui

serait quant à elle vraie, mais oriente l'objectif même de la cartographie qui vise à représenter la sphère terrestre de plus accessible et connue par les Européens dans le même espace que les sphères divines inaccessibles et inconnues.

L'œuvre de Fra Mauro, suggère Klaus Vogel, « marks the limit of geographical experience » (Vogel 2011, 83). Elle démontre néanmoins les considérations terrestres du cartographe qui consacra l'essentiel de ses efforts non pas à répondre aux problèmes de l'histoire naturelle chrétienne, mais à représenter les territoires afin de faciliter la mobilité des navigateurs et commerçants. La carte offre ainsi une représentation visuelle de la rencontre de deux modes de savoir distincts et non pas simplement, comme l'observateur contemporain pourrait être porté à croire, la manifestation naïve d'un savoir encore incomplet. Pour Falchetta,

> ancient maps existed as "autonomous texts in their own right; due to the synthesis operating within them, they themselves generated knowledge and skills. And such knowledge and skills were not merely the synthesis of components that might exist independently of each other; their most efficient manifestation—sometimes their sole manifestation—lay in their expression within works of cartography" (Falchetta cité par Nuti 2008, 170).

Pourtant, rappelle Falchetta, aussi longtemps que ces cartes anciennes seront jugées selon les critères de justesse et de précision actuels, elles ne pourront être appréciées pour ce qu'elles sont : des artefacts du savoir géographique médiéval (Olshin 2014, 839) et demeureront « gorgeous but obsolete medieval cartography » (Falchetta cité par Gow 2007, 235).

Outre que l'on ne pourrait qualifier les cartes produites par la NSA avec l'épithète splendide, celles-ci constituent néanmoins, à l'instar des cartes médiévales, des manifestations d'un savoir particulier qui se comprend qu'en relation avec un contexte social plus large. Car, malgré les prétentions mimétiques des cartes modernes, elles manifestent une façon particulière de voir et concevoir l'espace et le monde : une vision perspectiviste de l'espace générée à partir d'un point de vue unique et souverain (O Tuathail 1996).

Plusieurs lient le développement de la cartographie moderne à la formation des États notant la synchronie entre la prolifération des cartes et l'essor de l'État. « In 1400 few people in Europe used maps, other than the Mediterranean navigators with their portolan charts; » soulève Mark Neocleous,

> by 1600, however, maps had become essential to a wide variety of professions, (Buisseret, 1992). This was the very period in which the state came to the fore, and it is the emergence

> of the state and the need to delineate the borders of states, combined with the search for new trade routes, to which the theory and practice of cartography were committed (Neocleous 2003).

Vandermotten et Vandeburie dressent également le parallèle avec la construction de l'État absolutiste, rappelant que la première carte de France date du milieu du 16e siècle (Vandermotten & Vandeburie 2005). Cette nouvelle cartographie conteste les autres rapports à l'espace existant à l'époque, que ce soit la cosmologie chrétienne ou les portulans de navigation et les tables itinéraires qui décrivent les routes maritimes ou terrestres à suivre pour atteindre un endroit spécifique comme une côte, un marché ou un lieu de pèlerinage (Vandermotten & Vandeburie 2005, 117). Contrairement à ces dernières, la carte moderne n'a pas de vocation théologique et ne se conçoit pas uniquement sur la base de la mobilité. Elle est un outil d'inscription de l'État dans la fixité de son territoire. La carte moderne place l'État, entité politique naissant, en son centre. À travers elle, « space was homogenized … and measured from a central point, which was normally the seat of government or royal authority. This central point constituted the fixed spectatorial position from which panoramic visions of official state territory were constructed » (Ó Tuathail cité par Hughes 2007, 980). Elle constitue un instrument de pouvoir pour l'État. Par son travail de collecte et de représentation, la cartographie moderne offre à l'État un savoir particulier, voire unique lorsque les cartes sont gardées secrètes, sur les entités qui composent son espace intérieur et son environnement extérieur. En ce sens, elle aide les États à garder le contrôle et à maximiser les forces sur son territoire, de la même façon qu'elle répond aux besoins de connaissance du territoire des militaires (Perkins & Dodge 2009, 547). Dans un vocabulaire foucaldien, la carte joue ainsi un rôle policier.

La carte de l'État est également performative, rendant effectif ce qu'elle représente. « To map a territory, » écrit Neocleous,

> means to formally define space along the lines set within a particular epistemological and political experience — a way of knowing and dominating — transposing a little-known piece of concrete reality into an abstraction which serves the practical interests of the state, an operation done for and by the state (Neocleous 2003, 417).

La carte donne une existence à l'État, sert de point de départ à l'affirmation de sa puissance sur « son » territoire et vers l'extérieur. Les tensions au sein de l'État, tel que les droits particuliers de l'aristocratie et de l'Église, sont réduites au statut de détails régionaux ou secondaires, la carte unifiant un territoire encore juridiquement fractionné accentuant la domination du souverain sur

cet espace social. Parallèlement, la carte moderne crée l'État comme entité politique internationale. Elle lui attribue une de ses composantes essentielles : un territoire, nécessaire à l'existence de l'État, sans quoi il ne peut prétendre à la souveraineté face aux autres États. Sans frontière, un État n'a pas de présence. « Sovereignty does not just imply space, it creates it; » suggère Neocleous, « left to itself, the earth has no political form … [T]o the extent that the map helps create the borders, so it helps create the thing which is being bordered » (Neocleous 2003, 418).

En traçant des frontières encore contestées et imprécises, la cartographie moderne traduit une multitude de lieux géographiques et de relations sociales en un territoire homogène, cohérent, fini et particulier aux côtés d'autres territoires similaires qui menacent son intégrité. Elle naturalise aussi ces deux ordres sociaux intérieurs et extérieurs, effaçant les violences de la territorialité étatique nécessaires à la formation des identités nationales exclusives et celles qui habitent la géopolitique mondiale. Neocleous conclut :

> the map helps mask the violence that brings the state into being and the interests that sustain the ideological preponderance of the state system. Borders may be drawn in blood, but the blood never appears on the page. It is the repetitive impact of the image of the territory mapped that lends credence to the claims of control; that is the way of myth. … [T]he map legitimizes the great movement of territorialization through which the whole earth has been turned into an object of state ownership. Any other form of politics is regarded as obsolete, of no account at all (Neocleous 2003, 422).

La carte moderne perspectiviste est le modèle dominant de représentation du monde et de l'espace. Mais Secret Power suggère que ce modèle est peut-être en train de s'éroder. Coïncidence, l'œuvre de Denny est exposée la même année que TeleGeography publie sa carte des câbles sous-marins de fibre-optique rendant hommage au cartographe Mercator (TeleGeography 2017c). Dans celle-ci, TeleGeography reprend pour sa carte l'esthétique de la Renaissance que Denny utilise pour contester la production de savoir de la NSA. La carte de TeleGeography adopte l'approche perspectiviste de la carte de Mercator, situant le souverain en Europe, et recréant la territorialité associée à l'État : homogène et conflictuelle. Si la carte rappelle, malgré elle, la place de plus en plus importante des infrastructures numériques dans la géopolitique contemporaine, ce qui ne doit pas être négligé, certaines cartes issues de la NSA et reproduites par Denny semblent au contraire suggérer l'usure de ce mode de représentation de l'espace et avec elle une transformation de la conception de la géopolitique et de la souveraineté.

5.4 TREASUREMAP : chercher les secrets de l'univers numérique

Parmi les artefacts recréés et les programmes représentés dans Secret Power se retrouve la tête du Terminator, emblème du programme TREASUREMAP que la NSA mène avec ses partenaires du Five Eyes. Si l'attention médiatique s'est portée vers cette tête robotique, j'aimerais me tourner vers une autre partie de la vitrine où Denny reproduit trois diapositives d'une présentation PowerPoint intitulée « Bad guys are everywhere, good guys are somewhere » détaillant le programme. La première, du haut vers le bas de la vitrine, décrit les objectifs du programme. « What is TREASUREMAP? Capability for building a near-real time, interactive map of the global Internet, » est-il écrit, avant de souligner en caractères jaunes dans un encadré blanc : « Map the entire Internet — Any device, anywhere, all the time » (NSA 2010, 4).

La deuxième est une représentation satellitaire du globe terrestre de type Google Earth sur lequel apparaissent les frontières internationales. La vue est centrée sur la corne de l'Afrique, portant au premier plan le continent africain et le Moyen-Orient. Superposés sur le globe, des points nodaux bleus représentent l'emplacement géographique d'adresses IP et sont liés entre eux par des lignes blanches. Cette carte n'est pas sans rappeler celles d'IXmaps traçant avec l'application Google Maps les routes physiques prises par les paquets de données des communications Internet (IXmaps 2016). Comme pour les cartes d'IXmaps, les globes de TREASUREMAP ne représentent pas l'ensemble des connexions, mais ciblent, sans que l'on sache sous quel critère, certaines d'entre elles (NSA 2010, 24).

La troisième diapositive représentée montre cinq niveaux d'information — géographique, réseau physique, réseau logique, identité numérique (« cyber persona »), identité réelle (persona) — auxquels TREASUREMAP donne accès et le type d'analyse qu'il rend possible (NSA 2010, 6). La superposition des niveaux d'information suggère un raffinement de l'information de l'ensemble le plus vaste en bas, le niveau géographique représenté par un planisphère, vers le niveau le plus fin et le plus précis, l'identité réelle. Elle suggère également leur interconnectabilité, terme informatique signifiant la capacité d'un réseau d'être relié à un autre. Dans le contexte, l'interconnectabilité des réseaux n'est pas uniquement horizontale, elle l'est aussi verticalement entre les différents niveaux d'information.

Figure 5.4 : TREASUREMAP
installation de Secret Power (source : Denny 2015)

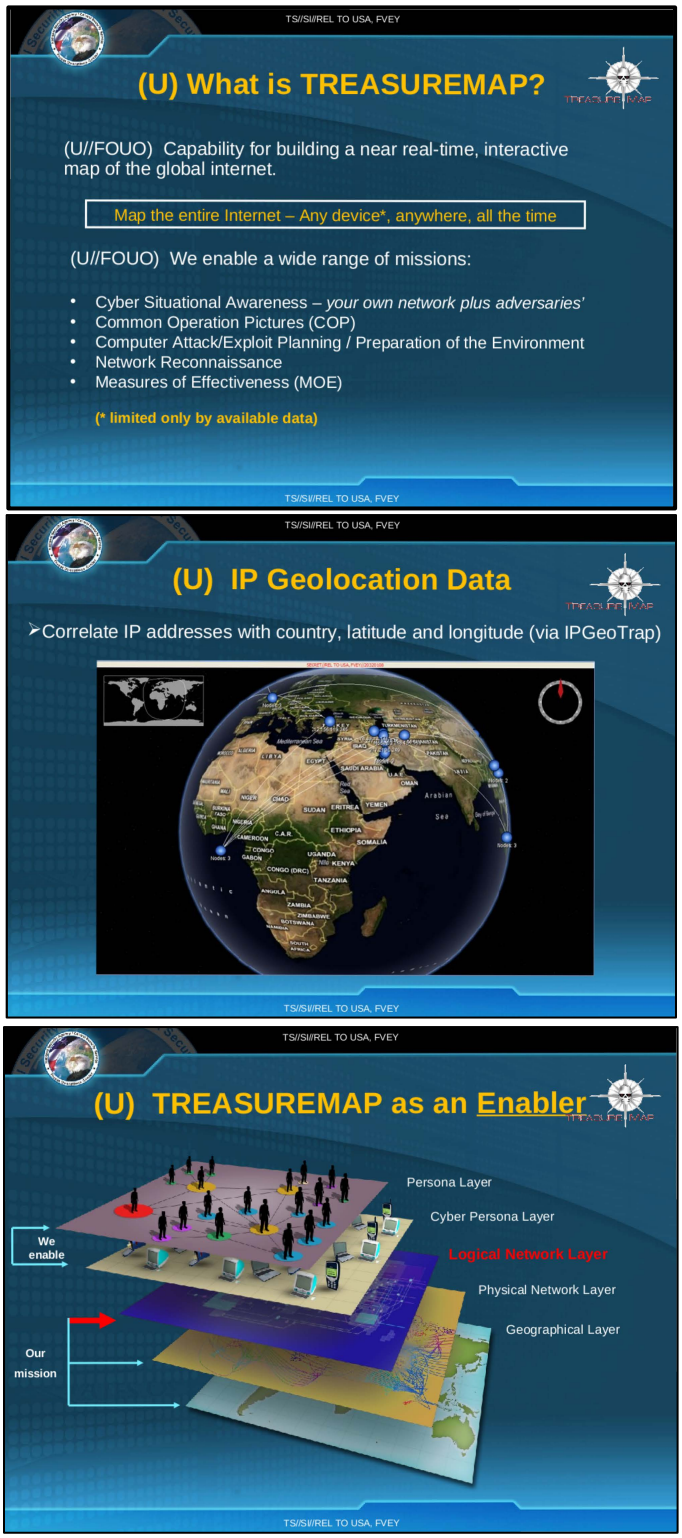


Figure 5.5 : TREASUREMAP, au-delà de Terminator
détails des diapositives reproduites (sources : Denny 2015; NSA 2010)

TREASUREMAP est un programme de cartographie d'Internet qui rappelle l'importance du concept d'espace dans le savoir de sécurité. L'organisation spatiale de la menace ne fait

d'ailleurs pas de doute dans le titre de la présentation PowerPoint : « bad guys are everywhere », seulement leur capacité à se cacher, et à infiltrer et imiter les normes sociales occidentales les rendent difficilement identifiables. TREASUREMAP cherche à résoudre une partie de ce problème, en rendant visibles les différentes interconnexions possibles ainsi que les lieux physiques et numériques de ses connexions. Or, la prétention de TREASUREMAP à pouvoir cartographier l'ensemble d'Internet et l'emphase que le programme et les cartes qu'il génère accordent à l'interconnectabilité dans sa méthodologie suggèrent un mode de représentation de l'espace relationnel supplantant à la fixité de la territorialité de l'État souverain.

Utilisant une multitude de sources d'information, il se présente comme un « [m]assive Internet mapping, exploration, and analysis engine » permettant de produire « a near real-time, interactive map of the global Internet » (NSA 2010, 3-4; voir aussi Risen & Poitras 2013; Müller-Maguhn et coll. 2014). L'objectif de TREASUREMAP n'est pas d'intercepter les communications. Il s'agit plutôt de cartographier Internet, de repérer les connexions qui composent les différents niveaux d'Internet et de les rendre intelligibles. « [TREASUREMAP] focus[es] on logical layers (router and autonomous system), but touches physical, data link, and application layers, » est-il écrit dans le document représenté par Denny, avant de conclure, anticipant le 45e président des États-Unis, « It's Huge » (NSA 2010, 5).

Les visées du programme sont ambitieuses, mais les moyens déployés aussi. En collectant des données de sources publiques, commerciales et issues d'opérations de surveillance des communications électroniques (« SIGINT ») — notamment à travers le programme frère PACKAGEDGOODS donnant accès à « 13 covered servers in unwitting data centers around the globe » — le programme déclarait, au moment de la création du document PowerPoint vers 2010, ajouter ou modifier plus de 30 gigaoctets de données chaque jour (NSA 2010). Concrètement, le programme cherche à cartographier les routes qu'empruntent les communications numériques pour recréer les niveaux des réseaux constitutifs d'Internet. Parmi les objectifs du programme se trouve celui de permettre (« We enable ») la reconstitution des réseaux d'individus et d'identifier les « bad guys », ceux qui apparaissent menaçants et doivent être interceptés (NSA 2010, 6). Pour ce faire, la NSA identifie les connexions entre les systèmes autonomes[2] (AS), c'est-à-dire les opérateurs de réseau qui se voient attribuer la charge de la répartition des adresses IP par les autorités Internet ;

[2] « autonomous system »

elle relève 16 à 18 millions de tracés de route de communication[3] ; et identifie de 30 à 50 millions d'adresses IP chaque jour. TREASUREMAP ingère en outre des données provenant de la pénétration de réseaux Wi-Fi et de l'identification d'informations de connexion à des réseaux privés, qu'il s'agisse de réseaux des fournisseurs de service conventionnels, de réseaux privés virtuels (« VPN : virtual private networks ») ou de réseaux anonymes comme TOR. TREASUREMAP collecte également des données de géolocalisation d'adresses IP (NSA 2010). Le type d'information reçu et cartographié par le programme est vaste, permettant aux analystes de la NSA de chercher autant des informations structurelles, telles que les systèmes autonomes, que des informations d'usager, telles que l'adresse MAC (« Media Access Control », ou adresse physique) qui identifie avec un code unique la carte réseau d'un appareil, ordinateur, téléphone ou autre.

Pour reprendre les mots de Denny, TREASUREMAP est « a Google Maps for the NSA » (Te Papa 2016b). Il reproduit l'œil de Dieu de Google en reproduisant la vision de l'espace et de la rue. TREASUREMAP offre ainsi une vue globale et détaillée d'Internet, une « 300,000 foot view of the Internet » et une « 300 foot view, router-to-router infrastructure » permettant de voir simultanément « the entire Internet » et « any device, anywhere, all the time » (NSA 2010, 9-10). La métaphore de la vision satellitaire reprise par le programme n'est pas fortuite, rappelant la relation fondatrice entre l'imagerie satellitaire du type Google Maps/Earth et le dispositif de sécurité. En effet, avant de devenir un produit commercial, l'imagerie satellitaire a été développée par les militaires américains et demeure encore aujourd'hui, malgré sa popularisation, en partie sous leur contrôle (Perkins & Dodge 2009, 547). Ainsi, la compagnie de cartographie géospatiale Keyhole qui a mis au point le format Keyhole Markup Language (KML) à la base des cartes Google était, avant son rachat par le géant californien, propriété du fonds d'investissement de la CIA et responsable de l'analyse des données du satellite de reconnaissance américain Keyhole-11 (Hu 2015, 127-129). Encore aujourd'hui, l'armée américaine conserve une forme de contrôle sur la production et la diffusion d'images satellitaires. La précision des images rendues publiques par Google est ainsi inférieure à celle des images accessibles aux militaires. Similairement, certains endroits classés n'apparaissent pas sur les cartes numériques (Marquez & Cançado 2010, 131; Perkins & Dodge 2009, 549).

[3] « traceroute »

La relation entre l'image satellitaire et le dispositif de sécurité ne peut toutefois se limiter aux rapports institutionnels entre Google et consorts et les militaires. Plusieurs ont noté la prétention à l'objectivité qui accompagne l'image satellitaire avec, pour effets, la naturalisation d'un espace politique inégal et l'effacement de la violence (Marquez & Cançado 2010; Hughes 2007; Kingsbury & Jones 2009). En ce sens, l'image satellitaire s'inscrit dans le même paradigme que la cartographie moderne à cette différence près que la première semble offrir une capture objective du réel sans l'intervention du sujet humain. Comme le proposent Wellington Cançado et Renata Marquez, la vision verticale, extérieure à la planète et au sujet voyant dont le regard est horizontal, offre le sentiment de pouvoir saisir l'entièreté de la Terre en un seul coup d'œil, et de pouvoir le faire sans intervention humaine. Ce faisant, la vision totale offerte par le satellite serait objective, non teintée par les biais du sujet. Ainsi semble-t-on avoir atteint le mimétisme parfait : la carte à l'échelle 1:1 (Marquez & Cançado 2010, 129-131). En plus de saisir objectivement le monde, la capacité de voir le monde dans sa totalité permettrait de voir ce qui demeure autrement invisible, masqué par l'horizontalité du regard ou les limitations de l'œil humain (Shim 2014, 157). En somme, écrit Rachel Hughes, « [r]epresentationally, GIS [geographical information systems] returns us to absolute (not relational) space, and promises an orgiastic fusion of geographical knowledge and territorial control » (Hughes 2007, 982). TREASUREMAP semble proposer cette vision similairement totale, précise et objective la planète numérique, sans ingérence humaine puisque la carte produite résulte de la façon dont le réseau prend acte de lui-même.

Pourtant, l'aura d'objectivité et de transparence qui accompagnent l'abstraction et le détachement de l'image satellitaire masquent des relations de pouvoir inhérentes à la production et à l'utilisation de cette image (Perkins & Dodge 2009, 547). « [T]he satellite's gaze is neither a neutral nor an objective view from nowhere — it is, of course, always a view from somewhere, » écrit David Shim. « In this regard, it is perhaps more accurate to note that it is also a view from someone » (Shim 2014, 154). L'image satellitaire, comme n'importe quelle photographie, fonctionne sur le mode de l'inclusion et de l'exclusion : elle cadre certains objets et en laisse d'autres à l'extérieur de l'image. Elle ajuste son niveau de précision d'image selon la zone ou l'objet. Dans le cadre d'une application comme Google Maps ou Google Earth, l'exclusion d'une ville ou région du monde du registre du visible peut prendre la forme de l'ajout d'un nuage numérique, d'une image ancienne ou encore d'une résolution imprécise. Inversement, certains espaces, comme la ville de New York, bénéficieront d'une précision d'image accrue, formant ainsi

« an irregular mosaic of the world » représentatifs des hiérarchies mondiales (Marquez & Cançado 2010, 129). Ce jeu dans le registre du visible et les relations de pouvoir qu'il met en œuvre est masqué par l'abstraction et la prétendue objectivité de l'image. Cela ne doit pas faire oublier l'importance de la visibilité dans l'organisation du pouvoir. « Satellite images are … always partial representations of space, even though they are (mistakenly) taken to provide 'a fuller view of space', » écrit Shim,

> (satellite) imaging rests upon an understanding of what is or is not entitled to representation, and how. So a satellite image is not simply an innocent mode of geographical depiction, but rather an interpretive response to what deserves to lie inside and outside of the satellite's field of vision (Shim 2014, 154).

Comme pour la cartographie moderne et la formation de l'État, l'image satellitaire n'est pas seulement représentative, mais elle est aussi performative, contribuant à forger la façon dont est conçu l'espace. Pour Shim, « satellite vision … shapes geographical imagination » (Shim 2014, 159).

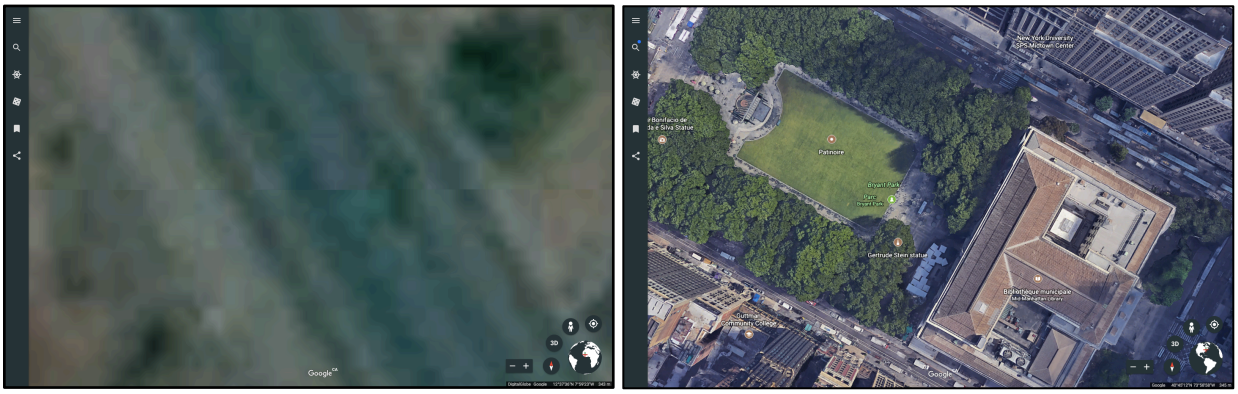
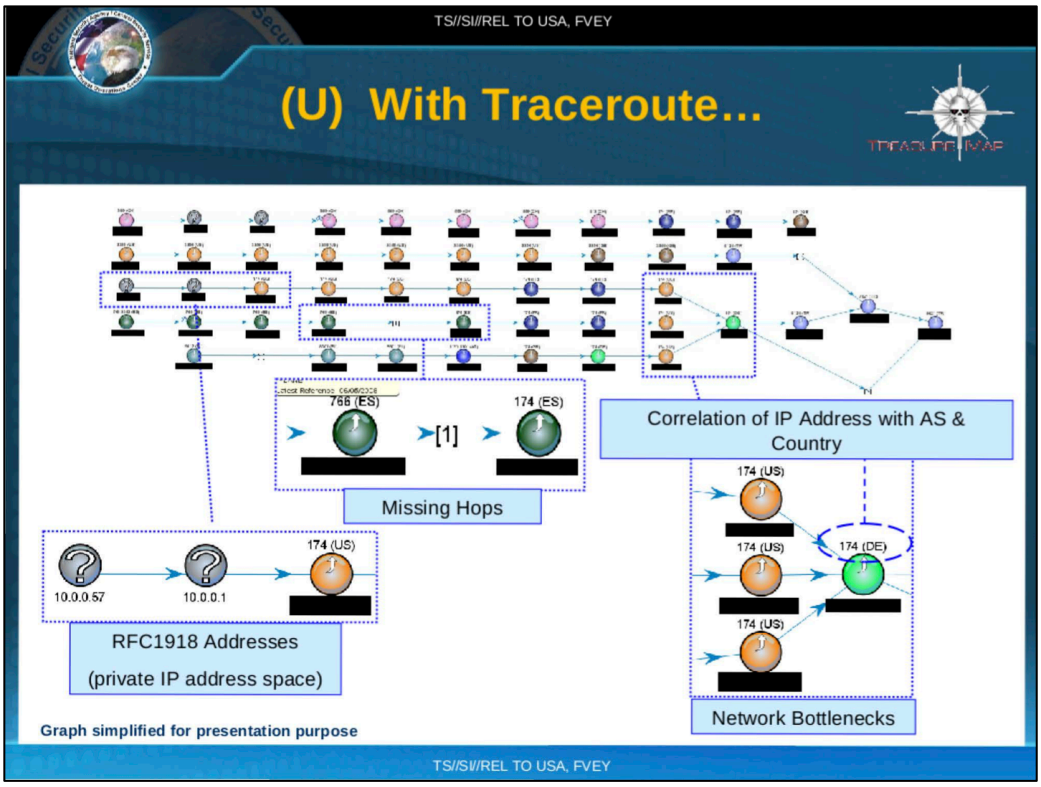
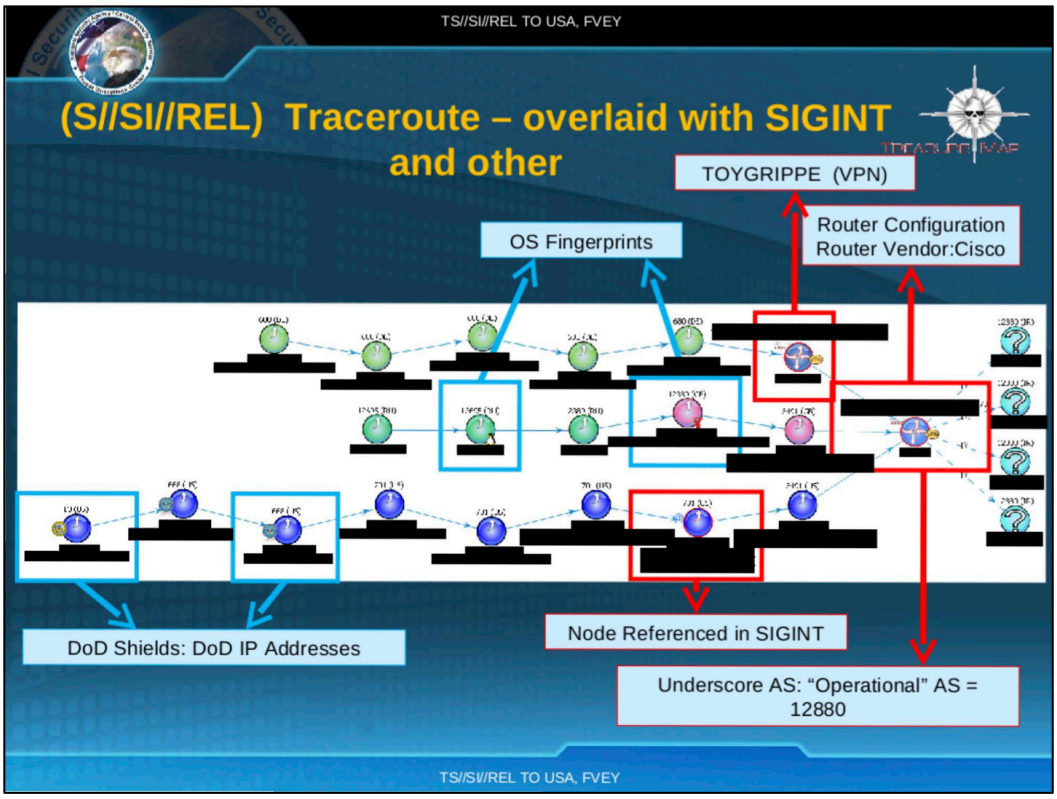


Figure 5.6 : Visibilité irrégulière et hiérarchie satellitaire
Bamako (Mali) et New York (États-Unis) à 340 mètres d'altitude (source : 2017a)

TREASUREMAP exploite les informations générées par les différents niveaux de réseau pour créer une base de données sur leur interconnectabilité, données d'autant plus « objectives » qu'elles sont issues des réseaux eux-mêmes et témoignent de la façon dont les réseaux conçoivent leur intelligibilité. Ces données sont ensuite visualisées à l'aide de cartes qui visualisent les nouvelles priorités de l'ère numérique : l'espace relationnel et la mobilité numérique au sein et entre les différents niveaux composant cet univers. TREASUREMAP propose une nouvelle géographie imposée par les infrastructures numériques qui ne se limite pas à la géographie des continents et à l'organisation du territoire, mais à la géographie des réseaux qui offre une voie

d'accès vers les utilisateurs. Elles rendent les lieux physiques et virtuels qui composent les différents réseaux visibles, identifient les infrastructures matérielles clés, établissent les points de convergence entre opérateurs de réseau (AS), entre les adresses IP, entre les noms de domaines, repèrent la géolocalisation de ces adresses, les goulots d'étranglement des réseaux (« network bottlenecks »), et, avec l'aide des programmes associés HYDROCASTLE et LEAKYFAUCET, les utilisateurs d'un réseau privé et ceux qui se connectent à un routeur Wi-Fi (NSA 2010). Ces cartes composent ce que les journalistes Andy Müller-Maguhn et Laura Poitras du Spiegel qualifient de « battlefield map for cyber warfare » (Müller-Maguhn et coll. 2014), rendant ce qui est stratégiquement significatif aux yeux de la NSA visible. Or, ce qui apparaît sur ces cartes horizontales ou en forme d'étoile, ce n'est pas la fixité du territoire national, mais le trait de l'interconnexion liant les réseaux. Pour paraphraser Shim, les cartes de TREASUREMAP façonnent l'imagination géographique au tour de la forme du réseau. Malgré des références géographiques et nationales, telles que les codes de couleur pour désigner les pays, ces cartes visualisent d'abord la fluidité numérique. Il ne reste, à l'instar des portulans de navigation ou des tables itinéraires médiévales, que les marqueurs de direction : de TELIANET, à PKTELECCM en passant par TTNETT. L'interconnectabilité des serveurs et appareils numériques remplace les détails de la côte.


TS//SI//REL TO USA, FVEY
(U) With Traceroute…
766 (ES)
[1]
174 (ES)
Missing Hops
Correlation of IP Address with AS & Country
174 (US)
174 (US)
174 (DE)
174 (US)
Network Bottlenecks
10.0.0.57
10.0.0.1
174 (US)
RFC1918 Addresses
(private IP address space)
Graph simplified for presentation purpose
TS//SI//REL TO USA, FVEY


TS//SI//REL TO USA, FVEY
(S//SI//REL) Traceroute – overlaid with SIGINT and other
TOYGRIPPE (VPN)
Router Configuration
Router Vendor:Cisco
OS Fingerprints
DoD Shields: DoD IP Addresses
Node Referenced in SIGINT
Underscore AS: "Operational" AS = 12880
TS//SI//REL TO USA, FVEY

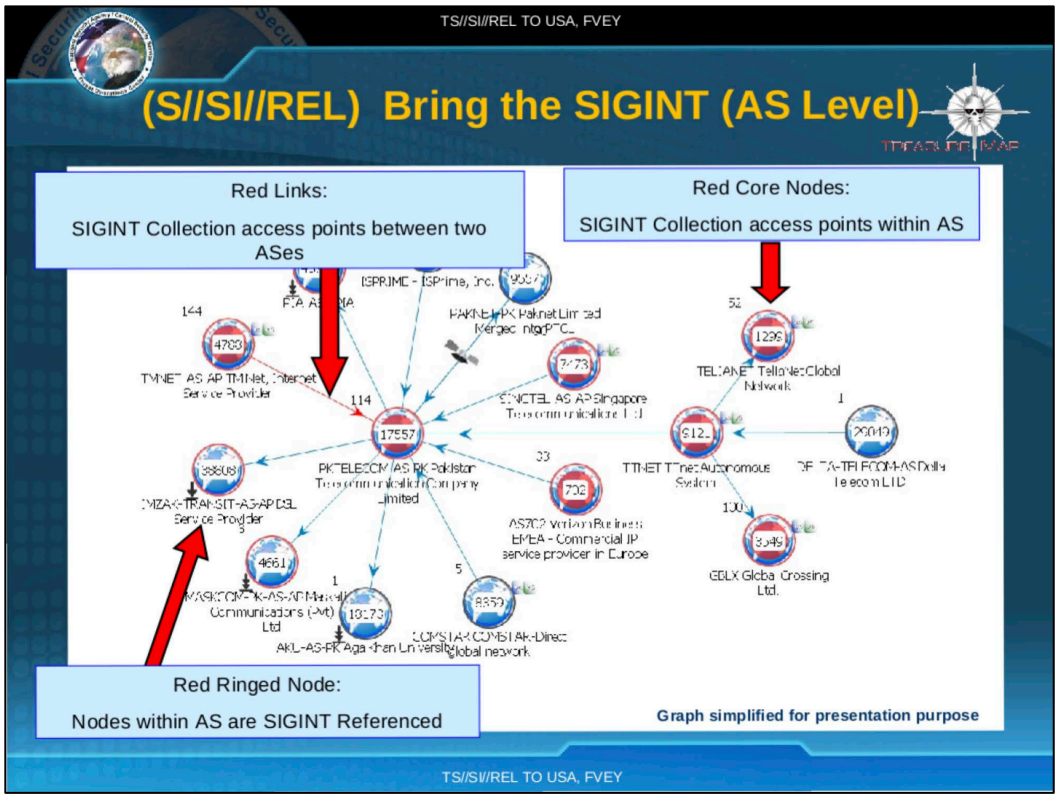


Figure 5.7 : Les réseaux de TREASUREMAP
cartographie du monde numérique et visibilité différenciée. En haut et au milieu, les routes horizontales d'une communication numérique, avec différentes catégories d'information collectée et exemples de pénétration de réseau (en rouge). En bas, les constellations d'opérateurs de réseau (AS), avec opération de surveillance (en rouge)(source : NSA 2010, 21-26)

TREASUREMAP offre ainsi un outil de visualisation qui permet à l'utilisateur des cartes de s'orienter dans une mer de données. À l'instar des Google Maps/Earth, ces cartes deviennent des plateformes de navigation reflétant, dans les mots de Sébastien Caquard,

> the dramatic transformation of the functions of maps on the internet. At a conceptual level, this navigational metaphor is replacing the conventional correspondence theory based on the illusory idea that maps should resemble as much as possible the territory and the phenomena mapped (Crampton, 2003; November et al., 2010). At a more concrete level, this metaphor reflects the growing role of maps in our daily lives. … Maps have recently become the main interface for accessing data over the internet (Ron, 2008). These maps are framing the way we interact with space and cyberspace (Caquard 2011, 138).

Avec TREASUREMAP, il ne s'agit plus de pouvoir établir une correspondance exacte entre les niveaux des réseaux de communication mondiale et leur géographie terrestre, mais de pouvoir chercher les données et les connexions pertinentes à partir d'une composante Internet. À l'instar du marketing et de la recherche sur Google Maps, TREASUREMAP fait de l'univers numérique une cible (Hu 2015, 129). Ainsi, si Google Maps propose des informations associées à un lieu —

commerces, services, et autres points d'intérêt — TREASUREMAP permet d'obtenir les informations de sécurité associées une composante de réseau — adresse IP, adresse MAC, opérateur de réseau (« AS »), etc. Les cartes issues de TREASUREMAP rendent ainsi visibles les points nodaux et les réseaux jugés importants. Les cartes de TREASUREMAP inscrivent les flux Internet dans une logique de mobilité de réseau liant dans une même dimension géographie, infrastructure, opérationnalisation des données, identités virtuelles et réelles. Ce faisant, elles brouillent les distinctions entre les différents niveaux qui composent les réseaux Internet et proposent un nouveau rapport à l'espace mettant à l'avant-plan l'élément relationnel. Si ces cartes ne font pas disparaître la fixité du territoire, elles semblent lui attribuer une fonction secondaire. La mobilité numérique ne se fait pas d'un territoire à un autre, mais d'un réseau à un autre grâce aux connexions permises par certains points névralgiques. La présence physique de ce réseau sur un territoire national est secondaire pour comprendre la mobilité numérique. Ainsi, la remarque sarcastique « Big deal » (NSA 2010, 21) accompagnant la mention d'un code de couleur pour les pays ne soulignerait-elle pas tellement la facilité ou la familiarité de ce paramètre, que sa désuétude, suggérant un nouveau rapport à l'espace qui ne se veut plus absolu et fixe, mais relationnel et fluide.

5.5 Connecter, connecter, connecter : la fièvre des réseaux atteint la NSA

Comme pour les cartes modernes, les cartes de TREASUREMAP sont performatives : elles confirment la centralité du réseau dans l'organisation spatiale de la sécurité en cette période d'âge d'or du renseignement électronique (« SIGINT »). Or, cette cartographie marque un changement tant dans la conception de l'espace et du territoire que de la façon dont ceux-ci doivent être contrôlés. La cartographie de l'espace numérique ne préconise plus tant l'occupation territoriale et la délimitation de frontières fixes, la sédentarité du politique pour reprendre l'expression de Mimi Sheller et John Urry (Sheller & Urry 2006, 208-209), que l'interconnectabilité, la présence de frontières souples et l'inégalité des mobilités conformément à la logique du réseau. Deleuze, retournant à Foucault et Virilio, entrevoyait déjà, dans Post-scriptum sur les sociétés de contrôle, le passage d'une société marquée par l'espace-clos vers une société marquée par des « formes ultra-rapides de contrôle à l'air libre » (Deleuze 1990). La fluidité, la rapidité et la permanence constituent, pour l'auteur, les mots-clés de cette forme de contrôle. « Les enfermements sont des *moules*, des moulages distincts, » écrit-il, « mais les contrôles sont une *modulation*, comme un

moulage auto-déformant qui changerait continûment, d'un instant à l'autre, ou comme un tamis dont les mailles changeraient d'un point à un autre » (Deleuze 1990), transformant du même coup la façon dont est conçu le savoir sur le monde et les outils pour y parvenir.

La cartographie de la NSA semble indiquer un passage vers ce contrôle à l'air libre. Cela ne signifie pas pour autant un rejet définitif de la territorialité étatique. Foucault mettait en garde contre l'idée de penser les rationalités de pouvoir — la souveraineté, la raison d'État et la gouvernementalité — en termes de succession ou de remplacement. L'auteur propose plutôt de porter attention à leurs chevauchements, l'un ne remplaçant pas nécessairement, en totalité et définitivement l'autre. La société de contrôle, malgré sa grande pertinence pour comprendre la politique de sécurité dans le monde numérique contemporain, ne doit pas masquer la présence et les mutations des autres rationalités de pouvoir. Si elle fait écho à la mobilité et à la déterritorialisation, il faut faire attention à ne pas sombrer, avertissent Sheller et Urry, dans le biais opposé à la sédentarité : le nomadisme, ou la célébration de la légèreté, de la fluidité et de la vitesse, sans prendre en compte ce qui est arrêté, fixe. (Sheller & Urry 2006, 210). « [A]ll mobilities entail specific often highly embedded and immobile infrastructures, » rappellent-ils (Sheller & Urry 2006, 210). L'univers numérique n'échappe pas à cette réalité. Si la communication mondiale est possible, c'est parce que les planchers océaniques sont sillonnés de câbles sous-marins immobiles, parce que le planisphère n'est pas vierge, mais découpé par des frontières internationales qui représentent autant de juridictions nationales. La mobilité et l'espace doivent se comprendre, suggèrent les auteurs, comme des systèmes « hybrides », rencontres entre mouvements, fixation, technologies et relations sociales.

> Thus there are hybrid systems, 'materialities and mobilities', that combine objects, technologies, and socialities, and out of those distinct places are produced and reproduced. … Places are thus not so much fixed as implicated within complex networks by which [individuals], buildings, objects, and machines are contingently brought together to produce certain performances in certain places at certain times. … Places are about relationships, about the placing of peoples, materials, images, and the systems of difference that they perform… We understand 'where' we are through "vision in motion" … practiced through the alignment of material objects, maps, images and a moving gaze (Sheller & Urry 2006, 214).

Certes, les infrastructures mondiales de communication jouent un rôle-clé dans l'architecture de surveillance, assurant à qui contrôle les principaux goulots d'étranglement entre les réseaux — points d'atterrissage des câbles sous-marins de fibre optique, points d'échange

Internet, centres de données — un accès privilégié aux données qui y circulent. En ce sens, la pertinence de la fixité du territoire et des infrastructures de communications ne disparaît pas, mais est complétée par la présence des réseaux numériques. Il est insuffisant de pouvoir tout collecter, il faut savoir quelles données chercher pour pouvoir repérer les réseaux terroristes. Dans la rationalité du réseau Internet, ce qui prime ce n'est pas le lieu géographique de la connexion, mais l'existence d'une connexion logique. La vitesse de circulation des données permet de contourner les culs-de-sac physiques. Ce recentrage dans la conception de l'espace vers le relationnel marque une distanciation de la vision par réseau par rapport à l'image satellitaire qui devait offrir, grâce à la projection de l'espace absolu, la quintessence de la cartographie de la souveraineté – le placage des frontières de l'État sur un territoire fixe assurant sans équivoque son appropriation d'une partie du sol terrestre (Hughes 2007, 982; voir aussi Leslie 2016, 170-173). Dans les cartes de TREASUREMAP, l'espace absolu laisse la place à l'espace relationnel, aux connexions entre les réseaux, aux façons dont ces connexions sont rendues possibles. Les réseaux écrivent leur propre géographie.

En tant qu'artefact de la production de savoir de sécurité par la NSA, TREASUREMAP participe à la construction de l'espace sécuritaire américain. Il fait apparaître en filigrane la nature du savoir mobilisée pour connaître et agir sur le monde, aux premières loges la recherche des lieux d'insécurité à travers les réseaux et le postulat de l'interconnectabilité des données et des individus. Le monde à surveiller est un monde qui se cache à l'intérieur de nos sociétés. Cette cartographie ne nie pas la persistance de l'État et du territoire, mais opérationnalise leur contournement à travers la logique du réseau. Mais, comme pour la cartographie médiévale et moderne, on ne saurait séparer la production de cartes par la NSA de son contexte épistémologique. TREASUREMAP s'inscrit dans cet exercice qui construit le monde et les différents niveaux composant Internet comme des espaces similaires, commensurables, où les données se connectent sans problème. En ce sens, le programme est une manifestation spatiale du désir de connexion à la base du savoir à l'ère des réseaux et des données de masse, de cette volonté de tout voir et de tout connecter. Aujourd'hui, relier les points est le mot d'ordre. Cela est possible par la mobilité des données, mais aussi par leur fluidité sémantique.

Avec son projet visant à cartographier chaque appareil et chaque connexion d'Internet, TREASUREMAP reproduit et renforce la vision du monde en réseau bien ancrée dans la culture numérique et, de plus en plus, dans la société occidentale en général. Dans son analyse du nuage

(« cloud ») comme organisation physique et métaphorique d'Internet, Tung-Hui Hu suggère l'impossibilité d'en dissocier les aspects matériels et idéationnels.

> [T]he network is always more than its digital or physical infrastructure. The network is primarily the idea that "everything is connected," and, as such, is a product of a system of belief. … Because reality can never match up to that system of belief, because, in fact, not everything is connected, the network exists primarily as a state of *desire.* ... The cloudlike nature of the network has much less to do with its structural or technological properties than the way that we perceive and understand it; seen properly, the cloud resides within us (Hu 2015, 10–11).

Certes, le réseau n'est pas nouveau. L'image du réseau interconnecté remonte au moins jusqu'à la menace nucléaire de la guerre froide. Il s'est imposé comme mythe fondateur d'Internet (Hu 2015, 5-9), puis après le 11 septembre pour comprendre la nébuleuse Al-Qaïda. De façon plus large, Hu suggère que le réseau s'est imposé comme modèle explicatif à travers l'ensemble de la société. Plus qu'un outil de communication, le nuage ou le réseau s'est constitué en idéal d'organisation sociale, contribuant à mouler à son image les identités individuelles et les relations sociales, la division du travail et la sécurité individuelle et nationale. Le réseau, constate Hu, a ainsi engendré une fièvre : « the desire to connect *all* networks, indeed, the desire to connect every piece of information to another piece » (Hu 2015, 11). Le modelage de la société selon les critères d'interconnectabilité distinguerait le réseau contemporain de ses itérations précédentes. TREASUREMAP, par sa volonté de cartographier l'entièreté d'Internet et l'interconnectabilité horizontale et verticale, est une performance de cette fièvre du réseau, à la fois produit et producteur de celle-ci : produit, car il est le résultat de l'ontologie de l'interconnectabilité entre tous les espaces géographiques, sociaux et numériques ; producteur, car il participe à la surveillance d'Internet et renforce la pertinence du modèle.

5.6 Spéculation paranoïaque : décontextualisation des données et création du savoir de sécurité

« [T]o construct a system of knowledge where everything is connected is, as psychoanalysis tells us, the sign of paranoia, » rappelle Hu (Hu 2015, 11). L'objectif de TREASUREMAP de cartographier l'entièreté d'Internet manifeste de la vision d'Internet comme étant un tout interconnecté : cet ensemble de réseaux aux connexions fluides, dont les frontières, même si elles sont toujours en expansion, demeurent finies. À l'image de la population irakienne devenue désormais objet de sécurité dans son ensemble et qu'on essaie de ficher afin d'avoir un portrait de

la menace en Irak (Hristova 2014; Bell 2015), Internet est un tout qu'il est possible de connaître entièrement. « You need the haystack to find the needle, » disait l'ancien directeur de la NSA, le général Alexander (Gellman & Soltani 2013a). Cette image en apparence banale est au contraire représentative d'une vision du monde où il n'y a plus d'espace extérieur, mais seulement un intérieur segmenté : une botte de foin dont il faut connaître chaque brin d'herbe et la façon dont ils se lient pour réussir à dénicher et exclure l'intrus. L'aiguille ne se cache pas à l'extérieur de la botte de foin, mais à l'intérieur, au vu et au su de tous.

Cette fièvre paranoïaque se nourrit de l'imagination d'une menace omniprésente, mais invisible qui justifie l'extension de la surveillance et du registre de la sécurité à l'ensemble du monde — « [e]verybody's a target; everybody with communication is a target » confiait un directeur supérieur du renseignement au journaliste James Bamford (Bamford 2012). La sécurité nationale du Homeland incite à l'intervention globale (Grondin 2010b) et à la surveillance de tous. Selon des données de novembre 2013, un million d'individus étaient inclus dans le Terrorist Identities Datamart Environment (TIDE), une base de données américaine regroupant des suspects potentiels, parmi lesquels 680 000 individus sont inclus à la liste de surveillance (« watchlist ») officiellement nommée la Terrorist Screening Database (TSDB), et 47 000 sont interdits de vol. Cela représente un ajout de 430 000 noms au registre TIDE depuis 2010. Toujours à titre de comparaison, en 2001, seulement 16 personnes étaient interdites de vol aux États-Unis (Scahill & Devereaux 2014). Cette extension de la sécurité se signale également par une réorientation de la surveillance vers l'intérieur des États-Unis, vers ses propres citoyens : le regard, jusqu'à maintenant dirigé essentiellement vers l'extérieur, se retourne vers l'intérieur des frontières nationales (Greenwald 2014; Cheney-Lippold 2016; Hu 2015, 85).

La fièvre paranoïaque du réseau montre l'extension horizontale et verticale de la menace et parallèlement de la surveillance : horizontalement, aucun espace géographique et social n'est exclu, verticalement, tous les individus jusque dans leurs moindres détails sont, ou sont potentiellement, soumis à la surveillance. Ainsi, une multitude de programmes ont été mis en place pour s'assurer de pouvoir collecter toutes les données produites mondialement. Dans cette opération de surveillance, aucun espace n'est épargné. Les échanges de courriel, la messagerie instantanée, les vidéos, les photos et les fichiers téléchargés, les communications par la voix sur les réseaux IP (VoIP), la navigation Internet, le transfert de données, les vidéoconférences, et les activités sur les médias sociaux sont collectés par PRISM et les programmes de surveillance en

amont (The Guardian 2013b). Les carnets d'adresses sont récupérés (Gellman & Soltani 2013a). Les images produites par les services de webcam de Yahoo! sont capturées par OPTICNERVE (Ackerman & Ball 2014). Les données cellulaires à travers le monde sont ciblées par AURORAGOLD et MYSTIC (Gallagher 2014; Devereaux, Greenwald & Poitras 2014; Gellman & Soltani 2014). Le réseau TOR est percé par FOXACID (J. Ball, Schneier & Greenwald 2013). L'univers des jeux vidéo, les Angry Birds, World of Warcraft, XboxLive et Second Life, est visé par la NSA et le GCHQ pour l'abondance des données qu'il produit ou parce que leurs plateformes numériques sont perçues comme de potentielles couvertures pour les comploteurs (J. Ball 2014; J. Ball 2013; Mazzetti & Elliott 2013). Aucun espace social n'est innocent, car la menace peut se trouver en tout lieu. « Bad guys are everywhere, » clame la présentation PowerPoint de TREASUREMAP. TREASUREMAP cartographie ce nouveau rapport à la menace en visualisant le postulat ontologique de cette extension : l'interconnectabilité ad infinitum.

Le postulat de l'interconnectabilité ne va cependant pas de soi. L'interconnectabilité verticale, notamment, pose problème dans le contexte numérique parce que la relation entre les composantes numériques et les supports physiques n'est pas toujours précise. Ainsi, si l'association entre les opérateurs de réseaux (AS) et les adresses IP est généralement précise, chaque opérateur cataloguant publiquement les adresses IP de son réseau, l'association parfaite entre les autres niveaux n'est pas si simple. Par exemple, les coordonnées géographiques des adresses IP sont souvent approximatives (McCann 2011). Remontant les niveaux d'interconnectabilité, l'association entre une identité numérique, caractérisée par les identifiants uniques d'un appareil, un nom d'utilisateur ou une adresse courriel par exemple, et un individu est tout aussi problématique comme le rappelle John Cheney-Lippold.

> When mediated through the technologies that compose the Internet, the identifiable citizen is recognizable. … An Internet protocol (IP) address, such as 93.45.225.191, is just a location for transmission control protocol packets to be sent to and from a device. A unique media access control address for a phone or computer, such as 00-50-5A-46-18-C1, is merely an identifier for network interface hardware. Neither has a political character, and neither is permanent; … User profiles, e-mail accounts, and even Facebook pages are all functionally disconnected from a singular, rights-bearing self (Cheney-Lippold 2016, 1722).

Ce problème d'identification a ainsi incité les grands joueurs de l'industrie numérique comme Facebook et Google à développer des témoins de connexion (« cookies ») parmi d'autres stratégies permettant d'établir des liens entre les différents appareils — téléphones intelligents et ordinateurs principalement — qu'un même utilisateur peut utiliser. L'objectif est d'abord commercial :

s'assurer de mieux connaître un utilisateur en réussissant à lier l'ensemble de sa navigation Internet afin de mieux cibler, en fonction de son profil d'utilisateur, les annonces qui lui seront présentées (Oremus 2014; T. Peterson 2014). La NSA, consciente du problème de la concordance entre un utilisateur et ses appareils, a trouvé un moyen pour s'attacher aux témoins de connexion de ces entreprises (Soltani, Peterson & Gellman 2013).

Toutefois, la difficulté d'associer un utilisateur et une identité numérique n'empêche pas le dispositif de sécurité américain d'agir, même lorsque des incertitudes demeurent quant à l'utilisateur. Ainsi, les États-Unis mènent-ils des assassinats menés par des drones contre des cibles terroristes sur la base d'informations numériques, c'est-à-dire que les informations permettant l'identification d'un terroriste sont majoritairement, sinon presque exclusivement, issues de données plutôt que de renseignements d'origine humaine. Ces données sont analysées et comparées à des modèles de comportement de terroriste afin de déterminer la « signature » terroriste de l'individu. Ainsi, selon un ancien pilote de drone du Joint Special Operation Commands interviewé sous couvert de l'anonymat par Jeremy Scahill et Glenn Greenwald pour le compte du site d'enquête The Intercept, la NSA « will develop a pattern where they understand that this is what this person's voice sounds like, this is who his friends are, this is who his commander is, this is who his subordinates are. And they put them into a matrix » (Scahill & Greenwald 2014). Dans ce contexte, explique Daniel Klaidman, une frappe de drone « requires no "target identification" but rather an identification of "groups of men who bear certain signatures, or defining characteristics associated with terrorist activity, but whose identities aren't known" » (Daniel Klaidman cité dans Cheney-Lippold 2017a, 39). Le terroriste est identifié à partir du savoir issu de l'opérationnalisation de ses données. À partir de là, « the use of targeted lethal force » pour reprendre les mots de la NSA est souvent guidé par d'autres données numériques : la géolocalisation d'un téléphone cellulaire associé au terroriste précédemment identifié. « After locating a target, usually by his cellphone or other electronics, » expliquent les journalistes Cora Currier et Peter Maass dans leur analyse des Drones Papers également révélés par The Intercept, « analysts would study video feeds from surveillance aircraft "to build near-certainty via identification of distinguishing physical characteristics" » (Currier & Maass 2015). Dans ce processus, l'association entre un appareil électronique et un utilisateur permet de passer outre l'identification hors de tout doute de la cible ; les deux niveaux de données deviennent

commensurables fusionnant le réel et le virtuel et assurant au dispositif de sécurité américain la possibilité d'agir sur le réel à partir de données numériques.

Malgré les incohérences et les victimes de l'interconnectabilité des données, le postulat demeure au cœur de l'opérationnalisation du savoir de sécurité. L'opérationnalisation des données de surveillance est défi pour la NSA et le dispositif de sécurité. D'autant plus qu'à l'abondance des données s'ajoute une autre difficulté : la nature des données issues de sources diverses qui n'ont souvent aucun lien direct avec un thème de sécurité. La NSA doit ainsi transformer cette masse informe en savoir de sécurité. La masse et la nature des données traitées par ou au profit de la NSA indiquent la présence d'un processus d'automatisation de traitement. Nécessaires pour parler la langue des données et accélérer la gestion de millions de données, il ne fait pas de doute que la NSA met à profit des algorithmes pour l'appuyer dans son travail d'analyse. À l'exception de l'algorithme mis au point pour le programme OPTICNERVE, peu de détails concrets sur leur nature ont filtré. Dans le cas de ce programme de surveillance, l'algorithme est élémentaire : il sert à exclure le contenu pornographique surabondant sur les services webcam de Yahoo! (Ackerman & Ball 2014). De la même manière que les détails techniques des algorithmes de Google et consorts demeurent secrets, protégés par la propriété intellectuelle, ceux de la NSA restent sous le scellé de la sécurité. Mais le secret de la compagnie californienne n'enlève rien à la réalité des effets de ces algorithmes. Il en va de même pour la NSA. La collecte et la connexion des données de masse demandent la présence d'algorithmes plus complexes permettant d'indexer et de stocker, puis de repérer et de relier des données, c'est-à-dire de catégoriser des comportements et d'établir des profils d'individu afin de déterminer, ultimement, si l'individu ainsi créé à partir de cette agrégation de données est un terroriste ou une menace à la stabilité nationale (Cheney-Lippold 2017a). Ce processus est répété chaque fois qu'un analyste fait une recherche ou qu'un programme signale une alerte en temps réel. L'algorithme, s'il demeure pour l'essentiel invisible, est crucial à l'entreprise de surveillance de la NSA.

Le recours aux algorithmes et aux données de masse, deux concepts à lire ensemble, par la NSA est lourd de conséquences. « Algorithms, » écrivent Louise Amoore et Rita Raley, « hold the promise of extending the threshold of human perception and cognition » (Amoore & Raley 2017, 2). Pour danah boyd et Kate Crawford, les données de masse auxquels sont associées les algorithmes sont un phénomène tant technologique que culturel

> that rests on the interplay of: (1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets. (2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims. (3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy (cité par Cheney-Lippold 2017a, 56).

Selon cette mythologie, la disponibilité de montagnes de données couplée à une puissance informatique accrue offre une nouvelle source de connaissance. À travers la reconnaissance de régularités et la détection d'anomalies, les algorithmes permettraient d'identifier des règles sociales et individuelles encore inconnues et inaccessibles sans les outils numériques. « Big data is … about understanding a new version of the world, one previously unavailable to us because in an antiquated era before digital computers and ubiquitous surveillance, we didn't have the breadth and memory to store it all » (Cheney-Lippold 2017a, 57).

En ce sens, la nouveauté du processus est indiscutable : sans ordinateur, le traitement d'une telle quantité de données est impossible. Plus fondamentalement, les données de masse suggèrent l'idée de pouvoir accéder à l'entièreté du contenu, comme TREASUREMAP et la botte de foin suggèrent la possibilité d'accéder à l'entièreté d'Internet, qui transforme la construction du savoir. Comme le propose Chris Anderson, ancien éditeur en chef du magazine Wired, l'arrivée des données de masse marque une nouvelle révolution scientifique : dorénavant, il n'est plus nécessaire d'établir des modèles à partir desquels des hypothèses sont proposées, testées et confirmées (ou infirmées). L'accès à la totalité à travers les données de masse, n=tout en terme statistique, propose Anderson, permet d'outrepasser la théorisation et l'élaboration d'hypothèses en offrant le savoir directement à qui sait utiliser adroitement les mathématiques appliquées.

> Sixty years ago, digital computers made information readable. Twenty years ago, the Internet made it reachable. Ten years ago, the first search engine crawlers made it a single database. Now Google and like-minded companies are sifting through the most measured age in history, treating this massive corpus as a laboratory of the human condition. They are the children of the Petabyte Age. … At the petabyte scale, information is not a matter of simple three—and four-dimensional taxonomy and order but of dimensionally agnostic statistics. It calls for an entirely different approach, one that requires us to lose the tether of data as something that can be visualized in its totality. It forces us to view data mathematically first and establish a context for it later (C. Anderson 2008).

Dès lors, pour Anderson, il ne s'agit pas de chercher la raison pour laquelle un événement se produit, mais partant de ces événements comme données, de les suivre et de les mesurer. « With

enough data, the numbers speak for themselves » (C. Anderson 2008). Dans ce contexte, il n'est pas pertinent de chercher à comprendre ou à trouver des causalités (dans la mesure où une telle chose est possible en science sociale), mais de laisser les données établir les corrélations nécessaires à l'avancement des sciences, peu importe que l'on soit capable ou non de les expliquer. « Petabytes allow us to say: "Correlation is enough…", » poursuit-il. « We can throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot » (C. Anderson 2008).

La mythologie des données de masse présente le savoir qui en est issu comme étant, enfin, objectif. Comme pour l'imagerie satellitaire, cette objectivité proviendrait du retrait du sujet humain du processus de production de savoir. Le savoir issu de l'analyse des données de masse par les algorithmes serait le résultat objectif de l'analyse de données elles-mêmes objectives. Cette objectivité est contestable. Contrairement aux croyances communes, les données ne sont pas des accès directs vers le réel. Comme l'écrit John Cheney-Lippold,

> Twentieth-century scientific positivism demands that we let data speak for itself. Following this mantra, wherever data tells us to go, we will find truth. But the data that Google uses to categorize people and assign status of identity does not speak; it is evaluated and ordered by a powerful corporation in order to avoid legal culpability. Indeed, scholars Lisa Gitelman and Virginia Jackson argue data doesn't speak but is spoken for. Data does not naturally appear in the wild. Rather, it is collected by humans, manipulated by researchers, and ultimately massaged by theoreticians to explain a phenomenon. Who speaks for data, then, wields the extraordinary power to frame how we come to understand ourselves and our place in the world (Cheney-Lippold 2017a, xiii).

Claudia Aradau et Tobias Blanke rappellent ainsi qu'il n'y a pas de consensus en science de l'information quant à la relation entre donnée et savoir, mettant en garde contre l'enthousiasme de la mythologie entourant les données de masse.

> Information scientists have indeed long argued that the imagination of data as 'discrete objects that can be located in time and space' or as 'raw numbers and facts' (Alavi and Leidner, 2001: 109) is fundamentally flawed. … Yet, they have also emphasized that data needs to be understood in the context of more fluid boundaries between data, information and knowledge (Aradau & Blanke 2015, 3).

Contre les discours optimistes, les auteurs avertissent que les données n'offrent pas d'accès direct à un savoir nouveau. Elles ne sont pas plus dénuées de sens. Pour les auteurs, ce serait une erreur de sous-estimer la valeur des méta/données comme le suggère le renseignement en défense de leurs pratiques de surveillance, ou au contraire de conclure que les données sont entièrement dépendantes

de leur interprétation. Plutôt, la fluidité entre les données, l'information et le savoir pousse à s'intéresser à la façon dont les données sont opérationnalisées (Aradau & Blanke 2015, 4).

Le contexte de sécurité occidental est marqué par la relation ambiguë qu'entretiennent les dispositifs de sécurité avec l'incertitude radicale et l'urgence d'agir (Amoore & Raley 2017, 2). Face à des menaces potentiellement catastrophiques, il devient nécessaire d'intervenir, comme le veut la devise de la NSA, pour défendre la nation et protéger le futur. Toutefois, la nature évasive des menaces pousse à la permanence des démarches de sécurité. Ben Anderson suggère que la sécurité est en fait impossible, néanmoins omniprésente. Pour être contrecarrées, les menaces doivent être imaginées et les mesures de sécurité continuellement réitérées. « Securing works … through the creation of supplements to the present — threats and promises, » explique l'auteur. « Hence the radical ambiguity of security. It can never be fully achieved. We can never be done with securing because it is dependent on invoking the future in a way that disrupts and opens up the here and now » (B. Anderson 2010, 229).

Par diverses pratiques d'invocation du futur, les professionnels de la gestion des inquiétudes, pour reprendre l'expression de Didier Bigo (Bigo 2005), projettent les peurs actuelles dans le futur (Amoore 2009a; Amoore 2013; de Goede 2008b; Aradau and Van Munster 2008). Ces peurs sont amplifiées par l'élaboration de scénarios de menace imaginant des événements catastrophes qui, dans le contexte d'incertitude radicale, pourraient se produire. L'objectif de ces pratiques créatrices n'est pas d'obtenir des prédictions justes du futur, mais de faire du présent un objet de contrôle par l'imagination de futurs possibles (Salter 2008a; B. Anderson 2010). Comme l'explique Amoore,

> [t]he pre-emptive deployment of data derivative does not seek to predict the future, as in systems of pattern recognition that track forward from past data, for example, because it is precisely indifferent to whether a particular event occurs or not. What matters instead is the capacity to act in the face of uncertainty, to render data *actionable* (Amoore 2011, 29).

Dans ce contexte, les algorithmes sont perçus comme une « computational capacity to act decisively and procedurally in the face of radical uncertainty » (Amoore & Raley 2017, 2). En organisant les données et en les présentant aux analystes à l'aide d'outils de visualisation, les algorithmes semblent offrir une lecture positiviste et objective du monde, à l'image de la cartographie satellitaire. Toutefois, les apparentes clarté et stabilité des algorithmes ne doivent pas masquer le fait que le processus créatif demeure central à leur fonctionnement. Non seulement le

travail d'imagination des menaces est-il à la base de la logique du risque, mais il transforme également les données collectées en données opérationnalisées en comblant les lacunes créées par les connexions incomplètes entre les données et en liant ces données aux scénarios existants (Amoore 2009b).

Malgré l'abondance des données collectées, la NSA doit travailler avec des données incomplètes, des zones d'ombre qui doivent être compensées. Ce travail de compensation est intégral à l'opérationnalisation des données, c'est-à-dire au processus de transformation de données diverses en savoir de sécurité à partir duquel il sera possible, pour les acteurs de sécurité, d'agir. La surveillance numérique réoriente des données de communication et des données commerciales vers les scénarios de risque. Dans ce processus d'opérationnalisation, les données sont décontextualisées : dissociées de leur origine, de leur histoire, pour être reconnectées à d'autres données puis introduites dans les scénarios de risque permettant d'évaluer les niveaux de menaces (Amoore 2011; Amoore 2014). « What is important about this process, » écrit Marieke de Goede, « is not so much the change of *context* in which the data are deployed, but rather the reinscription of meaning attributed to the data » (de Goede 2014, 101). L'inscription d'un sens de sécurité aux données se fait par l'agrégation des données. Les données deviennent opératoires à travers leur association avec d'autres données importantes ou jugées suspectes et leur projection dans un futur possible selon des lignes de fuite imaginées dans les scénarios de risque qui viennent combler les incertitudes. « What is the logic of this joining the dots… » demande Amoore ?

> It is an ontology of association, and it works according to association rules. Importantly … contemporary risk calculus does not seek a causal relationship between items of data, but works instead on and through the *relation* itself. The ontology of association does have a mathematical means of calculating uncertainty, an equation: if *** and ***, in association with ***, then ***. … Understood in this way, it is not strictly collected data that become an actionable security intervention, but a different kind of abstraction that is based precisely on an absence, on what is not known, on the very basis of uncertainty. … [T]he processes of data integration, mining and analytics draw into association an amalgam of disaggregated data, inferring across the gaps to derive a lively and alert new form of data derivative — a flag, map or score that will go on to live and act in the world (Amoore 2011, 27).

Le sens de sécurité des données n'est pas attribué à partir du contexte original des données, mais à travers leur résonance avec les inquiétudes et leur intégration dans les scénarios de menaces et les évaluations de risques. Amoore appelle le résultat de cette opérationnalisation des données, des données dérivées en référence aux produits financiers dérivés connus du public pour leur implication dans la crise financière de 2008. Ces produits financiers se démarquent des produits

conventionnels par le découpage et l'agrégation d'actifs réels et des risques associés de sorte que le produit dérivé final composé d'une multitude de couches d'actifs divers ne conserve qu'une connexion superficielle avec chaque actif. Ces produits dérivés sont ensuite échangés sur la base des caractéristiques de l'agrégat d'actifs sans que les actifs soient réellement affectés. « By 'slicing and dicing' and reaggregating underlying values, » écrit Amoore, « the financial instrument of the derivative thus sheds any encumbering causal relation to the underlying asset » (Amoore 2011, 28). L'auteur suggère que l'opérationnalisation des données en savoir de sécurité procède selon une logique similaire : « the data derivative is not centred on who we are, nor even on what our data says about us, but on what can be imagined and inferred about who we might be — on our very proclivities and potentialities » (Amoore 2011, 28). Dans ce contexte, « [w]hat is sought [in this manipulation of data], » explique Amoore, « is not the probable relationship between data on past activities and a future terrorist attack, but more specifically, a *potential* terrorist, a subject who is not yet fully in view, who may be unnamed and as yet unrecognizable » (Amoore 2014, 109). La surveillance numérique lie les données à cette catégorie imaginée de terroriste et recrée les individus afin de voir de quelle façon ils se conforment à celui-ci. Selon les résultats de cette catégorisation, les individus jugés suspects seront signalés et deviendront l'objet d'actions préemptives.

L'agrégation de ces données décontextualisées ne cherche pas à faire une reconstruction biographique des individus, mais à les catégoriser à partir de leur origine, de leur mobilité, de leurs connexions sociales, de leurs habitudes de consommation, de leur emploi, de leurs transactions financières, afin de déterminer leurs comportements futurs. Les données dérivées diminuent l'importance de la dichotomie entre contenu et métadonnée entretenue par les autorités pour justifier les pratiques de surveillance de la NSA. D'une part, comme le mentionnaient Aradau et Blanke, cette dichotomie est une construction sociale et en ce sens ne trouve pas d'écho en science de l'information (Aradau & Blanke 2015). D'autre part, dans un contexte d'association, ce que le dispositif de sécurité considère être des métadonnées, généralement définies comme les données sur les données, offrent des informations riches. À titre d'exemple, les métadonnées tirées de la navigation Internet seront le fournisseur de service Internet, les adresses IP de l'utilisateur et du site visité, l'activité de navigation comme la page visitée et l'heure de cette activité. Mais, ces métadonnées fourniront également des informations plus précises sur l'identité numérique de l'utilisateur lui-même : le système d'exploitation de l'appareil, la version du navigateur et certains

détails sur le type de matériel informatique comme le numéro d'identifiant unique de la carte réseau utilisée (adresse MAC). La diversité des activités numériques multiplie les informations et le type d'information disponible selon qu'il s'agit d'une connexion sur Facebook, d'un gazouillis, de l'envoi d'un courriel, d'un appel téléphonique, d'une recherche Google ou de la prise d'une photo, des activités fréquemment répétées (MacAskill & Dance 2013).

Citizen Ex de James Bridle, en proposant une reconstitution de notre citoyenneté algorithmique en fonction de notre navigation Internet, pointe également vers le pouvoir créatif des associations de données. Dans ce cas, Bridle, s'inspirant des travaux de John Cheney-Lippold, se penche sur l'opérationnalisation de la citoyenneté, concept juridique clé qui encadre les pratiques de surveillance de la NSA. En règle générale, la NSA n'est pas autorisée à surveiller les citoyens américains ou à procéder à des opérations de surveillance en sol américain. La NSA fait donc face au problème de l'identification du sujet de surveillance, problème d'autant plus aigu que l'identité de l'individu est masquée par l'appareil qu'il utilise pour communiquer sur Internet. Pour Cheney-Lippold, le dispositif de sécurité américaine procède à une redéfinition de la citoyenneté compatible avec les pratiques de surveillance de la NSA et l'opérationnalisation des données collectées. Ce faisant, il transforme la citoyenneté en objet de mesure. Le document interprétatif des pratiques de surveillance de la NSA en vertu de l'article 702 du FAA émis par le bureau du Procureur général, « Exhibit B: Procedures Used by the NSA in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended », définit la citoyenneté américaine ainsi :

> (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.
>
> (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person (cité par Cheney-Lippold 2016, 1727).

Cheney-Lippold voit dans ces deux définitions du citoyen américain le passage vers une citoyenneté non plus permanente, mais interprétée et fluide. La citoyenneté d'un individu est déterminée en fonction de sa position géographique dont la précision est toujours incertaine dans l'univers numérique, ou à la suite d'une évaluation des données de communication. Pour l'auteur,

le motif raisonnable plutôt que la certitude s'est établi comme fondement légal aux pratiques de surveillance de la NSA, transformant la citoyenneté en objet de calcul. Prenant au chiffre la proposition de Barton Gellman et Laura Poitras dans le Washington Post selon laquelle « the NSA instructed "analysts … [to] key in 'selectors' … that are designed to produce at least 51% confidence in a target's 'foreignness'" », Cheney-Lippold voit dans cette mesure probabiliste le nouveau standard de citoyenneté.

> The "51% confidence" standard is to *jus algorithmi* [algorithmic processing as a form of legal decision making] as blood quantum measurement is to *jus sangini* and a birth certificate is to *jus soli*. But unlike the materiality that articulates one's *sanginis* or *soli* belonging, like blood or birthplace, the materiality of *jus algorithmi* is a stream of data flowing through fiber-optic cables under the ocean and in the cloud server farms of companies such as Google. These data are then distributed into the dual frameworks of reasonable belief citizen or reasonable belief foreigner according to the NSA's algorithmic logic (Cheney-Lippold 2016, 1729).

Certes, les autorités contestent l'attribution d'une citoyenneté sur la base d'un calcul de probabilité. Dans son rapport sur les opérations de surveillance de la NSA conformément à l'article 702 du FAA, le Privacy and Civil Liberties Oversight Board écrit :

> The government has stated, and the Board's review has confirmed, that this is not a "51% to 49% test." If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting. While conflicting information must be resolved, the standard for making the foreignness determination is not a probable cause standard … [A] common understanding has been developed regarding what constitutes a sufficient basis for determining that a potential Section 702 target is a non-U.S. person reasonably believed to be located outside the United States. The NSA targeting procedures include a process for assessing non-U.S. person's status. This determination may not be made unless the analyst has first undertaken due diligence (PCLOB 2014, 44).

En suivant la définition commune et les procédures élaborées pour distinguer l'étranger du citoyen, la NSA aurait ainsi une note presque parfaite : une erreur d'identification aurait été commise dans seulement 0,4 % des cas (PCLOB 2014, 44). Si l'on se fie au nombre de personnes ciblées par la NSA en vertu de l'article 702 pour l'année 2016, information rendue publique dans un effort de transparence de la communauté du renseignement américain, cela représente néanmoins 4259 personnes, sur les 106 469 ciblées, erronément identifiées (ODNI 2017b).

Ce type de réponse offert par le PCLOB nous détourne toutefois de l'argument de Cheney-Lippold. L'auteur ne conteste pas la justesse de l'analyse de la NSA, mais relève le rôle

qu'occupent les algorithmes et l'opérationnalisation des données dans la transformation de la citoyenneté. Dans l'univers numérique, la citoyenneté est déterminée à partir de l'analyse de données produites par le réseau, malgré les imprécisions et déconnexions qui existent entre ces données et l'utilisateur réel. La présomption de l'interconnectabilité entre les niveaux constitutifs d'Internet permet de passer outre les possibles distorsions entre les mondes réels et numériques.

> Automated or not, the logic of *jus algorithmi* produces a new legal relation between people, their data, the U.S., and the concept of citizen. To phrase it differently, *jus algorithmi* is a formal, state-sanctioned enaction of citizenship that distributes political rights according to the NSA's interpretations of data. … *Jus algorithmi*'s logic enshrines this functional arbitrariness of citizenship—and its subsquent precarity—into an actionable legal standard (Cheney-Lippold 2016, 1729–1730).

Or, il est difficile de savoir exactement quelles variables sont prises en compte lorsque vient le temps de déterminer le statut de citoyen. Dans Citizen Ex, James Bridle a proposé ses propres spéculations qui s'avèrent, sans être nécessairement fausses, assurément incomplètes. Les deux documents interprétatifs des pratiques de surveillance de la NSA, « Exhibit B » et « Exhibit A: Procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended », offrent néanmoins quelques indices sur les données jugées pertinentes à l'opérationnalisation de la citoyenneté. Sachant qu'une communication est jugée pertinente si elle est associée à une puissance ou un territoire étranger (« foreign power or foreign territory »), les éléments pris en compte lorsque vient le moment de déterminer la pertinence des renseignements extérieurs de la surveillance (« foreign intelligence purpose of the Targeting ») offrent des indices intéressants sur la détermination du statut de citoyen. Ainsi, des informations indiquant que l'identifiant, l'adresse ou le compte de la communication électronique est utilisé par, ou a été utilisé par, ou a été révélé lors d'une communication avec une puissance ou un territoire étranger ou un individu relié à ceux-ci justifient la surveillance. De la même manière, des identifiants ou signatures électroniques, des signatures électroniques telles que la cryptographie et la sténographie, ainsi que des adresses IP associées à une puissance ou un territoire étranger justifient également la surveillance (Holder 2009, 5-6).

b. With respect to Internet communications:

- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the electronic communications account/address/ identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;
- Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Public Internet postings match the electronic communications account/address/ identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;
- Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or
- Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory, or are extensively used by individuals associated with a foreign power or foreign territory.

Figure 5.8 : Détermination du statut d'étranger
Exhibit A: Procedures Used by the NSA in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended: « Assessment of the Foreign Intelligence Purpose of the Targeting » (source : Holder 2009, 5-6)

Cheney-Lippold suggère que ces éléments, ainsi que la langue de la communication si l'on se fie au quotidien brésilien Globo, contribuent à déterminer le caractère étranger d'une communication ou d'un individu. Comme Google qui établit des profils à partir de la présence numérique d'un utilisateur, assignant une identité de genre, ethnique, de classe, d'intérêt, la NSA se rapporte à la visibilité numérique d'un individu pour désigner la citoyenneté. Dans l'absence de certitude sur l'identité de l'individu derrière une installation numérique, l'association avec ce qui

est extérieur aux États-Unis — un contact étranger, un échange de courriel avec un étranger, une adresse IP répertoriée, malgré toutes les imprécisions de ces repères territoriaux, hors du territoire américain, l'utilisation d'une langue autre que l'anglais — est marqueur d'étrangeté. En somme, est étranger ce qui s'associe avec l'extérieur, créant du coup une citoyenneté algorithmique sur la base d'une division nette entre les attributs intérieurs et extérieurs. « The resulting inverse of the ideal foreigner—the ideal citizen—is a user who never calls, e-mails, or makes it into the address book of another user who is a foreigner; never travels outside the United States; and speaks exclusively English, to other English speakers, without encryption, » résume ainsi Cheney-Lippold (Cheney-Lippold 2016, 1731). Face aux difficultés de soumettre les pratiques de surveillance numérique, rendues possibles grâce à une mobilité qui cadre mal avec les divisions légales traditionnelles elles-mêmes basées sur une territorialité fixe, la NSA force cohérence entre deux réalités dont la commensurabilité n'est pas évidente. Pour ce faire, elle joue avec la malléabilité du droit et des données. « The algorithmic citizenship of *jus algoritmi* is a citizenship of technical requirement, one that can neither be intentionally practiced nor remain functionally stable, » propose Cheney-Lippold.

> Jus algoritmi is instead a dynamic, temporal interpretation, similar to what Johanna Drucker and Bethany Nowviskie (2004) describe as "speculative computing," which "suggests that the concrete be replaced by plasticine that remains malleable, receptive to the trace of interpretive moves" (p. 433) (Cheney-Lippold 2016, 1723).

L'opérationnalisation renforce le pouvoir d'interprétation des données collectées de la NSA. Libérée par la décontextualisation et l'agrégation des données, la NSA, et à travers elle le dispositif de sécurité avec qui elle partage les informations, devient une spectatrice émancipée pour reprendre l'expression de Jacques Rancière. Être spectateur n'est pas un geste passif, suggère l'auteur. Au contraire, cela implique un travail d'interprétation continuel et de mise en relation avec le savoir actuel.

> Le pouvoir commun aux spectateurs ne tient pas à leur qualité de membres d'un corps collectif ou à quelque forme spécifique d'interactivité. C'est le pouvoir qu'a chacun ou chacune de traduire à sa manière ce qu'il ou elle perçoit, de le lier à l'aventure intellectuelle singulière qui les rend semblables à tout autre pour autant que cette aventure ne ressemble à aucune autre. … C'est dans ce pouvoir d'associer et de dissocier que réside l'émancipation du spectateur, c'est-à-dire l'émancipation de chacun de nous comme spectateur. Être spectateur n'est pas la condition passive qu'il nous faudrait changer en activité. C'est notre situation normale. Nous apprenons et nous enseignons, nous agissons et nous connaissons aussi en spectateurs qui lient à tout instant ce qu'ils voient à ce qu'ils ont vu et dit, fait et rêvé (Rancière 2008, 23).

Pour Rancière, le spectateur émancipé permet de contester la division entre sujets connaisseurs et ignorants. Nous sommes tous égaux face au savoir, partageant un même processus d'apprentissage à travers l'interprétation du monde et l'association des choses inconnues avec d'autres choses connues. En ce sens, l'interprétation et l'association font partie d'un processus normal d'apprentissage et d'attribution de sens. Pour cette raison, il faut cesser de présumer de l'effet d'une œuvre ou d'un texte pour chercher à connaître de quelle façon les autres, non seulement les instruits, construisent le monde. « L'effet de l'idiome ne peut être anticipé, » écrit Rancière. « Il demande des spectateurs qui jouent le rôle d'interprètes actifs, qui élaborent leur propre traduction pour s'approprier l'"histoire" et en faire leur histoire » (Rancière 2008, 28-29).

Rancière contesterait probablement le détournement de son concept esthétique, pensé comme vecteur de contestation sociale, pour l'analyse de l'opérationnalisation du savoir de sécurité. La position de pouvoir de la NSA n'a pas à être rappelée ou défendue. Dans le contexte de la visibilité numérique, la NSA est dans une position privilégiée de non-réciprocité : elle peut voir sans être vue. Le concept de Rancière demeure pertinent néanmoins, rappelant la mort de l'auteur et normalisant l'interprétation d'un texte ou d'une pièce de théâtre. L'autonomie du texte se combine à celle des spectateurs qui donnent un sens au monde et le conteste à travers des associations et dissociations d'idées, de concepts ou de savoir-faire. Or, dans le cas présent, le texte est constitué de données. Les données, une fois produites, se détachent de leur référent pour acquérir une vie autonome et permettent à la NSA de réinterpréter les performances des individus surveillés à la lumière de ses propres connaissances du monde. La NSA, interprète active, élabore sa propre traduction des données pour en faire son histoire, son savoir de sécurité.

Cette normalisation du processus d'opérationnalisation et d'interprétation de la NSA n'est pas une banalisation des pratiques de surveillance. Au contraire, elle permet d'accentuer la particularité de la démarche de sécurité. Dans le monde des données de masse, l'interprétation créative des données à travers les algorithmes est la norme plutôt que l'exception (Cheney-Lippold 2017a). De la même manière que le risque est étroitement lié à la logique économique. Ce qui distingue toutefois la NSA comme spectateur, c'est la peur de l'autre et la souveraineté de son regard qui conditionne sa reconstruction du monde.

5.7 Sécurité *über alles* : l'extension du regard souverain et l'exclusion de l'autre

Le processus d'opérationnalisation du savoir de sécurité se poursuit selon une logique paranoïaque et souveraine qui tend vers l'extension continuelle du spectre de la surveillance et la recherche de l'ennemi à abattre. Déjà, la définition des objectifs de sécurité nationale de la communauté du renseignement américain est large et inclusive favorisant l'extension de la surveillance. Ainsi, dans les mots du PCLOB :

> Foreign intelligence information concerning non-U.S. persons is defined in FISA as information that relates to the ability of the United States to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power. Foreign intelligence information concerning non-U.S. persons is also defined as information that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power (such as international terrorist groups or foreign governments) or foreign territory. The term "foreign territory" is undefined by the statute (PCLOB 2014, 27-28).

Comme le souligne Greenwald, cette définition est suffisamment permissive pour justifier la surveillance du secrétaire général de l'ONU, de la présidente brésilienne et la chancelière allemande et du renseignement économique (Greenwald 2014, 135-147). Le flou entourant la figure de ces terroristes se cachant au vu et au su de tous, ces « underspecified enemies » pour reprendre l'expression de William Connolly (cité par Amoore 2009a, 50), accentue en outre l'extension verticale et horizontale des pratiques de surveillance. La peur de l'événement catastrophique et la logique sécuritaire voyant la solution aux risques dans l'établissement paranoïaque de connexions, couplées au mythe entourant les algorithmes et les données de masse, nourrissent l'appétit insatiable des dispositifs de sécurité occidentaux pour les données avec pour conséquence de généraliser le soupçon. « [T]oday the normal relationship between the state and its citizens, » écrit Agamben, « is defined by suspicion, police filing and control. The unspoken principle which rules our society can be stated like that: *every citizen is a potential terrorist* » (Agamben 2013).

Dans le contexte où la menace est inconnue et potentiellement catastrophique, les dispositifs de sécurité américain et occidentaux ont adopté une approche managériale du risque afin d'assurer la continuité des flots économiques tout en diminuant les risques de déstabilisation à l'ordre politique actuel et en préparant les divers acteurs de la société à faire preuve de résiliente advenant

un événement déplorable (Adey & Anderson 2012; Amoore & de Goede 2008b; Collier & Lakoff 2007; Aradau & Van Munster 2007; Monahan 2006b; Dunn Cavelty, Kaufmann & Soby Kristensen 2015; Corry 2014). Dans ce processus, les dispositifs de sécurité ont déterminé des catégories de population et d'activité les plus susceptibles de devenir source de déstabilisation. La précision des technologies de collecte et d'analyse de données permet de mener une « gouvernance ciblée », plutôt qu'une gouvernance de masse, de la population, réduisant tant les risques que les obstructions au bon fonctionnement de la société (Amoore & de Goede 2005; Valverde & Mopas 2004). Les attentats du 11 septembre 2001 ont également amené le dispositif de sécurité américain à étendre sa sphère d'intervention afin de protéger le Homeland à distance. « [The] desire to resecure the "homeland", » écrit David Grondin, « has effectively established new frontiers… not simply the territorial borders of the homeland, but infinite boundaries of the homeland » (Grondin 2010b) portant la sécurité américaine au niveau global et engendrant une dynamique de dé/re/territorialisation. Cette extension du Homeland américain a été analysée, en parallèle au déploiement de la mondialisation néolibérale, comme une forme de « pacification » des populations, une biopolitique devant régulant et maximiser la bonne vie libérale (Grondin 2010b; voir aussi Dillon & Reid 2001; Reid 2006; Hardt & Negri 2000; Duffield 2010a). Plusieurs ont soulevé la nature conservatrice et discriminante de ces changements où la stabilité sociale rime avec néolibéralisme et où la menace est majoritairement associée à la figure de l'autre : arabo-musulman, noir, sud-américain, pauvre... (Amoore 2007; Aradau & Van Munster 2008; Amoore 2009b; Monahan 2010). TREASUREMAP, et la surveillance de la NSA plus généralement, ne font pas exception à cette rationalité. Ils s'inscrivent en continuité avec la logique du risque, mais aussi avec celle du réseau. C'est à travers la rationalité de l'interconnectabilité distinctive de l'épistémologie du réseau que la NSA attribue un sens aux données collectées.

Pour Michael J. Shapiro, l'état de la surveillance actuelle nous projette dans la science-fiction, dans un monde digne du film Minority Report du réalisateur Steven Spielberg. Le film raconte l'histoire de John Anderton (Tom Cruise), inspecteur responsable d'une unité de préemption des crimes. Accusé à tort d'un crime qu'il ne commettra pas, il est pris en filature par son ancienne équipe. Pour l'auteur, le sentiment de suspicion qui habite le film et l'objectivité attribuée aux rapports de précrime offrent une image saisissante de la sécurisation des sociétés occidentales contemporaines. « *Minority Report* … displays a coercive society-wide securitization …, » écrit Shapiro.

> That securitization is effectively an imposition of a 'peace' that stifles all forms of dissonance… With its form as well as its content, Steven Spielberg's film version of the story provides the most notable representation of a contemporary politics of surveillance (Shapiro 2013, 96–97).

Shapiro associe cette sécurisation au concept de microfascisme de Deleuze. « [W]hen fascism is interpreted as a *dispositif* — a complex, coercive apparatus — rather than merely as a mentality, we are in a position to appreciate its insidious effects on the social order — its war against difference in the name of social peace » (Shapiro 2013, 98). Ce qui distingue le fascisme, c'est la peur qui envahit l'entièreté des relations sociales faisant de la sécurité le seul objectif politique et de la guerre un instrument de gestion de la société.

> The new fascism is not the politics and the economy of war. It is the global agreement on security, on the maintenance of peace — just as terrifying as war. All our petty fears will be organized in concert, all our petty anxieties will be harnessed to make micro-fascists of us; we will be called upon to stifle every little thing, every suspicious face, every dissonant voice, in our streets, in our neighborhoods, in our local theaters (Deleuze cité par Shapiro 2013, 86).

La relation entre la peur, la sécurité et la guerre montre le refus de la contingence du fascisme : les différences sont niées et le monde, décliné suivant un narratif unique, cohérent et organique.

Compte tenu de son poids historique et éthique, l'utilisation du terme fascisme est toujours inquiétante, souvent le résultat de surenchère rhétorique. Il faut néanmoins reconnaître avec Shapiro l'exploitation de la peur du terrorisme pour combattre, par l'extension de la sécurité nationale à toutes les sauces, la différence. Benjamin J. Muller propose un constat similaire :

> [g]overned by a desire to try and anticipate all threats, prevent and preempt dangers, and securitize everything, contemporary impulses to surveil everything are connected to visions of an overwhelming proliferation of threats and dangers [and supported by m]oves to securitize nearly all forms of mobility and otherness (Muller 2014).

La place centrale qu'occupe la peur de l'autre dans les pratiques de surveillance et la sécurisation à tout vent devrait inciter à la prudence lorsque l'on suggère que la surveillance de la NSA est indiscriminée. Certes, elle filtre toutes les données mises à sa disposition à la recherche de quelque 90 000 sélecteurs si l'on en croit les informations publiées sur le site Internet IC on the Record du Bureau du directeur du renseignement national (Office of the Director of National Intelligence) des États-Unis. En ce sens, pour les cibles qu'elle identifie, la NSA possède les moyens de collecter les données en masse. Nous ne sommes néanmoins pas tous des cibles. Son attention n'est pas également répartie.

En effet, nous ne sommes pas tous égaux face à la surveillance. L'indétermination de la menace alimente la vigilance, une vigilance biaisée par la peur de la différence et les stéréotypes et dé/formant la catégorisation des terroristes potentiels (Amoore 2007). Dans le contexte de la peur du terrorisme islamique, c'est sans grande surprise de voir les références religieuses sonner l'alarme. Ainsi dans une enquête du FBI intitulé « Indicators of Mobilization to Violence » proposant, à travers une liste de questions, une méthode statistique permettant d'attribuer une série de notes sur 100 quant au niveau de radicalisation ou de mobilisation des individus, plusieurs questions font référence à la religion et à l'islam plus spécifiquement. « While the survey is, in theory, meant to be universal, » écrivent Cora Currier et Murtaza Hussain, journalistes pour The Intercept, « it contains several references to Islamic terminology and seems to be focused on concerns about Muslim terrorism » (Currier & Hussain 2017). Au côté des questions sur l'accès à des armes ou à un entraînement au port d'armes, se trouvent des questions sur l'association à des groupes extrémistes, sur le statut marital, médical et criminel des individus ainsi que sur leur point de vue au sujet de la justification religieuse de la violence, leur volonté de poursuivre le jihad ou leur allégeance à un leader islamique promouvant la violence (voir le document rendu public par Currier & Hussain 2017). La volonté affichée du président Trump de renommer et réorienter le programme antiterrorisme Countering Violent Extremism pour Countering Islamic Extremism montre également le biais religieux des pratiques sécuritaires aux États-Unis (Ainsley, Volz & Cooke 2017). Dans le même ordre d'idée, les cinq villes américaines où habitent le plus de personnes inscrites à la liste de surveillance (« watchlist ») antiterroriste américaine sont New York, Houston, San Diego et Chicago. À travers ces agglomérations de plus d'un million d'habitants s'insère la petite municipalité de Dearborn, Michigan, comptabilisant moins de 100 000 âmes. Dearborn, qui se classe deuxième à ce palmarès, se distingue des précédentes par une importante population de confession musulmane, ainsi qu'une population à 40 % arabe (Scahill & Devereaux 2014).

Comme il a été question précédemment, le processus d'imagination des scénarios de risque ne cherche pas à prévoir le futur avec précision. « [P]remediation [as Richard Grusin names this process] … is not necessarily about *getting the future right* as much as it is about trying to imagine or map out as many possible futures as could plausibly be imagined, » suggère Grusin (cité dans de Goede 2008b, 159). Ces futurs possibles deviennent la fondation pour des interventions dans le présent. Or, pour Marieke de Goede, ce processus créatif est problématique notamment parce qu'il

efface, sous l'apparente objectivité des programmes, mesures et autres algorithmes, le caractère politique de ces scénarios.

> Perhaps precisely because of its ability to foster current action, we could argue that premediation has *itself* become the catastrophe (Coutin, 2008). Not only does security premediation offer a fantasy of control and rational management of the uncertain future that 'depoliticises the limits of knowledge' (Best, 2006: 13–14); more worrying still is the fact that premediation is performative. This does not mean that disastrous imagined futures will inevitably play out, but it does mean that the imagination of some scenarios over others, the visualization of some futures and not others, entails profoundly political work that enables and constrains political decisionmaking in the present (de Goede 2008b, 171).

Les algorithmes accentuent cette dépolitisation. Comme le relève Amoore, les algorithmes utilisés pour associer et visualiser les risques normalisent les biais existant dans les scénarios (Amoore 2009b, 19-20). Dans le traitement et la visualisation des données, les algorithmes renforcent l'importance des catégories prédéterminées de risque, laissant à l'extérieur du cadre de visibilité les autres données collectées, au risque de sombrer dans une logique circulaire. Ils vont ainsi attirer toute l'attention sur certains détails décontextualisés, par exemple un voyage à la frontière du Pakistan et de l'Afghanistan, qui vient valider l'existence du scénario.

> In effect, algorithms precisely function as a means of directing and disciplining attention, focusing on specific points and cancelling out all other data, appearing to make it possible to translate *probable* associations between people or objects into *actionable* security decisions… In this sense, the algorithm produces a screened visualization of suspicion, on the basis of which 'other' people are intercepted, detained, stopped and searched (Amoore 2009b, 22).

Les algorithmes, explique Amoore, ne permettent pas d'identifier de nouvelles menaces, mais confirment les scénarios actuels en visualisant les peurs et les préjugés inscrits dans ces scénarios. Ce processus d'opérationnalisation des données participe à la normalisation des sociétés occidentales en passant outre les corps et les comportements « normaux » pour mettre l'emphase que sur les déviances à la norme. En parallèle à cette marginalisation accrue de populations souvent déjà reléguées aux recoins des sociétés occidentales, la projection de lignes de fuite remplace les corps réels par des corps numériques dans lesquels l'anormalité est naturalisée, une anormalité d'autant plus difficile à contester que les données agrégées permettant la production de ce corps ne sont pas accessibles (Amoore 2009b, 21-23).

Le recours à un monde imaginé n'est pas entièrement irrationnel dans la mesure où les attentats du 11 septembre 2001 ont prouvé que l'on ne peut plus se fier à ce que l'on voit. Les

terroristes se cachent parmi la population, au vu et au su de tous, feignant la normalité. Cependant, cela ne se fait pas sans accroc. L'opérationnalisation des données afin de pouvoir les introduire dans les scénarios contraint le dispositif de sécurité à voir uniquement ces scénarios imaginés qui réapparaissent dans les algorithmes (Amoore 2009b; Amoore 2011). Ces scénarios se transforment en prophéties autorévélatrices qui ne peuvent être démenties puisque le risque ou l'événement déstabilisateur peut toujours subvenir dans un contexte d'incertitude radicale. Cette opérationnalisation du savoir de sécurité accentue un sentiment d'insécurité permanent et ce fait aux dépens de l'exclusion de populations importantes. « Premediation, » explique de Goede, « has the ability to foster societal fragilities and resentment, while disregarding its present victims as 'collateral damage' » (de Goede 2008b, 171). Les victimes représentent les risques potentiels qui ne se sont pas encore produits. Dans ce contexte, elles ne sont jamais lavées de tout soupçon. Cela explique l'obligation grandissante de localisation, le devoir investi dans chaque sujet de la surveillance d'être toujours localisable physiquement ou numériquement comme le propose TREASUREMAP (Amoore 2009a).

La sécurisation à tout vent des sphères sociales participe au processus de la normalisation des pratiques d'exception qui, dans une lecture schmittienne du politique, ramène au concept de souveraineté (Agamben 1998; Huysmans 2006; Aradau 2008; Aradau & Van Munster 2008; Edkins, Pin-Fat & Shapiro 2004; W. Brown 2010; Walker 2006; M. C. Williams 2003; Schmitt 1988). Pour Carl Schmitt, le souverain est celui qui détermine l'exception, qui suspend la loi et identifie l'ennemi de la nation. D'une part, la souveraineté est étroitement liée à la délimitation du territoire sur lequel il a pleine autorité et autonomie. Retournant aux textes du philosophe, Wendy Brown suggère en effet que

> [f]or Schmitt, "land appropriation is the primary legal title that underlies all subsequent law." It "constitutes the original spatial order, the source of all further concrete order and all further law."… There is first the enclosure and then the sovereign. Or, put the other way around, it is through the walling off of space from the common that sovereignty is born (W. Brown 2010, 45).

Que la question du territoire dans la discussion sur la souveraineté soit délaissée au profit de l'autorité ne doit pas faire oublier le rôle fondationnel de la clôture. D'autre part, ce pouvoir décisionnel est autonome, au-dessus de toute norme ou tout code législatif. Il est l'expression de l'autorité du politique. Wendy Brown explique :

> The sovereignty of the political proceeds from its purview over the life-and-death matter of the friend-enemy relation and more precisely from two facts: One the one hand, life is at stake, while on the other, there can be no norm to decide on or about the enemy. … [T]his decision … necessarily rests outside whatever norms bind the polity, even as it may pertain to protecting the way of life these norms govern and bind (W. Brown 2010, 55).

Si les idées de Schmitt sont souvent décriées pour leur antilibéralisme, Brown suggère au contraire une similitude d'esprit avec les thèses contractualistes qui voient dans le contrat social la naissance temporelle et spatiale de la souveraineté politique et suggère la primauté du politique face à l'économie et à la religion. Pour l'auteur, cette proximité permet de relativiser la portée du pouvoir décisionnel du souverain et de l'autonomie du politique suggérée par Schmitt. La souveraineté schmittienne serait « aspirational, ideological, even mythical, rather than literal » (W. Brown 2010, 56). Elle illustre davantage la lutte du politique pour imposer son autonomie sur les autres sphères sociales. Comme son autonomie demeure incomplète, son pouvoir décisionnel l'est également concurrencé par le religieux ou l'économie notamment. Reprenant les thèses foucaldiennes, Brown suggère que la « sovereignty is never simply held and wielded but from the beginning *circulates*… (Just as sovereignty takes over theological practices of power, including making its word into law, it takes over economic practices of power, including circulation, fetichism, incorporation, and more) » (W. Brown 2010, 57).

Tout en conservant la définition schmittienne de la souveraineté, c'est-à-dire celui qui détermine l'ennemi envers qui le droit et la norme sont suspendus, Brown propose de réinsérer le concept dans un rapport de forces : le souverain n'est plus parfaitement autonome et son pouvoir décisionnel n'est pas illimité. Contre la figure du roi ou l'homogénéité du demos, décharger la souveraineté schmittienne permet aussi de penser son fractionnement. Judith Butler propose ainsi le terme de petit-souverain (« petty-sovereign ») en référence aux acteurs des administrations publiques et des firmes privées qui se voient attribuer un rôle décisionnel dans la gestion de l'autre sans passer par le cadre juridique. « [T]hey are … part of the apparatus of governmentality; » écrit Butler, « their decision, the power they wield to 'deem' someone dangerous and constitute them effectively as such, is a sovereign power, a ghostly and forceful resurgence of sovereignty in the midst of governmentality » (cité dans de Goede 2008a). Ce pouvoir souverain se manifeste lorsqu'au nom de la sécurité nationale un juriste autorise la surveillance d'un individu en vertu de la localisation numérique de son appareil informatique, lorsqu'un analyste attribue une citoyenneté à un individu ou qu'il le place sur la liste de surveillance, lorsqu'un programmeur structure un

algorithme de façon à ce qu'il sonne l'alarme pour une association avec un certain réseau de contacts, lorsqu'un pilote de drone lance un missile sur une cible identifiée par les données de son téléphone. Mais l'exceptionnalité du souverain s'exprime aussi lorsque le dispositif de sécurité se soustrait, sous couvert du secret d'État, à la normalité du politique, lorsque l'État intimide les journalistes et les membres de leur famille pour obtenir les informations divulguées par Snowden (Borger 2013; The Guardian 2013a), ou lorsque le Directeur du renseignement national offre, avec l'appui du président, la « least untruthful » réponse à une question d'un membre du comité sénatorial sur le renseignement (Ackerman 2013). Malgré les exigences de la loi qui menacent les responsables d'outrage au Congrès d'une peine allant jusqu'à cinq ans d'emprisonnement, la légitimité du secret entourant la sécurité nationale justifie l'exception à la règle du Congrès.

Ces exceptions ne correspondent peut-être pas à la suspension de la loi et de la norme que Schmitt imaginait, mais certainement à l'idée foucaldienne d'attribuer à l'un un droit de vie et à l'autre un droit de mort. En outre, constater la normalisation de l'exception permet de contourner le débat constitutionnel sur la surveillance. Comme il a été question précédemment, les pratiques de surveillance de la NSA sont basées sur une architecture légale complexe mélangeant acte législatif, ordre exécutif et interprétation légale. En ce sens, la NSA se soumet à une loi. Dans le débat constitutionnel, la question est de savoir si cette architecture légale respecte la constitution américaine et sa jurisprudence. L'exception est définie exclusivement en fonction de la constitutionnalité de la surveillance, la soumettant au registre du droit. Mais penser l'exceptionnalisme en fonction de la détermination de l'ennemi, cet autre indésirable à proscrire, par les gestes d'une myriade d'acteurs institutionnels permet de constater que le geste d'exception n'a rien de grandiose et d'unique. Au contraire, la pratique de l'exception est quotidienne, commune et répétitive, le produit d'analystes et d'algorithmes qui sélectionnent certains individus auxquels sont retirés leurs droits ou attribués des droits différents.

La souveraineté est quotidienne, elle est aussi transformée par la dé/reterritorialisation opérée par la superposition des réseaux numériques aux territoires nationaux. Dans une réflexion sur le retour paradoxal des frontières dans le contexte de la mondialisation, Brown suggère que la souveraineté se retrouve aujourd'hui scindée :

> One the one hand, there is sovereignty after the fence, sovereign powers (capital, religiously sanctioned violence) without specified jurisdiction or enclosure and without even the promise of containment or protection. On the other, there is fencing after sovereignty,

> nation-states lacking sovereign powers to delimit and secure their territories and populations (W. Brown 2010, 71).

Les pratiques de surveillance de la NSA illustrent ces deux aspects de la souveraineté contemporaine. D'une part, la souveraineté américaine[4] se projette bien au-delà de ses frontières « naturelles ». La défense du Homeland se mène de l'extérieur. Le numérique fusionne avec le réel. À ceux qui sont identifiés comme ennemi, le souverain met fin à sa promesse de protection : on leur retire ou l'on fait fi de leur citoyenneté, témoignage de l'inclusion à une communauté politique et supposer protéger contre l'arbitraire, pour les emprisonner ou les assassiner hors de tout cadre légal (Gallagher 2015b; Greenwald 2017). D'autre part, face à l'incertitude des menaces, le dispositif de sécurité américain étend la portée de la sécurité à toutes les sphères sociales, les transforme en autant de frontières pour contrôler et éviter la venue d'indésirables.

Porter attention à ces pratiques d'exception permet de s'intéresser aux effets politiques et sociaux de la surveillance plutôt qu'à sa constitutionnalité. Prétendre que l'insertion de l'univers numérique et de tout ce qui y transite dans une fièvre paranoïaque où l'interconnectabilité horizontale et verticale des composantes Internet garantit la réduction de la contingence et l'interception des risques à la stabilité des sociétés occidentales est lourd de conséquences. Dans ce contexte de gestion du social par la rationalité de sécurité, l'exception n'est plus le contournement de la constitution, mais l'érection d'une architecture légale normalisant des pratiques d'identification et d'exclusion de l'autre au profit de la normalité. En plus des conséquences réelles pour des milliers, voire des centaines de milliers d'individus, l'inscription du social dans le registre ennemi-ami crée des œillères empêchant d'imaginer les solutions aux problèmes du monde autrement que par la lunette de la violence.

5.8 Conclusion : fluidité et symétrie, de la surveillance numérique à l'esthétique critique

Pour qui désire participer, Secret Power de Simon Denny offre une expérience immersive de la culture institutionnelle de la NSA. L'artiste se tourne vers le détail d'artefacts issus de la NSA pour explorer l'iconographie du pouvoir et à travers lui, les méthodes déployées pour acquérir le

[4] Il est vrai que Brown fait référence à des sources de souveraineté non-politique. À l'encontre de celles-ci, le dispositif de sécurité incarne la souveraineté politique. Je m'en remets néanmoins à l'observation de l'auteur pour illustrer la disparition de certaines frontières.

savoir de sécurité et le rendre intelligible. L'iconographie de l'organisation résonne avec cette quête de sécurité et permet de voir le processus d'opérationnalisation des données de surveillance et les conséquences qui en résultent pour les concepts de géopolitique et de souveraineté. Pour la NSA, Internet est un lieu de pouvoir où transitent les menaces, mais aussi un lieu producteur de savoir : un monument du savoir contemporain.

L'œuvre de Denny propose une série de symétries. En refusant de fournir un scripte à sa collection d'objets, l'artiste joue avec la fondation épistémologique derrière l'interconnectabilité de la rationalité de la NSA. Sans explication ni repère, le spectateur est invité à associer ce qu'il voit pour le comprendre : à associer le secret qui se cache derrière la transparence trompeuse des portes vitrées, à associer les pratiques de surveillance à la permanence du traitement de données, à associer la sécurité du monde contemporain aux représentations d'un monde archaïque. À travers cette dernière symétrie, Secret Power fait écho au moment de rupture promis par Prométhée. Après la naissance de l'homme moderne, assisterait-on à la naissance de l'homme numérique, à l'homo digitalis pour reprendre le titre d'une série de documentaires produits par Arte (2017b) ?

Si la proclamation d'une ère nouvelle est hâtive, la surveillance de la NSA s'inscrit néanmoins dans un technofétichisme qui fait de l'identification des réseaux et de l'analyse des données de masse des solutions révolutionnaires aux problèmes nouveaux propres à un monde en changement. La mondialisation fait pression sur les frontières et les souverainetés, engendre des menaces terroristes plus fluides qui utilisent les réseaux de communication mondiaux pour se cacher et s'organiser. Or, conformément à la mythologie des données de masse qui lie son effectivité et son objectivité à sa capacité à tout analyser, les dispositifs de sécurité occidentaux, avec aux premières loges les dispositifs américains, déploient les infrastructures nécessaires pour tout surveiller, projetant le monde comme un ensemble statistique entier. Des individus ne sont plus la cible de la surveillance, mais le monde dans sa totalité devient un objet sécuritaire pertinent, même si le niveau d'attention et de visibilité de chacun varie. Dans ce contexte, la sécurisation du social qui motive et résulte de la surveillance numérique manifeste d'une valorisation de la mobilité et de la fluidité dans l'opérationnalisation du savoir de sécurité. Non seulement les pratiques de surveillance contournent-elles la fixité du territoire national et la division du monde en ensembles distincts, elles rejettent également la fixité des données, usant de leur plasticité pour les connecter, les associer et reconstituer des réseaux de terroristes statistiques à partir desquels il devient possible d'agir. Comme le relève Cheney-Lippold à propos du contrôle social des algorithmes, l'association

entre les données de masse et le traitement algorithmique transforme l'élément savoir du couple foucaldien savoir/pouvoir (Cheney-Lippold 2017a, 28). Les catégories de contrôle, qu'il s'agisse du terroriste, du genre ou des classes sociales, deviennent fluides au gré des scénarios.

Ces changements ne signifient pas la disparition des frontières, des fixités et des territoires. L'importance de l'accès aux infrastructures internationales de communication mondiale et les architectures légales mises en place pour profiter de l'extensibilité des droits nationaux rappellent leur importance. Comme le proposaient Sheller et Urry (Sheller & Urry 2006), la surveillance numérique ne s'inscrit pas uniquement dans un processus de déterritorialisation, mais participe à une reterritorialisation en réseau (J. Ferguson 2005). L'argument n'est pas nouveau, sinon qu'à travers la surveillance numérique, le réseau s'étend à l'univers numérique. La reterritorialisation de la menace lie la géographie aux individus, les infrastructures de communications aux appareils électroniques pour recréer une carte de l'insécurité où les niveaux physiques et virtuels s'additionnent. La nouvelle mobilité à surveiller, à craindre et à cartographier n'est plus seulement physique, mais de plus en plus virtuelle ; ou plutôt, la nouvelle mobilité relève de la physique des corps et de la lumière.

Le choix de la tête robotique de Terminator comme symbole du programme TREASUREMAP n'est peut-être pas si ironique après tout. Contrairement à ce que laisse entendre Denny, le Terminator n'est pas uniquement associé aux dangers de la militarisation de l'intelligence (Te Papa 2016b). Incarné par Arnold Schwarzenegger, le Terminator constitue également un allié de taille de la rébellion humaine dans la guerre contre les machines. Dans la deuxième itération de la série, le cyborg constitue une réponse masculine et virile à la menace liquide qui infiltre la société californienne, le cyborg nouvelle génération T-1000 (Robert Patrick) envoyé du futur pour abattre John Connor. L'anéantissement de la menace et la sauvegarde du monde contemporain sont possibles grâce aux technologies.

Secret Power introduit le spectateur à la culture géopolitique de la NSA. Mais Denny propose également un autre effet des révélations Snowden : une prise de conscience de la vulnérabilité de l'espace numérique en rupture avec l'espoir de la liberté de mouvement et de parole investi dans Internet. Grâce aux capacités technologiques de surveillance et au pouvoir interprétatif des données de masse, Internet aujourd'hui est un espace sécurisé.

6 De l'anonymat à une politique de contre-visibilité : la performance d'une communauté numérique égalitaire en rupture avec la surveillance numérique

If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.
Eric Schmidt, ancien PDG de Google[1]

« Welcome to your new NSA partner network ». C'est ainsi que les visiteurs de l'Art Hack Day, événement tenu dans le cadre de la 27e édition du festival berlinois transmediale 2014, apprirent que leurs téléphones avaient été piratés. Il ne s'agissait pas de l'acte d'individus mal intentionnés, mais le produit de *PRISM: The Beacon Frame*, projet des artistes Julian Oliver et Danja Vasiliev (Oliver & Vasiliev 2014a). Pour stimuler la réflexion sur l'omniprésence et le secret entourant la surveillance de masse à des fins de sécurité, les artistes entreprirent de reproduire et de rendre visible les pratiques et technologies déployées par le dispositif de sécurité occidental. Au cœur de cette réflexion sur la surveillance se situe le thème de la divulgation non volontaire d'informations personnelles.

PRISM: The Beacon Frame reproduit la surveillance de masse de la NSA et GCHQ en interceptant et collectant des données d'identification des téléphones cellulaires à portée de l'œuvre. Concrètement, l'œuvre se présente comme une mallette de type militaire contenant un ordinateur, un projecteur et un prisme de verre sur un socle rotatif. Un programme d'identification et de piratage de tours cellulaires est installé sur l'ordinateur. Ce programme repère, copie et imite les propriétés des tours cellulaires des opérateurs de réseaux comme Vodafone, o2, AT&T, de sorte que les téléphones qui tentent de communiquer avec leurs opérateurs sont trompés et attirés sur le faux réseau de *PRISM: The Beacon Frame*. Une fois connectées au réseau parallèle, les informations d'identification uniques des téléphones, par exemple les noms d'utilisateur, les adresses IP et MAC, sont collectées et projetées à travers le prisme de verre, créant selon les mots des artistes, « a rich and exploitative light show » (Oliver & Vasiliev 2014a). En parallèle, l'ordinateur envoie un message « of a troubling, humorous and/or sardonic nature » à chaque

[1] (Schmidt cité par Cheney-Lippold 2017a, 207)

téléphone piraté, informant leur propriétaire de l'acte de transgression et les invitant à consulter le site Web de l'œuvre (Oliver & Vasiliev 2014a). *PRISM: The Beacon Frame* alerte, comme son nom le suggère, les spectateurs à l'existence de la surveillance de masse, rappelant au passage que des informations jugées personnelles comme celles sur les téléphones intelligents sont l'objet de surveillance.

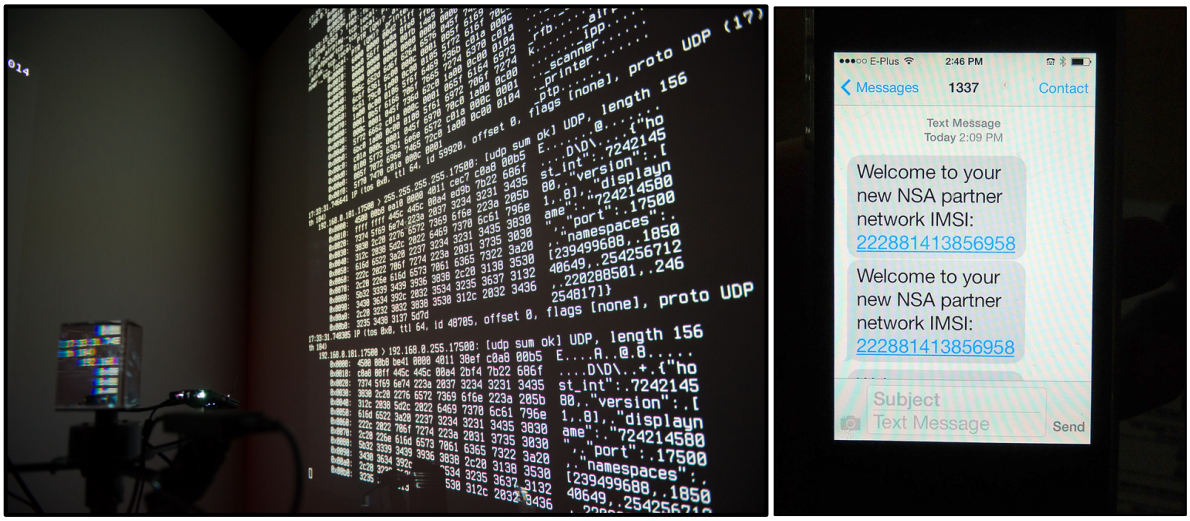


Figure 6.1 : PRISM : The Beacon Frame
(source : Oliver & Vasiliev 2014b)

L'œuvre se veut subversive (« exploitative ») permettant de visualiser les pratiques de surveillance secrètes du dispositif de sécurité. Dans les mots des artistes,

> PRISM: The Beacon Frame is a speculative, functional response to the general absence of information as to what NSA PRISM equipment actually looks like. Centered with the image of the prism, the project seeks to provide public direct contact with the aesthetics, technology and strategies used by states against their publics (and others), retained from critical contact by an opaque and coveted surveillance culture (Oliver & Vasiliev 2014a).

Comme le notent les artistes, l'œuvre est spéculative, reconnaissant la difficulté, voire l'impossibilité, de connaître les détails techniques des pratiques de surveillance de la NSA et de GCHQ, notamment ceux liés au programme PRISM comme le suggère le titre du projet. Pour les artistes, la nature spéculative de l'œuvre, voire l'inexactitude de la représentation, ne pose pas problème, puisque l'objectif principal de l'œuvre est de contourner le secret de la surveillance. Dans cette perspective, que *PRISM: The Beacon Frame* copie les pratiques de surveillance de téléphone de type StingRay plutôt que celle du programme de même nom ne contrecarre pas l'entreprise de contre-visibilité de l'œuvre. Pour mémoire, PRISM permet à la NSA d'accéder aux

données stockées sur les serveurs des grands joueurs de l'économie numérique. La NSA a certes mis en œuvre des programmes de surveillance des téléphones cellulaires, les RAINFALL, AURORAGOLD, MYSTIC et autres CO-TRAVELER, mais ceux-ci diffèrent considérablement de PRISM (Gellman & Poitras 2013; Gallagher 2014; Gellman & Soltani 2013c; Devereaux, Greenwald & Poitras 2014). La surveillance des téléphones par la simulation d'une tour cellulaire comme celle pratiquée par les artistes constitue une interception IMSI (International Mobile Subscriber Identity), analogue aux intercepteurs déployés à proximité de la colline parlementaire à Ottawa au printemps 2017 (Cullen & Bureau 2017). Plutôt que de chercher à reproduire avec précision la surveillance des dispositifs de sécurité occidentaux, *PRISM: The Beacon Frame* signale l'existence de pratiques intrusives. La transparence de l'œuvre, qui permet aux « [a]udiences peering into the prism [to] 'see inside' the internal workings of this intervention » (Oliver & Vasiliev 2014a), viendrait, semblent suggérer les artistes, compenser l'opacité de la surveillance d'État afin d'en éclairer les structures invisibles et de susciter la contestation des spectateurs.

Au-delà de la critique esthétique de *PRISM: The Beacon Frame*, mon intérêt pour le projet vient de la controverse qui l'a accompagné. Choqués par son caractère intrusif, des spectateurs ont demandé au festival transmediale de désactiver l'œuvre sans quoi ils contacteraient les autorités fédérales allemandes pour violation des lois sur la confidentialité des données et l'attribution de fréquence. Face aux risques d'être confrontés à des poursuites judiciaires, le festival a obtempéré, à contrecœur faut-il préciser. Dans une lettre explicative, le festival précise qu'il ne pouvait supporter les charges financières et pénales associées aux procédures judiciaires, tout en réitérant son appui au projet. « [I]t is absurd, » écrit le festival,

> that this work would even risk being reported in these times of highly illegal surveillance operations carried out by governments on entire populations. The credit certainly goes to those who keep revealing these structures rather than those who seek to target artists who contribute to our awareness of them (transmediale 2014c).

D'un même souffle, plusieurs dans le milieu artistique se sont offusqués des plaintes, les associant à la censure, et ont répondu en louangeant le projet (Pangburn 2014; Lechner 2014; Pearlman 2014; Squires 2014; Brucker-Cohen 2014). Olof Mathé, co-commissaire de l'Art Hack Day, écrit ainsi :

> "PRISM: The Beacon Frame" is as visually stunning as it is technically audacious. … It raises questions around our exploitative relationship to critical infrastructure. As such, it was universally acclaimed by visitors to the exhibition. In a certain light, it's ironic that a component of the installation be taken down since it merely re-articulates some of the core questions raised by the piece: Who controls our infrastructure? Why is certain technology the prerogative of those in power? How can we foster public debate around the ramifications of technological choices? The threat of reporting to the police is equally ironic and sad. It's ironic because the work highlights the violations the German Parliament, next door to the exhibition hall and the epitome of power, has been exposed to. It's sad because the type of pseudo-"citizen's arrest" Danja and Julian were victims of is the hallmark of the faceless bureaucracy and tacit obedience on which many power structures rely (Mathé cité par Oliver & Vasiliev 2014a).

Rendre visibles les pratiques secrètes constitue une avenue traditionnelle de la résistance à la surveillance. En ce sens, les louanges adressées à *PRISM: The Beacon Frame* sont justifiables. Esthétiquement intéressante et provoquante, l'œuvre invite à la réflexion, mais à une réflexion orientée devrait-on préciser où la seule véritable conclusion possible est le refus de la surveillance actuelle.

Dans ce concert d'éloges, au moins une voix brise l'harmonie. En conversation avec Laura Poitras dans le cadre de l'événement Seven on Seven organisé par Rhizome, Kate Crawford s'interroge sur les relations de pouvoir que certaines œuvres, mentionnant à titre d'exemple celle de Oliver et Vasiliev, reproduisent :

> KC:… While there are lines of questioning that artists are exploring with these technologies, they also must confront that they are also surveilling the already-surveilled. What do you think of the ethics of surveillance art [she asks Poitras]? Do you think it's a case of that old problem that the master's tools cannot dismantle the master's house?
>
> LP: … I think art should provoke. But I do think it's a complicated terrain, and I do think consent has to be factored in, and whether or not the people being subjected to the surveillance have consented.
>
> KC: Exactly. Otherwise it runs the risk of being what Allison Burtch has called 'cop art' (Poitras & Crawford 2015).

Outre Crawford, personne parmi les défenseurs de *PRISM: The Beacon Frame* ne semble avoir cherché à comprendre pourquoi certains spectateurs se sont sentis envahis dans leur vie privée, voire trahis quant à la forme et au message de la critique esthétique. Une réaction aussi radicale que de faire censurer une œuvre est pour le moins étonnante dans un contexte artistique, plus encore dans le contexte du festival qui accueillait l'œuvre de Oliver et Vasiliev. L'événement Art Hack Day, comme l'écrit Mathé, « was initiated with the express purpose of providing a haven for

hackers whose medium is art and artists whose medium is tech to express themselves to their fullest ability » et de les protéger contre les poursuites jugées excessives auxquelles ils sont souvent confrontés (Mathé cité par Oliver & Vasiliev 2014a; voir aussi Art Hack Day 2017). De façon générale, le festival transmediale est un des principaux espaces mondiaux de réflexion sur la culture numérique. Afterglow, thème de l'édition 2014, se voulait l'occasion de repenser les conséquences indésirables de la culture numérique : « transmediale 2014 proposed the post-digital moment of 'afterglow' as a diagnosis of the current status of the digital hovering between 'trash and treasure' » (transmediale 2014a).

La controverse invite à approfondir la question de la subversion qui fonde la démarche et légitime l'œuvre d'exploitation. Qu'est-ce que l'œuvre subvertit ? Qu'exploite-t-elle ? Le secret des pratiques de surveillance de la NSA, pourrait-on immédiatement répondre. Pourtant, comme le relève Crawford, il y a plus : la présence d'un élément oppressif. *PRISM: The Beacon Frame* met en vedette les spectateurs de l'œuvre, surveille ceux qui sont déjà surveillés, sans demander leur consentement. Certes, d'autres projets retournent également les technologies de surveillance vers leurs spectateurs. Tant les œuvres *Sorting Daemon* de David Rokeby (Rokeby 2010), *Database* de Tobias Zimmer et David Ebner (Zimmer & Ebner 2017) que *Zoom Pavilion* de Rafael Lozano-Hemmer et Krzysztof Wodiczko (Lozano-Hemmer & Wodiczko 2017) surveillent leurs spectateurs sans consentement, mais n'ont pas eu à subir les mêmes foudres. Elles le font, cependant, différemment, à l'aide de caméras de surveillance qui les filment déambulant. Ces œuvres surveillent le visage et le corps des spectateurs dans l'espace public. Contrairement à ces dernières, *PRISM: The Beacon Frame* pénètre sur le téléphone des spectateurs, de plus en plus perçu comme une extension technologique de l'identité, et en expose certaines informations sans en demander le consentement. Comme l'écrit Gary T. Marx, « [c]onsent involves participants who are fully apprised of the surveillance system's presence and potential risks and of the conditions under which it operates » (Marx 2006, 43). Peut-être les spectateurs de *PRISM: The Beacon Frame* qui demandèrent sa désactivation évaluèrent-ils différemment les risques associés à l'intrusion non désirée sur leurs téléphones ? Peut-être la controverse illustre-t-elle la normalisation de la surveillance par caméra et la reconnaissance faciale devenues omniprésentes dans les espaces publics, dans les médias sociaux et même, comme le suggère l'iPhone X, la dernière mode de sécurité informatique.

Certes, l'objet de *PRISM: The Beacon Frame* est précisément de faire prendre conscience aux spectateurs des limites du consentement. Leurs données sont observées par le dispositif de sécurité et nombre d'acteurs économiques, qu'ils le désirent ou non. Comme l'écrivent les artistes en réaction à la désactivation de leur œuvre :

> [i]t was our intention to provide an opportunity for public to critically engage precisely the same methods of cellular communications interception used by certain governments against their own people and people in sovereign states. It was not, in any way, our intention to harm anyone and nor did we. … It is vital that technology-based art remain [sic] a frame with which we can develop critical discourses about the world we live in, from the engineered to the cultural and political. Sometimes that requires that we are not limited by exaggerated fears and legal definition, but that we act proportionally and with conscience in our efforts to understand the power struggles and tensions in our (technically mediated) environment (Oliver & Vasiliev 2014a).

Or, la démarche adoptée par les artistes ne fait pas que provoquer la réflexion sur cette mise à nu numérique, elle confirme les spectateurs dans leur statut d'objet de surveillance, sans égard pour les individus assujettis. L'absence de considération des artistes pour les récriminations des spectateurs concernés, qui seraient limités par des peurs exagérées et à qui ils n'ont fait aucun mal, démontre les limites de leur analyse des conséquences sociales de la surveillance de sécurité. Non seulement, les artistes ne demandent-ils pas le consentement des spectateurs, ils martèlent en outre la soumission des individus à la surveillance en profitant de leur ignorance ou naïveté. La critique de la complicité, de l'obéissance tacite pour reprendre les mots de Mathé, formulée par les artistes est faite en reproduisant les structures de pouvoir qu'ils disent contester. Ils exploitent la présence des spectateurs, leurs performances numériques, sans se soucier des conséquences de cette visibilité forcée pour les différents individus. Là se situe le problème fondamental de l'œuvre : l'absence de contrôle sur notre visibilité et les effets discriminatoires des mécanismes de contrôle de la surveillance numérique. L'œuvre d'Oliver et Vasiliev reproduit un travers commun de la critique esthétique, à savoir la représentation de la surveillance comme un phénomène auquel nous sommes tous également soumis. Cette représentation focalise l'attention critique sur la production de données et la liberté individuelle, plutôt que sur ce qui est fait de ces données et la poursuite de l'égalité sociale.

Dans le reste de ce chapitre, j'approfondis, à travers l'analyse de l'œuvre *Autonomy Cube*, la question de la visibilité des utilisateurs d'Internet. La société de contrôle soumet sa population à un impératif de visibilité en vertu duquel tous doivent apparaître pour assurer la prospérité et la

stabilité de l'ordre social. *Autonomy Cube* propose l'anonymat comme forme de résistance à cet impératif, mais divergeant de l'individualisme des discours sur la vie privée, l'œuvre propose une démarche collective. Après avoir approfondi les contraintes à la résistance numérique, je suggère qu'*Autonomy Cube* met en œuvre une politique de contre-visibilité préfigurant une communauté numérique égalitaire et ouverte qui brouille les processus de contrôle de la surveillance numérique.

6.1 [redacted]

La surveillance de masse justifie le refus d'apparaître dans le monde numérique. Edward Snowden s'est fait le promoteur du chiffrement des données comme moyen le plus efficace pour éviter le regard du dispositif de sécurité. Son appel a été repris par plusieurs personnalités et institutions de la société civile telles que Glenn Greenwald, Laura Poitras et Jacob Appelbaum et des organisations comme Human Right Watch, Electronic Frontier Foundation (EFF), Privacy International et, plus localement, Crypto.Québec (AccessNow 2017; Poitras & Crawford 2015). De nombreux organes de presse offrent maintenant des points de dépôt sécurisés et affichent des clés publiques chiffrées pour permettre aux lanceurs d'alerte de les contacter (SecureDrop 2018). De nombreux sites Web ont adopté le protocole de transfert hypertexte sécurisé[2] (HTTPS) permettant de chiffrer les contenus des communications. Pour les sites qui ne l'ont pas adopté, l'EFF a développé une extension pour les navigateurs Internet permettant d'appliquer le protocole à toutes les communications (EFF 2017a). Plusieurs entreprises ont également entrepris de sécuriser leurs réseaux en chiffrant le contenu y circulant, au grand dam des autorités américaines qui réclament au contraire un accès privilégié leur permettant de contourner la cryptographie (Mott 2016; Nakashima 2014). La controverse entourant le déverrouillage des téléphones cellulaires des auteurs de la fusillade de San Bernardino aux États-Unis est emblématique de cette opposition entre Silicon Valley et les autorités américaines (Yadron, Ackerman & Thielman 2016).

Certains ont également fait la promotion de logiciels sécurisés qui ne collectent ni ne partagent les données de leurs utilisateurs et adoptent plutôt un modèle d'affaires payant ou libre. Les projets Prism Break (Zhong 2017) et Alternative App Center du Tactical Technology Collective (Tactical Technology Collective 2018) par exemple répertorient les logiciels libres de messagerie et de courriels, de synchronisation de données ou de médias sociaux qui protègent les

[2] « HyperText Transfer Protocol Secure »

données des utilisateurs, des guides d'utilisation et des programmes de visualisation sur le thème de la vie privée. D'autres poursuivent des entreprises d'anonymisation et de contrôle des données visant à faire disparaître les traces numériques à l'image de l'extension Ghostery qui bloque les témoins de connexion (« cookies ») ou encore de projet *Data Detox Kit*. Présenté dans le cadre de l'exposition The Glass Room par le Tactical Technology Collective et la Fondation Mozilla, connue pour son navigateur Firefox, le *Data Detox Kit* propose, comme son nom l'indique, une cure de désintoxication numérique. Contre le « data bloat—a toxic build-up of data that can lead to uncomfortable consequences in the longer term », la cure promet qu'« [i]n just half an hour or less per day, you'll be well on your way to a healthier and more in-control digital self » (MozillaTactical Technology Collective 2017). À travers divers thèmes, tels que notre présence numérique, la pénétration de Google, les historiques de recherche, les médias sociaux, *Data Detox Kit* amène l'utilisateur à explorer la richesse et la profondeur des informations personnelles qui sont entre les mains des entreprises numériques. *Data Detox Kit* connecte aussi l'utilisateur à une série d'applications comme *Data Selfie*, *Panopticlick*, *Privacy Badger*, *HTTPS Everywhere*, *AdNauseam*, qui visualisent ou résistent la surveillance numérique.

Dans ce courant vers un plus grand anonymat des données, Trevor Paglen et Jacob Appelbaum, spécialiste de la cryptographie numérique et membre de l'équipe du projet Tor jusqu'en juin 2016 (Le Monde 2016), ont créé, en 2014, *Autonomy Cube*. « Autonomy Cube is a sculpture … meant to be both "seen" and "used", » explique Paglen.

> Several Internet-connected computers housed within the work create an open Wi-Fi hotspot… But Autonomy Cube does not provide a normal internet connection. The sculpture routs all of the Wi-Fi traffic over the Tor network… In addition, Autonomy Cube is itself a Tor relay, and can be used by others around the world to anonymize their internet use. When Autonomy Cube is installed, both the sculpture, host institution, and users become part of a privacy-oriented, volunteer run internet infrastructure (Paglen 2014a).

Même si le cube de Plexiglas contenant les cartes maîtresses Novena et le logiciel libre exploitant le relais TOR est, par sa taille et sa discrétion, « easy to miss » à l'avis de la critique d'art Harriet Riches (Riches 2016), la portée de l'œuvre de Paglen et Appelbaum est vaste : éveiller les consciences aux problèmes de la surveillance numérique et offrir une infrastructure Internet libre conformément à la double vocation de l'œuvre à être vue et utilisée.

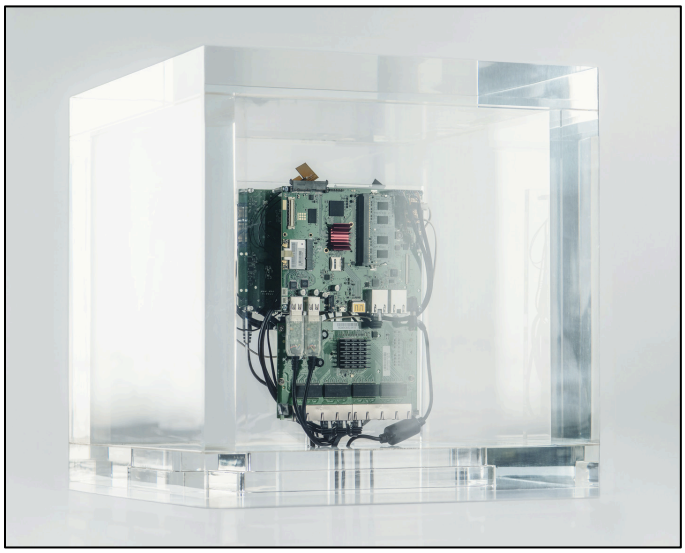


Figure 6.2 : Autonomy Cube
par Trevor Paglen et Jacob Appelbaum (source : Edith-Russ-Haus for Media Art 2015)

Le point de départ du projet est l'insatisfaction des artistes-activistes face à Internet. Vecteur de savoir, Internet est parallèlement devenu une infrastructure de contrôle des populations. « The Internet was designed for all of [the interconnected] devices to trust each other and be transparent with each other, » explique Paglen lors d'une entrevue. « In part because of [its] very openness … the Internet is an incredible tool of global communication, but also the greatest tool of surveillance that humankind has ever created » (Aikens & Paglen 2016). En s'attaquant à la surveillance numérique, *Autonomy Cube* « revives the utopian ideas from the initial years of the Internet » (Edith-Russ-Haus for Media Art 2015). L'œuvre ravive cette utopie en informant les visiteurs, en permettant aux visiteurs et internautes naviguant sur le réseau Tor d'échapper à la surveillance numérique tout en conservant l'accès à la richesse du contenu d'Internet, et en transformant les institutions muséales en havre de protection de la vie privée et de la liberté d'expression. Comme le suggère Tim Adams, Paglen et Appelbaum sont à la recherche d'un modèle Internet « that would still give you access to all the world's information, but would preserve anonymity and not collect your data … [and] at ways in which art might take that utopian principle into space » (Adams 2017).

Dans un premier temps, *Autonomy Cube* a pour vocation d'être vue, rappelant aux visiteurs les pratiques de surveillance économique et sécuritaire décriées. En ce sens, l'œuvre partage la sensibilité critique de Paglen pour l'image que l'on retrouve dans ses photographies. Comme l'explique Paglen,

> I'm interested in images that don't speak themselves, images that you look at and can't really get much information from… There is a politics in that process: first, ascertaining where those places [or images] are, second insisting on my right to take that photograph, and then third introducing—in this kind of elliptical, metaphorical way—these images and their associations into the world (Aikens & Paglen 2016).

Certes, contrairement à ses photographies, *Autonomy Cube* ne jette pas un regard transgressif sur une installation secrète. La sculpture se veut néanmoins une image de rupture qui ne peut s'expliquer d'elle-même. Elle est ce que Paglen nomme un « "impossible objec[t]," [a] thin[g] that seem [s] to have arrived from another world that contrasts with our own » (Paglen cité dans Greenberg 2016). La sculpture demande à être inspectée pour comprendre que l'objet contenu dans la boîte, une partie du réseau Tor, est transgressif. Tor permet de contourner la dystopie Internet et de retourner aux espoirs fondateurs. « The Internet is a predatory network, » juge Paglen,

> that is, on one side, potentially a very coercive tool of totalitarian power and, on the other side, a tool that will increasingly be used to allocate rights and privileges through commercial means—credit scores or insurance rates and that sort of thing. Given that situation, can we imagine a different kind of network? Can we envision a network that is nonhostile? Our project Autonomy Cube is an attempt to imagine what this alternative network might be like (Paglen & Appelbaum 2016).

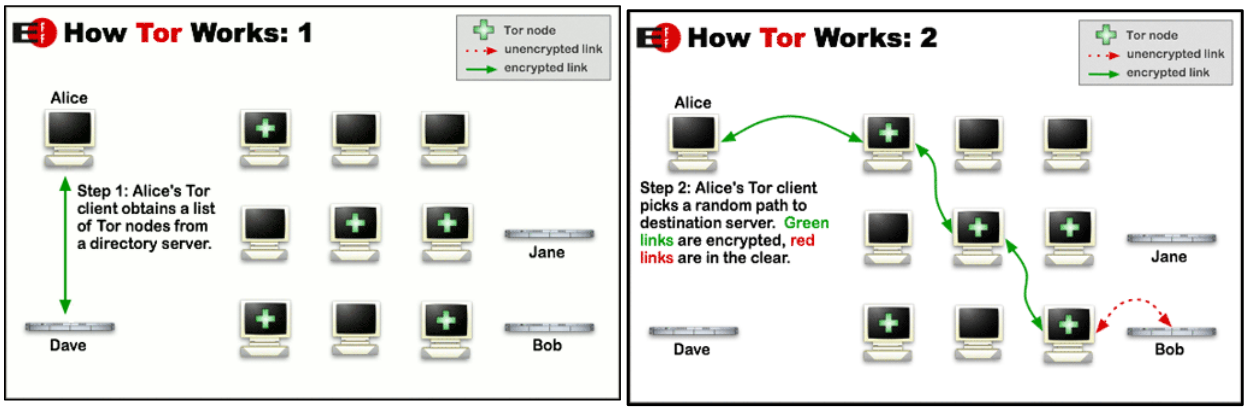
Pour les artistes-activistes, Tor offre un modèle Internet alternatif au capitalisme actuel. Tor, diminutif de The Onion Router, est un réseau distribué géré bénévolement qui permet de rendre les communications numériques anonymes. Et il le fait très efficacement, le réseau dans sa totalité étant pratiquement impossible à percer (J. Ball, Schneier & Greenwald 2013). Pour cette raison, Tor est souvent représenté par les autorités comme un repère de fornicateurs, de déjantés et de criminels — « [t]he front-runners of the "info apocalypses," as people like to call them, … essentially child pornographers, drug dealers, terrorists, and money launderers » (Paglen & Appelbaum 2016) — à la recherche d'anonymat dans la conduite de leurs vices. L'Edith-Russ-Haus for Media Art, l'un des premiers endroits où a été exposé *Autonomy Cube*, a d'ailleurs cru bon informer la police locale de la présence d'un relais Tor au sein du musée, qui l'a alors déconseillé de procéder à l'installation de l'œuvre (Edith-Russ-Haus for Media Art 2015).

Tor rend les communications anonymes, mais n'est pas un service de chiffrement. Ces derniers chiffrent généralement le contenu des messages de bout en bout de sorte que seul le destinataire puisse les déchiffrer et les lire. Tor est un système de routage en pelure d'oignon (« onion routing ») qui masque plutôt la route des paquets de données dans le but de créer une

déconnexion entre les points d'origine et de fin des communications, entre l'utilisateur et le site Web visité (Reed, Syverson & Goldschlag 1998). L'organisation derrière le projet Tor décrit ainsi la logique du réseau :

> Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going (Tor 2018d).

Concrètement, lorsqu'un utilisateur se connecte au réseau Tor, le logiciel établit un contact avec un point d'entrée gestionnaire d'une liste de relais. Partant de cette liste, le logiciel crée une série de communications chiffrées entre les relais du réseau. Chaque saut à travers le réseau est chiffré différemment afin d'assurer qu'en aucun temps un des relais ne puisse connaître l'ensemble de la route prise par les paquets de données. Alors que le paquet de données progresse à l'intérieur du réseau, chaque relais décode une couche de chiffrement puis transmet le paquet de données vers un autre relais. Après trois sauts, le paquet de données quitte le réseau par un point de sortie (« exit node ») et poursuit sa route numérique normalement à travers les différentes infrastructures des opérateurs de réseau qui pourront collecter des données sans entrave puisque celles-ci ne sont pas chiffrées. Seulement, il ne sera pas possible de relier les données collectées à l'utilisateur. En amont, les données révéleront le point d'origine avec pour destination le réseau Tor. En aval, elles révéleront la destination et le réseau Tor comme point d'origine. Jamais ne révéleront-elles à la fois l'origine et la destination réelles.



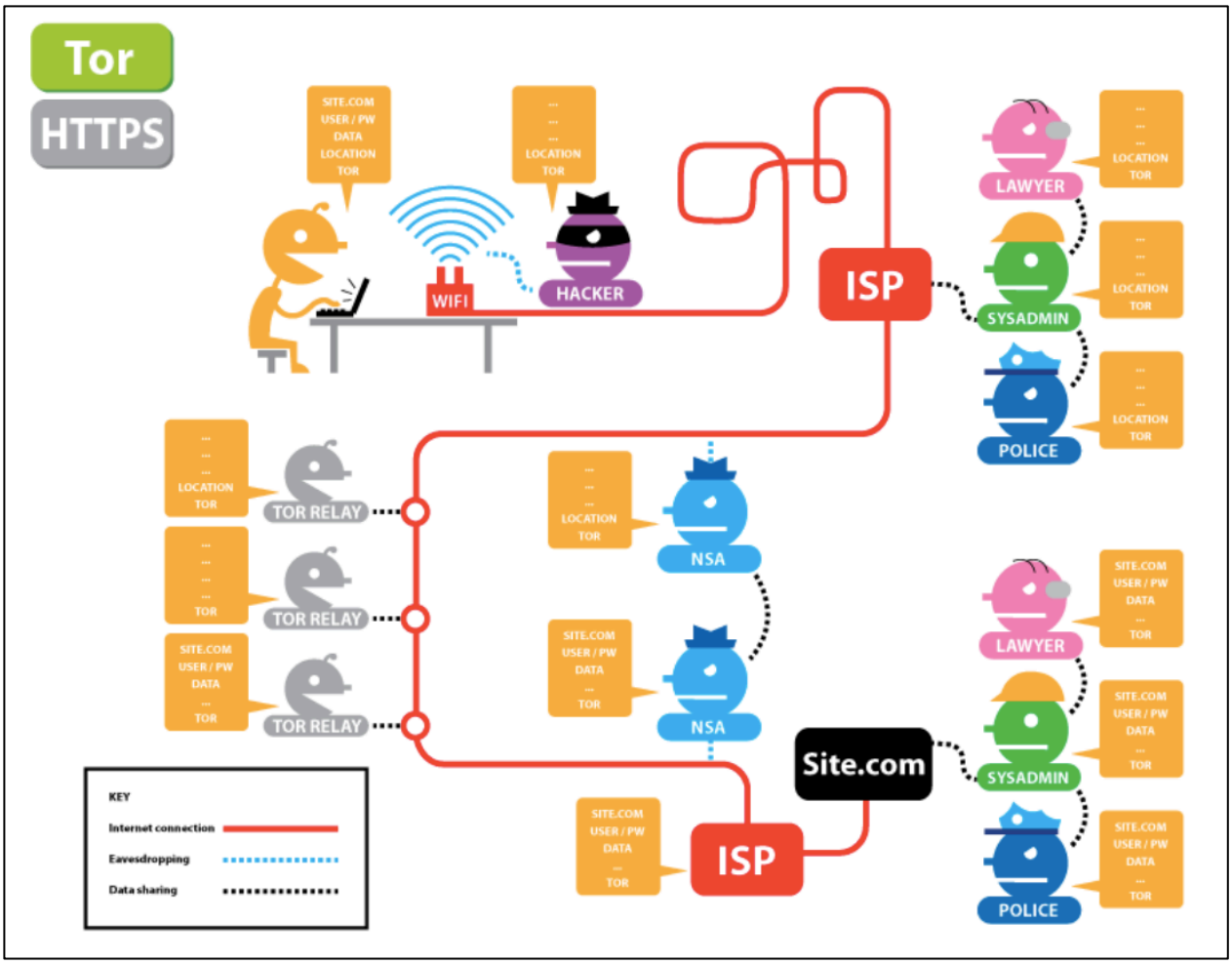


Figure 6.3 : Tor, réseau permettant l'anonymat des données
diagramme résumant le fonctionnement de Tor, et tableau interactif produit par l'EFF montrant la nature des données collectées suite à l'utilisation de Tor (sources : EFF 2017b; Tor 2018d)

Si le réseau Tor a été mis en place, financé à l'origine par le Naval Research Laboratory du Département de la défense américain, pour contourner la censure et la surveillance d'État, favoriser la liberté d'expression et l'activisme dans les régimes autoritaires, et permettre aux autorités de mener des activités de surveillance et d'espionnage sans être repérées, *Autonomy Cube* se veut une revendication radicale du droit à l'anonymat numérique pour tous (Aikens & Paglen 2016). Le projet Tor rapporte ainsi la diversité des utilisateurs du réseau. Journalistes, officiers des forces de l'ordre, militaires, activistes, dirigeants d'entreprises, professionnels des technologies de l'information utilisent Tor qui comptent des millions d'utilisateurs par jours. Tor s'adresse aussi aux « normal people … [desiring to] protect their privacy from unscrupulous marketers and identity thieves … [to] protect their communications from irresponsible corporations … [to] protect their children online … [to] research sensitive topics … [to] skirt surveillance … [to] circumvent

censorship » (Tor 2018e). Malgré les critiques formulées à l'encontre du réseau Tor, les artistes-activistes invitent les spectateurs à une plus grande conscience de la surveillance numérique et de l'importance de la vie privée.

Pour le duo, les craintes que le réseau rende possible la réalisation d'actes répréhensibles ne peuvent justifier la suppression de la vie privée. « You always hear that the reason you can't actually have any civil liberty on the Internet is because of these four groups [the child pornographers, drug dealers, terrorists, and money launderers], » explique Appelbaum lors d'une vidéoconférence publique avec Paglen organisée par l'Institut Goethe de New York.

> It is the case, of course, that the Tor network is a reflection of the larger Internet … if you give people this anonymity they will use it, in theory, to do very good things and also clearly very bad things… Of course, Tor won't be able to stop people who have the desire and the ability to break a law and are willing to commit heinous crimes… Tor is the option for law-abiding, reasonable people… But it's really hard to design a system where, for example, the Chinese idea of the bad guy, or the German or the American idea of the bad guy, would be stopped. And what would happen when you have built in such a facility? So the idea instead is to increase everyone's liberty and to give regular people an option that doesn't cost them money and is helpful in the sense that they are now more protected. Meaning that their rights are now larger than they were before. This is very important for not only resisting censorship of certain things, but also for making sure that there isn't mass data collection that's tied to you for the rest of your life and that becomes a function of wealth and privilege. With Tor, you'd be able to have some sort of privacy (Paglen & Appelbaum 2016).

Le projet de Paglen et Appelbaum a une fonction éducatrice, critique face à la surveillance numérique et au modèle économique dominant basé sur la collecte de données personnelles. « One of the biggest issues of our time is this combination of surveillance and algorithms, » explique Marcel Schwierin, codirecteur de l'Edith-Russ-Haus for Media Art. « Yet people can't feel it. It's completely invisible. There must be a way to make this more visible. That's what the Autonomy Cube does. You see it and you know that thousands of people are anonymizing their data to defend their privacy » (Edith-Russ-Haus for Media Art 2015). En présentant le réseau Tor, l'œuvre offre un modèle Internet alternatif sécurisé et non commercial, géré par quelque 6000 bénévoles qui opèrent le réseau en offrant leurs matériels informatiques et leur bande passante (Tor 2018b). Mais le projet n'a pas que valeur de critique. Il a aussi une vocation fonctionnelle. « Critique can be easy and it doesn't necessarily get you anywhere, » suggère Paglen. « So I'm definitely thinking about projects that instead of critiquing the existing infrastructures and institutions, try to make them better. Instead of 'institutional critique' we can think about 'institutional enhancement' » (Aikens & Paglen 2016).

Autonomy Cube est usuel et transformateur en offrant aux visiteurs un accès à Internet gratuit et sécurisé et en servant de relais Tor pour les autres utilisateurs du réseau. Comme le rapporte Riches, « [i]nteracting with the sculpture in the exhibition, visitors become part of a resistant infrastructure, invisible and unseen—if only for a moment » (Riches 2016). La démarche d'*Autonomy Cube* est aussi collective. Elle dépasse l'individu et s'inscrit dans une critique transformatrice et sociale des infrastructures numériques. La participation d'institutions muséales permet d'accélérer la performance du réseau dans son ensemble en mettant à contribution les infrastructures numériques institutionnelles beaucoup plus puissantes que celles fournies par les bénévoles. Ainsi contre les quelques mégaoctets des relais moyens, les serveurs institutionnels des musées abritant l'œuvre offrent un débit de bande passante pouvant aller jusqu'à 100 mégaoctets. Un réseau plus rapide dans son ensemble accroît l'attractivité de Tor pour tous (Greenberg 2016). La présence institutionnelle est aussi importante parce qu'en offrant un point d'accès Internet gratuit, elle augmente le nombre d'utilisateurs de Tor. Or, la présence d'utilisateurs est au cœur de l'anonymat du projet. Contrairement à un programme de chiffrement classique qui code les données, Tor masque l'identité des individus derrière le réseau. Le collectif apparaît en lieu et place de l'individu. Un utilisateur demeure par exemple vulnérable à une attaque de synchronisation de bout en bout (« end-to-end timing attack ») reliant le moment d'envoi des paquets de données à celui de l'arrivée sur un site destination (Tor 2018d). La force de Tor provient de sa pluralité. « Tor hides you among the other users on the network, » expliquent les concepteurs du projet, « so the more populous and diverse the user base for Tor is, the more your anonymity will be protected » (Tor 2018d).

L'Edith-Russ-Haus for Media Art était bien conscient de la dimension collective de l'œuvre lors de son exposition. *Autonomy Cube* y a été présenté en solo, et le musée a suspendu la tarification lors de l'exposition afin d'assurer l'accessibilité à l'œuvre et à un Internet sécurisé, créant du coup « a truly inviting public space, an Agora for anyone to activate the sculpture by using it » (Edith-Russ-Haus for Media Art 2015). Plutôt que de servir de point de rencontre pour les gens s'y trouvant physiquement, le musée s'est offert comme porte d'accès vers une socialisation numérique à l'abri de la surveillance de masse. Comme l'écrit le musée, « the sculpture and its repeaters has turned the whole Edith-Russ-Haus into an Autonomy Cube providing free, unsurveilled Internet access » (Edith-Russ-Haus for Media Art 2015). Cette idée de transformer le musée en espace protégé est un des aspects centraux de la démarche de Paglen et

Appelbaum. Avec *Autonomy Cube*, le duo politise les infrastructures numériques et le musée qu'ils tentent de projeter en havre de la liberté d'expression et de la vie privée. Comme le propose Glen Helfand, critique artistique au Guardian, *Autonomy Cube* « offers a sense of refuge, turning the gallery into a functionally politicised space » (Helfand 2015).

Pour Paglen et Appelbaum, il n'y a probablement pas de sortie à court terme de la surveillance numérique actuelle. Et même si Tor ni la technologie n'offrent de salut, cela n'empêche pas d'y résister néanmoins. « [W]hat this project is about is trying to show the ways in which technologies congeal social, political, economic, and cultural relationships, » expliquent les concepteurs.

> Let's think about what technologies and communication infrastructures may look like if we try to build them with different values at their core. We imagine an alternative to the hostile network that is preying upon us all the time, and try to enhance the parts of the network that do allow us the kinds of freedom and intellectual exploration and participation in democratic projects that were previously unavailable to us (Paglen & Appelbaum 2016).

Faute de mieux, si l'on peut dire, *Autonomy Cube* permet de transformer un espace, celui du musée, en zone démocratique protégée, à l'instar des bibliothèques. Ces dernières ont su protéger la vie privée de leurs lecteurs contre le Patriot Act américain voulant donner accès aux registres d'emprunt de livres (Aikens & Paglen 2016). Seulement, pour Paglen, le principal lieu d'exploration et de production de savoir aujourd'hui est Internet. Les curieux se tournent davantage vers Internet que vers les bibliothèques. Déjà, le Library Freedom Project d'Alison Macrina sensibilise les bibliothèques à la question de l'information numérique (LFP 2018). Pour le duo, le musée, autre institution civique importante, doit également servir de havre garantissant la liberté d'explorer et de parole des personnes (Paglen & Appelbaum 2016). « Free libraries foster a society where you have an educated populace and diversities of opinions, » explique Paglen.

> But the other very important thing about libraries is that the police don't get a record of the books that you check out. In other words, you are able to use a library to explore culture and information anonymously. And that anonymity is a crucial part of the freedom and the contribution to a democratic society that a library affords. Our proposal is that museums should do the same. They should be places where you can go and encounter ideas that might be challenging, where you are given permission to look at images and think about concepts that you don't always have permission to think about in your everyday life. We propose to approach museums as safe spaces from a world that is increasingly tracking everything you do and collecting as much information as possible about you (Paglen & Appelbaum 2016).

Autonomy Cube poursuit cet objectif en offrant un « institutional enhancement » qui contribue à un créer un espace Internet anonyme au sein des musées et pour tous les utilisateurs du réseau Tor. Le projet fait du musée, au côté des bibliothèques, un espace d'exception, un sanctuaire contre la surveillance numérique.

6.2 Refuser la société de contrôle, protéger l'anonymat

Interrogeant les dimensions politiques et éthiques des infrastructures de communication Internet, Paglen et Appelbaum poursuivent, avec *Autonomy Cube*, plusieurs pistes critiques. Ils alertent les spectateurs aux problèmes oubliés ou invisibles de la surveillance numérique. Le projet offre aussi, à travers la mobilisation de la participation des musées au réseau Tor, une infrastructure Internet libre favorisant l'anonymat et, à travers celui-ci, l'autonomie politique.

Pour les concepteurs du projet, la surveillance numérique participe à l'attribution de privilèges et participe à la mise en place d'une société de contrôle :

> TP: Today, in large part, that information is being used to sell you things, or they try to sell your information to advertisers. But tomorrow, that information will be used in all kinds of other ways. … But the point is that—although it's not evenly distributed yet, this will increasingly be true in the future—the rights and the privileges that you have will be modulated according to these kinds of metrics. In China this is already beginning to happen.
>
> JA: The Chinese scoring system is part of their identity intelligence—these guys are all about doing everything they can to identify everybody in every way. The scary part about what's happening in China is how we can imagine it as the future everywhere. … It's a paternalistic control and surveillance that informs automatically. You no longer need people to tell on each other. The mere existence of certain devices ensures that the devices themselves tell automatically. This is the nightmare of the science-fiction writer Philip K. Dick. Not that everyone would be a spy—that's sort of a trope about the former East Germany—but that every *thing* would be a spy… I mean, it's really an extreme of the control society tied directly to your identity. And there are in fact plans for something called real-time tipping. … if someone decided that I was a person of interest, I would get tipped off and sent to an analyst in real time. And now you start to see how these things tie together—it becomes extremely alarming to think about how this information might be used to impact your life. It's a very scary thing.
>
> The system might also work in your favor when you behave well. You buy the right brand of thing, which needs to be bought today because the centrally planned economy says so, and you may get VIP treatment at the airport. You get a high score and preferential treatment because you're leading the way by doing your civic duty and it's automatically "told" that that's the case.
>
> Trevor and I are not futurists when we talk about this. This is a present thing. It just isn't entirely clear yet how and when it works and how it is in fact doing this. The Chinese,

> weirdly to their credit, are actually completely open about it. It took Edward Snowden for us to learn that the NSA has the same plan. When you fall into the bad credit score in the NSA system and you happen to be a twelve-year old Muslim in Pakistan, you get droned (Paglen & Appelbaum 2016).

Il faut reconnaître chez Appelbaum le sens de l'image davantage que celui de la nuance. Néanmoins, le portrait qu'il dresse avec son partenaire de création n'est pas si distant des tendances sociales actuelles. Pour les artistes-activistes, la surveillance numérique sert, pour le moment, des visées principalement capitalistes. Dans le futur, elle risque toutefois d'étendre sa portée sécuritaire. Dans les deux cas, le contrôle fonctionne à travers la modulation des droits et privilèges des individus. Dans la société de contrôle, tous n'ont pas les mêmes accès comme le suggérait Deleuze il y a un quart de siècle. La particularité du temps présent, disent Paglen et Appelbaum, est l'automatisation des processus de contrôle. La surveillance n'est plus le fait du travail d'espions aux aguets. Elle est automatisée à travers le déploiement d'appareils et d'infrastructures de surveillance qui repèrent les individus et distribuent en temps réel les bénéfices ou imposent les contraintes.

La surveillance de masse observée jusqu'à présent montre que toute mobilité numérique est potentiellement inscrite dans un narratif de sécurité, striant l'univers numérique en espace de contrôle fluide et permanent. Cette insertion du numérique au cœur de la logique sécuritaire s'inscrit en parallèle à l'extension de la société de contrôle déjà observée. Pour Amoore, le dispositif de sécurité maximise le contrôle sur les mobilités en restructurant l'environnement quotidien. Portant son attention vers l'utilisation des puces RFID (« radio frequency identification », identification par radio fréquence) pour la mise en place des frontières intelligentes, notamment américaines et britanniques, l'auteure suggère que ces technologies permettent la localisation permanente des individus et objets. Ces technologies « sans contact » concrétisent « the dream of the security apparatus, as seen through Foucault's eyes: departing a city that "encloses," "checks," and "regulates" and embracing an urban world that "is given freedom," the "possibility of movement," and the "freedom of circulation" » (Amoore 2013, 115). Les puces RFID permettent de réconcilier les contraintes de mouvement créées par les impératifs de contrôle de la sécurité et le besoin de mobilité et de fluidité de l'économie moderne.

La mobilité accrue de l'ennemi et son imprévisibilité, la difficulté à l'identifier et à le départager de la population civile transforme l'action de cibler note Amoore. Cibler nécessite désormais de pouvoir localiser au préalable un ennemi fuyant. « The *identification*, *localization*,

naming, and *depiction* of mobile targets is, in this war by other means, conducted in and through daily life, in advance of any possible future strike or intervention, » écrit-elle.

> The targeting of mobile bodies, things, objects or monies is becoming a matter of locating—positioning in the sights, if you like—so that the opportunities of a mobile global economy might be seized, while the capability to take out the target remains. "Freedom is nothing but the correlative of the deployment of apparatuses of security", states Foucault, "the very possibility of movement, change of place, and processes of circulation of both people and things" (Amoore 2009a, 58–59).

Malgré les risques associés à cette mobilité, celle-ci est nécessaire à l'économie mondialisée. L'économie (néo)libérale est une économie de laissez-faire, et d'acteurs rationnels et libres où la profitabilité provient de la prise de risques (Amoore 2013, 117). Plutôt que de travailler contre la mobilité, les technologies RFID démontrent de quelle façon les dispositifs de sécurité occidentaux profitent de cette mobilité pour accroître leur contrôle sur les objets et personnes qui y circulent.

Si les zones de guerre demeurent visiblement striées comme le laisse entendre Stefka Hristova (Hristova 2014), les villes modernes apparaissent quant à elles de plus en plus lisses. La striation de l'espace urbain par le système d'adresse est supplantée par le déploiement d'une infrastructure de contrôle largement invisible, intégré dans l'environnement, répondant aux exigences de mobilité en continu des personnes, des biens et des capitaux. Les technologies numériques, notamment les récepteurs/émetteurs RFID qui occupent l'espace urbain dans les transports publics, dans les commerces, etc., rendent possible une localisation de plus en plus rapide, voire en temps réel, et sont par conséquent propices pour la reconnaissance en mouvement (Amoore 2009a, 60). Pourtant, ceux-ci sont au cœur des transactions et des mobilités, autorisant (ou refusant) les achats ou le passage, promouvant un accès libre à l'économie mondialisée tout en assurant le contrôle des circulations. « Where RFID appears to render movement around the subways, highways, and superstores of the global economy as a smooth and seamless experience, it aligns the security practices of the state with the mobilities of the consumer » (Amoore 2013, 122). La technologie répond aux fantasmes de liberté de chacun : les consommateurs peuvent consommer sans contrainte, le dispositif de sécurité, suivre à la trace chaque individu.

La localisation (« locatability ») est ainsi une fonction et stratégie du dispositif de sécurité pour maximiser les profits et minimiser les risques. Les technologies numériques possèdent ces caractéristiques nécessaires au contrôle des mobilités dans un espace lisse que sont l'invisibilité et l'automatisation du système (Amoore 2009a, 60). Elles lient en outre les transactions présentes à

celles passées et futures à travers son interconnectabilité avec les autres bases de données existantes (Amoore 2013, 115). Pourtant, l'invisibilité des contrôles ne doit pas faire oublier leur présence ni leurs conséquences. « The appearance of smooth space, » écrit Amoore,

> of course, conceals the intense striations of the integrated databases and fractionated risk scores… Where RFID "pleasures and anxieties cohabit," the economy of circulation meets security so that, for some, "the edges are smoothed" as they "blend seamlessly into the crowd." For others, of course, the locative device targets heightened exposure to visibility—to stop and search, to continually verify identity, to have movement in public space checked and intercepted (Amoore 2013, 123–124).

Les conséquences de ce contrôle ciblé sont multiples : calcul des cotes de crédits par les institutions financières et des primes par les assureurs, évaluations préventives des futurs locataires et employés, détection des fraudes automatisées refusant sans explication certaines transactions (Christl 2017, 27–39), facturation différenciée selon le profil de l'acheteur (Cheney-Lippold 2011), détermination algorithmique de l'âme sœur (Cheney-Lippold 2017a, 182–186), autorisation de traverser les frontières (Pallister-Wilkins 2016; Adey 2006). En Chine, cela va même jusqu'à la mise en place d'un système de crédit social prévu pour 2020 ayant pour but « to encourage positive economic and moral behaviours (Kshetri 2016), in order to "ensure that sincerity and trustworthiness become conscious norms of action among all the people" (China Copyright and Media 2015) » (Cinnamon 2017, 617).

L'univers numérique n'échappe pas à la stratégie de localisation et de contrôle où les sphères économiques et sécuritaires se superposent, la seconde mobilisant les données produites par la première. Ce qui y transite devient une source permanente de savoir de sécurité. Toute information, aussi triviale puisse-t-elle apparaître, se retrouve dans la mire sécuritaire. Mais Internet ne fait pas que véhiculer des informations, il est aussi producteur de données. L'univers numérique en apparence sans barrière ni frontière est en réalité un espace de contrôle où tout et tous doivent être visibles. Certes, en Occident, les barrières à la mobilité numérique sont souvent faibles. Le contrôle d'accès au contenu d'un site Web en fonction de l'origine de l'utilisateur, identifiée par son adresse IP, constitue un exemple de barrière, tout comme la promotion ou le retrait de certains sites ou produits par des plateformes dominantes comme Google, Facebook, Apple Store ou Spotify. Ces barrières ont cependant une portée réduite particulièrement pour qui maîtrise les rouages informatiques. Dans certains cas, comme sur l'Internet clandestin ou anonyme (« dark web »), les barrières semblent tout simplement inexistantes. Amoore suggère déjà que dans

un contexte de contrôle les barrières ne servent pas uniquement à intercepter. Le rôle des points de contrôle mis en place avec les technologies RFID n'est pas tant d'interdire que de maximiser les profits de la circulation. « [T]he sovereign, » écrit-elle, « is no longer establishing limits of restricting movement but is in fact establishing the impossibility of limits and finding novel ways to, as Foucault describes it, "live dangerously" » (Amoore 2013, 123). Polly Pallister-Wilkins va dans la même direction. Selon l'auteure, les barrières même physiques n'ont pas qu'une fonction d'interruption. Elles permettent aussi la capture, ou la production, de données. Ces données, explique-t-elle, sont ensuite réintégrées dans des assemblages de pouvoir, parfois déconnectées avec la fonction originale de la barrière. L'objet technologique de la barrière acquiert ainsi une fonction de gestion sociale. « [S]ecurity barriers, » écrit Pallister-Wilkins,

> not only channel and check, but also capture, categorize and create particular sets of data about the populations they govern, which makes them productive technologies, producing the very datasets that come to make up knowledge about particular populations. … As devices of data capture, security barriers come to produce the data that are often used, at a later time or in another place, to govern movement and wider (in)securities (Pallister-Wilkins 2016, 6–8).

La suggestion de Pallister-Wilkins éclaire le fonctionnement des barrières numériques. Si l'espace numérique apparaît lisse et sans contrainte, laissant l'utilisateur s'y mouvoir sans restriction, son organisation demeure fracturée, comme le rappellent d'ailleurs le projet IXmaps et les cartes de TREASUREMAP, par un nombre important de points de passage. Si elles assurent pour l'instant qu'un rôle d'interception réduit — quoique l'apparente fin de la neutralité d'Internet puisse venir changer la situation —, ces barrières sont productrices de données, générées en continu et en quantité. Les barrières sont des lieux de visibilité où l'individu doit être vu. Les données, d'abord générées pour permettre le fonctionnement des technologies de communication puis à des fins économiques, sont ensuite échangées entre les acteurs économiques et étatiques et insérées dans des mécanismes de contrôle capitalistes néolibéraux ou sécuritaires (Cinnamon 2017; Amoore 2013). Par cette circulation, la production de données par les barrières numériques participe ainsi à la mise en place d'outils de gestion sociale par la localisation.

L'impératif de localisation du dispositif de sécurité se comprend au regard de l'étendue des filets la NSA et de ses consœurs dont il a déjà été question, et des efforts déployés par les autorités pour combattre la cryptographie. Ces derniers offrent un indicateur de la crainte que suscite l'invisibilité numérique. Dans un document stratégique, l'agence faisait de la cryptanalyse un de

ses cinq principaux objectifs. Ainsi a-t-elle dans ses plans « [to b]olster our arsenal of capabilities against the most critical cryptanalytic challenges … and [to c] ounter the challenge of ubiquitous, strong, commercial network encryption ». Le déchiffrement constitue une étape nécessaire « [to d]efeat adversary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere » (NSA 2012c, 4). Pour percer les structures d'invisibilité, l'agence agit sur plusieurs fronts comme l'ont révélé les journalistes du Guardian et du New York Times (Perlroth, Larson & Shane 2013; J. Ball, Borger & Greenwald 2013; voir aussi Appelbaum et coll. 2014). À travers le projet SIGINT Enabling, financé à hauteur de 250 millions de dollars américains pour l'année 2013, la NSA travaille à convaincre ou forcer les compagnies privées à installer sur leurs produits ou services des portes dérobées (« backdoor ») permettant de faire fi du codage des données. La NSA a ainsi conclu des ententes avec Microsoft lui permettant de contourner la cryptographie de la messagerie instantanée Outlook, et d'obtenir les courriels préencodés des services Outlook et Hotmail (Greenwald et coll. 2013). De façon plus générale, la NSA disait avoir accès aux données des Big Four du numérique : Microsoft, Yahoo!, Facebook et Google[3] (Perlroth, Larson & Shane 2013). La NSA entretient d'ailleurs le Key provisioning service responsable spécifiquement de la gestion de liste des clés de codage obtenues des entreprises (Perlroth, Larson & Shane 2013).

Dans ses efforts pour contourner la cryptographie, la NSA a également infiltré les discussions entourant l'établissement des codes internationaux de cryptographie, instrumentalisant l'US National Institute of Standards and Technology afin qu'elle promeuve son code sur la scène internationale. La NSA a aussi mis au point le programme BULLRUN qui permettrait de contourner le codage lié au protocole HTTPS et aux protocoles de sécurisation Secure Sockets Layers (SSL) utilisés notamment pour le commerce et les transactions financières en ligne (J. Ball, Borger & Greenwald 2013; Perlroth, Larson & Shane 2013). Si les spécificités du programme n'ont pas filtré — celui-ci demeurant très secret au point où la NSA a averti ses employés « there will be NO 'need to know'… Do not ask or speculate on sources or methods underpinning BULLRUN successes, » avertit-elle ses analystes (Perlroth, Larson & Shane 2013) — BULLRUN donnerait accès à un secteur d'Internet jugé jusqu'alors sécuritaire contrecarrant le récent passage d'un grand nombre de sites Web vers le protocole HTTPS. En 2012, la NSA aurait ainsi été capable de percer

[3] Aujourd'hui, l'acronyme GAFA semble montrer une modification des membres du Big Four : la diminution de la part des deux premières au profit d'Amazon et Apple

les chiffrements de 10 millions de communications par jour (Appelbaum et coll. 2014). Les communications téléphoniques ne sont pas en reste. Le programme AURORAGOLD permet de pénétrer les protections du réseau cellulaire 4G standardisées par l'Association GSM représentant les principaux fournisseurs de service de téléphonie mondiaux (Gallagher 2014).

La NSA, en collaboration avec GCHQ, travaille également à pénétrer les réseaux privés, notamment ceux de Yahoo! et Google (Gellman & Soltani 2013b). GCHQ, à travers le programme EDGEHILL, prévoyait quant à elle pouvoir de craquer les réseaux de quinze joueurs majeurs de l'Internet et plus de 300 réseaux virtuels privés (J. Ball, Borger & Greenwald 2013) souvent utilisés à des fins d'anonymat. Sans grande surprise, le réseau Tor, hôte de « very naughty people » (NSA citée par J. Ball, Schneier & Greenwald 2013), constitue également une des cibles des deux agences. La NSA et GCHQ ont déployé une série de programmes exploitant certaines faiblesses de logiciels associés au réseau ou de maladresses de leurs utilisateurs. Ainsi, ont-elles trouvé une faille dans le navigateur Firefox à la source du navigateur Tor — faille qui a par la suite été comblée lors d'une mise à jour de sécurité — et ont-elles eu accès à quelques (« very few ») relais du réseau. Aussi, réussissent-elles à exploiter directement certains utilisateurs. La connexion initiale d'un utilisateur au réseau Tor est, en effet, publique. Tor garantit l'anonymat en cachant un utilisateur du réseau dans la masse des utilisateurs, mais la connexion au réseau est connue. Les agences ont profité de ce moment de visibilité pour cibler certains utilisateurs. Malgré cela, selon les documents datés de 2013, certes une éternité dans le monde numérique, les agences seraient incapables de percer le réseau dans son ensemble. « We will never be able to de-anonymize all Tor users all the time, » est-il écrit dans la présentation intitulée Tor Stinks. « With manual analysis we can de-anonymize a very small fraction of Tor users, however, no success de-anonymizing a user … on demand » (NSA 2012b). La NSA et le GCHQ sont au mieux en mesure d'identifier et de suivre un certain nombre d'utilisateurs à la fois (J. Ball, Schneier & Greenwald 2013).

Les efforts de localisation du dispositif de sécurité se doublent d'un impératif de visibilité pour le sujet numérique. Comme le rappelle Foucault, chaque structure de pouvoir produit un sujet. Le monde numérique n'y fait pas exception. L'individu est un utilisateur libre de consommer les produits et services qui correspondent le mieux à ses désirs. L'utilisateur est aussi producteur de l'univers numérique lorsqu'il bloque les messages impertinents ou publicités mal-dirigées ou identifie un ami sur une photo ou « aime » un événement ou une organisation. « The net result, » écrit Hu,

> is that we have become willing partners with the algorithms that channel our online experience. Interpellated as "users," we identify with use and use value, and therefore mend and build the gates that keep us within a zone of productivity online. It is … a kind of active consumerism (Hu 2015, 64).

L'utilisateur se comprend ainsi en lien avec le néolibéralisme ambiant qui, comme le résume David Harvey, « propos[es] that human well-being can best be advanced by the maximization of entrepreneurial freedoms within an institutional framework characterized by private property rights, individual liberty, unencumbered markets, and free trade » (Harvey cité par J. E. Cohen 2016, 222). L'utilisateur est mobilisé comme producteur de contenu Internet, mais il l'est également à des fins de sécurité.

La rationalité de sécurité se tourne vers le quotidien, notamment l'univers numérique, afin d'identifier et préempter les risques à la stabilité d'Internet et de l'État. Actes de piratage divers comme des violations de droits d'auteur, des vols d'information ou d'identité, attaques par déni de service (DDoS — « Distributed Denial of Service ») touchant des infrastructures névralgiques, fuites de documents classifiés vers des sites de diffusion libre comme WikiLeaks, production de contenu indésirable ou immoral comme des théories du complot, des fausses nouvelles ou de la pornographie infantile, le monde numérique serait soumis à un nombre croissant de dangers. « [T]he networks of power that govern us always seem to contain or even produce the fantasy of another network: the deviant network », écrit Tung-Hui Hu (Hu 2015, 84), d'où la mission de cyberdéfense de la NSA ou la décision de mettre en place un centre d'expertise de l'OTAN dédié à la cyberdéfense (Kaiser 2015).

Comme dans les discours de résilience qui demandent la participation de l'individu, l'utilisateur n'échappe pas à cette mobilisation, le dispositif de sécurité lui enjoignant certaines tâches telles que sa propre protection contre les actes de piratage et plus globalement la protection d'Internet contre les menaces provenant de réseaux déviants. « "[W]ar as big data" produces the subject position of a user, that is, a subject that actively participates in securing the system as a whole, » suggère Hu.

> Likewise, the cloud's disaster recovery functions make disasters and security threats continuously imaginable. When users are responsible for selecting privacy settings, making disaster recovery backups, and even flagging suspicious behavior online, security becomes an everyday responsibility. One of the most unique aspects of digital culture is therefore a user's ability not just to become a target, but also to defend him—or herself, "target back," and participate in a shared project of security with the state (Hu 2015, 113–114).

L'observation d'Hu est juste lorsque la menace perçue contre Internet provient de pirates. L'on ne saurait toutefois limiter la sécurisation de l'univers numérique à la défense du réseau. Elle procède aussi de la sécurisation de tout ce qui y transite. À ce titre, si l'utilisateur doit assurer la protection de ses données contre les intrusions malicieuses, il doit en même temps demeurer transparent. La sécurisation de l'univers numérique s'accompagne d'une participation qui passe par un impératif de visibilité. En bon consommateur, l'utilisateur doit veiller à l'essor de l'économie numérique. En bon citoyen numérique, celui-ci qui n'a rien à cacher doit participer à la défense de l'État en montrant patte blanche et en n'éveillant aucun soupçon sur son identité et ses intentions. Se protéger, protéger l'État, mais aussi demeurer visible sont des tâches imparties à l'utilisateur.

Dans cette ère numérique, la visibilité est de mise, l'invisibilité est suspecte. En même temps, cet impératif de visibilité est aussi inégal qu'il est paradoxal. Il est inégal, car si Giorgio Agamben (Agamben 2013) relève que chacun peut potentiellement devenir objet de sécurité, cela ne signifie pas pour autant que tout utilisateur devienne nécessairement une personne d'intérêt. Alors que la surveillance de masse tend vers une sécurisation à l'infini de l'univers numérique, la présence de sélecteurs et le processus d'opérationnalisation du savoir de sécurité suggèrent que tous ne sont pas également soumis à la surveillance de sécurité. Certains sont plus susceptibles d'être sujets à la surveillance de sécurité. Dans le contexte de l'identification du terrorisme islamique comme menace principale à la sécurité des États occidentaux, les individus arabes, de confession musulmane ou en contact avec les États refuges pour les terroristes comme la Somalie, le Pakistan ou les Philippines, apparaissent être des cibles de premier choix. La logique du risque statistique fonctionne sur la détermination de catégories, ou profils, à partir desquels mener les politiques de sécurité, et plus largement la gouvernance de la société. Or, le profilage accentue la pression sur les individus appartenant aux groupes en question, accroissant du coup les dangers de surreprésentation de ces individus dans les interventions de sécurité ou, pour reprendre une terminologie associée aux algorithmes, de faux positifs. Si, comme le suggère Oscar H. Gandy Jr., ce type de discrimination statistique peut être rationnellement expliqué, le profilage n'en demeure pas moins associé à une discrimination raciale illégale en vertu du droit occidental et cible de façon récursive les individus les plus marginalisés dans la société contribuant à accentuer les inégalités sociales (Gandy 2012). Dans cette perspective, la caractéristique distinctive de la surveillance de sécurité n'est plus sa nature indiscriminée, mais au contraire, son effet discriminatoire.

Paradoxalement, alors que l'on essaie de réduire la visibilité politique des classes inférieures et des marginaux, la visibilité sécuritaire de ces groupes est essentielle au maintien de l'ordre, malgré les risques que cela représente pour les individus. Les cas de violence contre la population noire américaine sont emblématiques de ce paradoxe de visibilité. Trayvon Martin, jeune homme noir de 17 ans tué en 2012 par le vigile civil George Zimmerman, a été abattu parce qu'il refusait de s'identifier. Sa présence qui semblait « up to no good » aux yeux de Zimmerman devenait menaçante (Zimmerman cité par Teasly et coll. 2018, 37). Cet exemple n'est pas unique. Depuis, Michael Brown, Eric Garner, Tamir Rice, Freddie Gray sont tous devenus de tristes symboles de la brutalité policière à laquelle est confrontée la population noire américaine. La surreprésentation des hommes noirs comme sujet des interventions policières, par exemple dans les opérations de contrôle de routine des conducteurs d'automobiles dites « stop and search » (Teasly et coll. 2018, 38-39) tend à indiquer des pratiques de profilage racial de la part des autorités et des exigences particulières de visibilité pour cette population. Comme l'écrit Russell Rickford,

> mass incarceration and the techniques of racialized policing on which it depends—"broken windows," stop-and-frisk, "predictive policing," and other extreme forms of surveillance—have exposed the refurbished, but no less ruthless, framework of white supremacy. In poorer black and brown communities, recognition that cops serve primarily to monitor and subjugate rather than "to serve and protect" has fostered both deep resentment and radical, oppositional consciousness (Rickford 2016, 38).

Cette visibilité est dangereuse : selon des données compilées par le Washington Post, en 2015, 40 % des hommes non armés morts suite à une intervention policière sont noirs alors qu'ils ne représentent que 6 % de la population américaine (Chernega 2016, 242). Des parallèles similaires existent également avec la population latino-américaine confrontée à des contrôles abusifs ou avec la population arabo-musulmane. En février 2012, Matt Apuzzo et Adam Goldman révélaient que le service de police de la ville de New York, dans le cadre du Demographics Unit et en collaboration avec la CIA, procédait à une surveillance étroite et à une cartographie de la communauté musulmane des États de New York, du New Jersey et du Connecticut (Hawley 2012; Goldman & Apuzzo 2012). Le NYPD aurait surveillé des mosquées, des groupes communautaires, des restaurants et des centres d'entraînement notamment soulevant des critiques de profilage racial et contre l'exercice du pouvoir du NYPD au-delà de son territoire (Apuzzo, Goldman & Sarsour 2013).

Les impératifs de visibilité accentuent les pressions sur les groupes profilés. Le dispositif de sécurité de la société de contrôle joue de l'accélération et du ralentissement des mobilités au profit de la stabilité et de prospérité des économies néolibérales en mettant en place des infrastructures de contrôle des flux de circulation des personnes et des objets physiques et immatériels. Les contrôles aux aéroports, le passage des frontières et les privilèges financiers offrent autant d'exemples de la vitesse et de la liberté de déplacement et de consommation des individus privilégiés, alors que la mise en place de clôtures aux frontières, de camp de détention d'immigrants ou le refus de crédit matérialisent les contraintes au mouvement voire l'immobilité des déclassés.

L'ambivalence entre l'universalité de la surveillance de masse et ses effets discriminatoires ne semble pas jeter d'ombre, aux yeux de Paglen et Appelbaum, sur la contribution de l'anonymat numérique à la justice sociale. Pas plus que les attaques menées contre le réseau Tor ne semblent ébranler la confiance en son efficacité pour assurer l'anonymat numérique. Discutant des difficultés qu'éprouveraient toujours la NSA et son partenaire britannique à percer certains programmes de chiffrement et le réseau Tor, Appelbaum et ses coauteurs du Spiegel écrivaient ainsi : « [t]o a certain extent, the Snowden documents should provide some level of relief to people who thought nothing could stop the NSA in its unquenchable thirst to collect data. It appears secure channels still exist for communication » (Appelbaum et coll. 2014). L'anonymat qu'offrent *Autonomy Cube* et Tor est à l'avis de Paglen et Appelbaum nécessaire à la préservation de la démocratie contre l'expansion d'une société de contrôle totalitaire en protégeant la liberté d'exploration, la liberté d'expression et la vie privée puisque le droit ne semble plus une mesure efficace contre les pratiques de surveillance. La démarche est étrangement résiliente et utopiste, résolument politique.

6.3 L'autonomie individuelle, une démarche collective

La maîtrise des technologies permet la création de havres numériques : un espace, comme le nom de l'œuvre le suggère, d'autonomie au cœur d'un monde soumis à la surveillance. Par leur démarche, la connexion que les artistes-activistes établissent entre anonymat et autonomie politise la notion de vie privée. Paglen et Appelbaum ne rejetteraient probablement pas la notion de vie privée comme sanctuaire du soi, essentiel à l'intégrité individuelle au bien-être spirituel, émotionnel et intellectuel et au bonheur individuel qui définit le concept dans le droit américain depuis la fin du 19^{e} siècle (Cheney-Lippold 2017a, 201-216). Pour le duo, l'anonymat et

l'autonomie permettent l'autodétermination. « Within autonomy there is the idea of self-determination, » explique Paglen en entrevue. Dans le contexte actuel, l'atteinte de cet objectif est particulièrement difficile. « Self-determination is something that's very difficult to engage with in an environment of mass surveillance and political repression, like the conditions we live in today » (Aikens & Paglen 2016). Cela l'est plus encore sur une base individuelle. Elle nécessite une intervention collective, la construction d'un monde alternatif, qui permettra l'autodétermination. « [T]his project goes beyond resistance by building an alternative. It is real and it is the best thing that we have, » explique Appelbaum.

> Part of what we want to do is to inspire other people past the security nihilism that brings us into a passive place where we don't critique the system anymore because we feel disempowered, where we don't speak because mass surveillance silences us, where we say there's nothing to be done because technology alienates us. If we can imagine something different, we might participate in another way. In fact, we could build a different world (Paglen & Appelbaum 2016).

Si les artistes-activistes font avec leur œuvre la promotion du réseau Tor auprès d'utilisateurs potentiels, la recherche de l'autodétermination ne peut se limiter à une entreprise individuelle. Ainsi, partageraient-ils probablement les observations de Cheney-Lippold sur les tensions créées par la surveillance numérique sur l'intégrité des individus. Certes, à travers la constitution de doubles numériques par les algorithmes des entreprises et gouvernements, les individus perdent le contrôle sur leur identité. Certes, l'incompréhension des modes de gestion sociale algorithmique complique pour les individus la pratique de la vie privée et la défense de son intégrité. Face à la surveillance numérique, nous n'avons pas su développer ces réflexes, tels parler à voix basse, fermer la porte ou tirer le rideau, exécutés machinalement dans d'autres contextes quotidiens où l'on recherche une plus grande intimé (Cheney-Lippold 2017a, 212-216). Pour Paglen et Appelbaum, les infrastructures de communication actuelles compromettent l'autodétermination individuelle et collective. *Autonomy Cube* est une pièce additionnelle dans l'établissement d'une structure plus vaste de communication alternative. « In a small way a tool like Tor—and this is why Tor was invented—is a way to try and give marginalized people or oppressed people a means to circumvent structures of oppression, with the goal of promoting self-determination and autonomy, » suggère Paglen (Aikens & Paglen 2016). Le rôle de l'œuvre, rappellent-ils d'ailleurs, n'est pas simplement d'assurer l'anonymat des spectateurs des musées où l'œuvre est exposée, mais de contribuer à la création d'un réseau plus performant.

Les limites de l'autonomie individuelle et la nécessaire collectivisation des démarches d'autodétermination se manifestent également dans la critique institutionnelle du musée. *Autonomy Cube* s'inspire des projets *Systems Work* (1970 jusqu'à aujourd'hui) de Hans Haacke qui interroge et expose les conditions sociologiques de l'art et les liens entre les institutions artistiques et économiques, et *Condensation Cube* (Aikens & Paglen 2016).

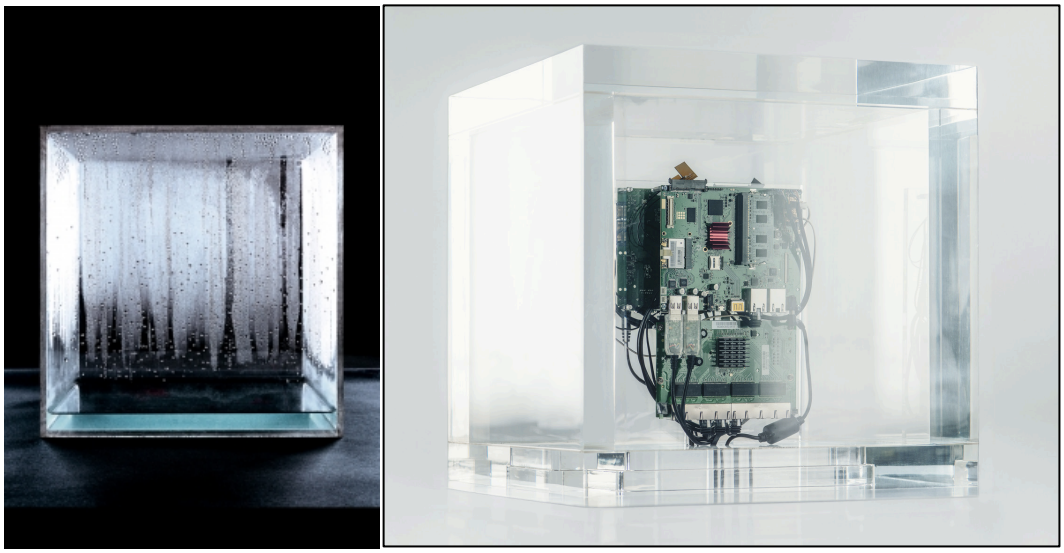


Figure 6.4 : Citation visuelle et emprunt conceptuel
Condensation Cube de Hans Haacke et Autonomy Cube de Trevor Paglen et Jacob Appelbaum (sources : MACBA 2018; Edith-Russ-Haus for Media Art 2015)

À l'instar de Haacke qui décrie la participation des institutions culturelles dans l'industrie du divertissement (Carrillo & Haacke 2006, 3), Paglen et Appelbaum s'insurgent contre le manque de réflexion sur la place qu'occupent ces institutions dans la promotion de la liberté d'expression et la défense de la démocratie. La surveillance numérique brime l'autonomie des individus au profit d'un capitalisme de surveillance, selon le terme de Shoshana Zuboff (Zuboff 2015), lui-même annexé à la logique sécuritaire. Cette économie de la surveillance, résume Tuukka Lehtiniemi, « monetizes data acquired through surveillance. It operates on data extracted from users, turns extracted data into behavioral predictions, and often monetizes them through markets that users cannot participate in » (Lehtiniemi 2017). Malgré l'apparente place offerte à la participation des utilisateurs, l'opacité du système, l'inégalité et l'absence de réciprocité entre les individus et les acteurs institutionnels limitent l'autodétermination individuelle et collective (voir aussi Cinnamon 2017; Andrejevic 2007), sans compter les pratiques discriminatoires et exclusives du dispositif de sécurité.

Autonomy Cube rejette ainsi la prétendue autonomie de l'art. Les artistes-activistes reprennent à leur compte la critique de Haacke voulant que l'art ne soit pas extérieur au monde dans lequel il habite (Carrillo & Haacke 2006). À la différence de *Systems Work* toutefois, *Autonomy Cube* ne se limite pas à exposer un problème, mais propose des moyens pour le contourner. « *Autonomy Cube* isn't actually exposing anything but it is descended from that tradition in the sense that it is intimately integrated within the nuts and bolts of the institution, » explique Paglen.

> But instead of being critical it tries to help the institution become more of a civic space as well as contribute to a more civic version of the Internet. If we understand infrastructure is how politics is imbedded in a kind of social and political script, this is a proposal for an object that has different social and political scripts associated with it that as a result feed into the institution (Aikens & Paglen 2016).

Les institutions muséales ne peuvent faire fi de la société contemporaine et de la présence de la surveillance. Présentant son exposition, l'Edith-Russ-Haus, cite ainsi Glenn Greenwald qui rappelle la centralité d'Internet :

> … the Internet is not some standalone, separate domain where a few of life's functions are carried out. … Rather, it is the epicenter of our world, the place where virtually everything is done. It is where friends are made, where books and films are chosen, where political activism is organized, where the most private data is created and stored. It is where we develop and express our very personality and sense of self (Greenwald cité par Edith-Russ-Haus for Media Art 2015).

La présentation poursuit :

> In developing an entire exhibition around a single artwork, the Edith-Russ-Haus seeks to make a statement on the proliferation of surveillance technology upon our daily lives, and the disconcerting obliviousness of public knowledge on this issue. An issue that risks transforming open societies into control states (Edith-Russ-Haus for Media Art 2015).

Face à l'attaque que subit Internet, les institutions muséales qui se targuent d'être des espaces de créations et de critiques doivent se positionner, devenir des cubes protégeant l'autonomie. Pour Paglen, le courant artistique autonomiste est « a beautiful idea, but it doesn't work. Or rather, it's a theoretical argument that's hard to actualize » (Aikens & Paglen 2016). Au contraire, l'œuvre montre et matérialise une forme d'autonomie qui ne peut être garantie que par la collectivité.

> Using the word "autonomy" in the title of the work was deliberately meant to poke at art theory a bit. We figured it was obvious that because the piece can only function by being part of a larger volunteer network of Tor relays (of which "Autonomy Cube" is one), we

> were suggesting a very different notion of autonomy than the classical modernist formulation. There's nothing autonomous at all about the piece—it's utterly dependent on being part of a larger array of people and institutions working together to create volunteer-run, open-source and secure networking protocols and infrastructures. So in that sense, whatever "autonomy" can be conferred on a user by providing them with privacy-enhancing tools and infrastructures is only possible through collective effort. We thought it was obvious that in this case, we were proposing something closer to an anarchist notion of autonomy (Lind 2016).

Si Paglen préfère la conception anarchiste de l'autonomie à celle de l'esthétique, il n'offre toutefois pas davantage de précision sur le sens du concept. Théoricien anarchiste, James C. Scott situe la notion d'autonomie, ainsi que celle de liberté et de réciprocité, au cœur de l'anarchisme (J. C. Scott 2012, 55). Les trois valeurs sont intrinsèquement liées. L'autonomie fait référence à la possibilité, pour un individu ou une collectivité, de choisir. Ainsi, dans le pamphlet From Democracy to Freedom, écrit pour la série The Anarchist Critique of Democracy et publié sur le site anarchiste CrimethInc.[4], l'autonomie se définit comme « the ability to act freely on one's own initiative » (2016a). Ce qui est imposé ne peut être une action autonome (J. C. Scott 2012, 1). Une action est autonome seulement si elle est libre, mais l'autonomie, suggère Scott, est aussi une aspiration. « [T]he desire for autonomy, for control over the working day and the sense of freedom and self-respect such control provides, » écrit-il, « is a vastly underestimated social aspiration for much of the world's population » (J. C. Scott 2012, 55). D'où son commentaire on ne peut plus hérétique sur la nécessité de reconnaître la légitimité de l'accumulation petite-bourgeoise vue comme la défense de leur autonomie face au capitalisme. D'où, plus généralement, la recherche d'un mode d'organisation sociale qui saurait protéger la liberté de tous et assurer leur aspiration pour l'autonomie. Dans le même ordre d'idée, David Graeber, anthropologue anarchiste et figure phare du mouvement Occupy Wall Street, insiste également sur l'absence de contrainte dans sa définition de la liberté et de l'anarchisme. « Anarchism, » écrit-il,

> is a political movement that aims to bring about a genuinely free society—and that defines a "free society" as one where humans only enter those kinds of relations with one another that would not have to be enforced by the constant threat of violence. … Anarchists thus envision a world based on equality and solidarity, in which human beings would be free to

[4] CrimethInc. se présente comme « an anonymous network of anarchists and insurgents, a desperate measure against quantification and computation, a flaming hearse for the hierarchies of our age ». Tous les textes y sont publiés anonymement, protégeant les auteurs contre les représailles et reproduisant la structure des groupes d'affinité. Chacun et tous peuvent faire partie d'un groupe d'affinité et être, nonobstant son apparence quotidienne, de réels partisans anarchistes. L'anonymat du réseau symbolise ainsi cette idée de la diffusion de l'avant-garde. Parallèlement, elle pratique l'horizontalité des idées et empêche le fétichisme des personnalités (voir 2018).

> associate with one another to pursue an endless variety of visions, projects, and conceptions of what they find valuable in life (Graeber 2013, 187–188).

L'anarchisme refuse la coercition et la violence et permet, tant aux individus qu'aux collectivités, de décider pour eux-mêmes, en d'autres mots de s'autodéterminer. Pour l'anarchisme, l'individu et la collectivité sont indissociables. Contrairement aux notions de liberté à somme nulle, où la liberté de l'un s'arrête où débute celle de l'autre, et de liberté comme protection individuelle vis-à-vis des autorités, la liberté dans la perspective anarchiste est dite cumulative ou sociale. « I am truly free only when all human beings, men and women, are equally free. The freedom of others, far from negating or limiting my freedom, is, on the contrary, its necessary premise and confirmation, » écrivait Mikhaïl Bakounine (Bakounine cité par 2016a). Il n'y a pas de liberté pour un si tous ne sont pas libres : « it approaches liberty as a collectively produced relationship to our potential, not a static bubble of private rights » (2016a). Dans la même logique, l'autonomie ne peut être restreinte à un seul. L'autonomie d'un seul s'apparente davantage à l'exercice de l'autorité sur les autres. « By contrast, self-determination means disposing of one's potential on one's own terms: when people engage in it together, they are not ruling each other, but fostering cumulative autonomy » (2016a). Autonomie, liberté et réciprocité vont de pair.

Critique de la démocratie libérale ou représentative, qui ne livrerait pas ses promesses d'égalité, d'inclusion, et d'autodétermination en remettant entre les mains d'une majorité souvent privilégiée les pouvoirs coercitifs du gouvernement, l'anarchisme propose l'horizontalité, la décentralisation et l'autonomie (2016a). Dans cet objectif, l'anarchisme opte pour une structure organisationnelle consensuelle qui s'assure qu'aucune mesure coercitive ne doit être imposée. Afin de protester contre les structures de pouvoir sans en reproduire les dérives autoritaires, l'anarchisme

> seek[s] to respect others' autonomy by not subjecting them to actions that violate their consent—that is, by staying within the boundaries of others' desires as they determine and articulate them. We reject coercion of any form, whether physical, verbal, economic, or otherwise, and assert our self-determination to participate in or abstain from whatever we choose (2012a).

Le consensus reconnaît et promeut également chaque individu comme acteur politique à part entière (J. C. Scott 2012, xxiii). La parole au « je » de l'individu renforce le collectif comme la somme de solidarités individuelles plutôt que la soumission des individus à une identité unique que l'on retrouve généralement dans les organisations politiques telles que les syndicats, et pourrait-on ajouter les États. Ainsi Christophe Aguiton et Nicolas Haeringer décrivent les pratiques internes

des mouvements d'occupation anarchiste qui apparurent à travers l'Amérique du Nord et l'Europe en 2011.

> [L]e « nous », cher aux mouvements sociaux et aux syndicats, est remplacé par le « je ». Le poids ainsi donné à l'individu ne veut pas dire qu'il ne s'agit que d'additionner des egos et de fortes personnalités. Au contraire : ces mouvements sont marqués par la volonté de créer du collectif et de la solidarité, à partir de l'autonomie de chacun-e. Le préalable est donc d'accepter que chaque voix ne parle que pour un-e — un choix organisationnel qui tranche avec ceux faits par les syndicats et les associations (en interne comme dans leurs espaces de coordination) dans lesquels chaque représentant parle pour plusieurs (Aguiton & Haeringer 2012, 123).

Ainsi, face aux désaccords pouvant émerger des consensus, certains vont-ils jusqu'à promouvoir la dissociation de groupes et la flexibilité des configurations collectives afin d'assurer l'autonomie de chacun. « Disagreeing and dissociating can be just as desirable as reaching agreement, provided they occur for the right reasons, » suggère-t-on (2016a). Surtout, il faut s'assurer que respecter le droit à l'action de chaque individu, autrement le consensus risque trop souvent de mener à l'inaction. « [W]e don't need a more participatory—and therefore even more inefficient and invasive—form of government, » propose l'auteur du pamphlet Occupy: Democracy versus Autonomy. « We need the ability to act freely as we see fit, the common sense to coexist with others wherever possible, and the courage to stand up for ourselves whenever there are real conflicts » (2016b). Après tout, comme le remarque un autre auteur anonyme, s'il avait fallu atteindre un consensus sur l'occupation du Zuccotti Park, Occupy Wall Street n'aurait probablement jamais vu le jour (2012a).

En parallèle à la définition négative de l'autonomie, c'est-à-dire la défense de la liberté de chacun la coercition, l'anarchisme propose une définition positive : la liberté d'entreprendre des actions directes sans avoir à demander la permission. Aguiton et Haeringer précisent :

> Les militants n'entendent en effet pas attendre de l'État qu'il mette en œuvre une politique plus juste, pas plus qu'ils ne se dédient à la construction d'un basculement de type révolutionnaire : ils font le choix d'agir *à la place de*, de manière autonome, quitte à enfreindre la loi et à préférer préfigurer une autre société, plutôt qu'à attendre l'effondrement du système actuel (Aguiton & Haeringer 2012, 122-123).

Trois visées guident les actions directes des anarchistes. La lutte contre les inégalités est à elle seule insuffisante, car les inégalités sont inhérentes aux structures sociales contemporaines. La lutte doit également passer par le changement personnel à travers l'éducation aux valeurs anarchistes afin de briser les moules de contrôles capitalistes et patriarcaux notamment et d'enseigner la pratique de

la liberté et de l'autonomie. Enfin, la préfiguration d'une société anarchiste permet, même si elle est à petite échelle, d'expérimenter avec une alternative sociale libre, autonome et réciproque. La société anarchiste passe notamment à travers le consensus et la création d'espaces de rencontre « where people may open themselves to each other's influence and find others who share their priorities. Encounter means mutual transformation: establishing common points of reference, common concerns » (2016a). Afin d'assurer son autonomie, les individus participants doivent travailler à rendre la société préfigurée autosuffisante. « To be free, you need control over your immediate surroundings and the details of your daily life, » écrit-on dans From Democracy to Freedom.

> No single institution should be able to monopolize access to resources or social relations. A society that promotes autonomy requires what an engineer would call redundancy: a wide range of options and possibilities in every aspect of life. … If we wish to maximize autonomy for everyone rather than simply seeking it for ourselves, we have to create a social context in which no one is able to accumulate institutional power over anyone else (2016a).

L'action directe organisée préfigure une société à l'image des individus qui y participent, où l'ensemble des efforts déployés pour promouvoir la liberté et l'autonomie des individus, en d'autres mots la réalisation du pouvoir des individus face aux structures dominantes, ne visent, dans un effet retour, que la promotion d'un projet partagé. Pour reprendre les mots de Simon Springer, théoricien anarchiste :

> It is in spaces of the public that the discovery of both *power* and *demos* is made, and it is in the contestation of public space that democracy lives. Emancipation must accordingly be understood as an awakening, a (re)discovery of power that is deeply rooted in processes of mobilization and transformation, and in this sense, emancipation cannot be conceived as a subject—object relationship in which some are emancipators (revolutionaries, mavericks, academics) and others are being emancipated (the poor, the propertyless, the marginalized) (Kothari 2005). Either the whole of humanity is liberated, or no one is. This may seem an impossible goal to achieve, but thinking so misinterprets what is at stake. It is not a utopian end state resulting from revolution or consensual deliberation that should be pursued. Instead, through a relational, processual, and forever-protean understanding of space, the aspiration becomes radical democracy viewed as an agonistic *means without end*. Such is the promise of public space (Springer 2010, 555–556).

Autonomy Cube fait écho aux revendications anarchistes. Les artistes-activistes cherchent, à travers l'action directe préfigurant un Internet libre, l'autonomie individuelle et collective : la possibilité, pour ceux qui en font le choix, de naviguer sur Internet anonymement, à l'abri des structures de pouvoir de la société de contrôle. Alors que le courant artistique autonomiste cherche à dépolitiser l'art, à exclure l'œuvre et l'artiste de l'influence et de la charge sociale, Paglen et

Appelbaum affirment la nature politique l'art et de l'autonomie. L'art doit prendre position en concrétisant le principe d'un Internet libre et ouvert. Grâce à *Autonomy Cube*, l'espace muséal servira, à l'image des bibliothèques, de sanctuaire comme la surveillance numérique. En ce sens, le projet partage avec *Condensation Cube*, l'autre influence de Haacke duquel *Autonomy Cube* tire sa facture visuelle, la relation de l'œuvre avec son environnement. L'œuvre de Haacke est un cube de Plexiglas contenant de l'eau. Progressivement, l'eau s'évapore puis se condense, créant des gouttes d'eau le long des parois du cube. Ce cycle est affecté par l'environnement dans lequel se retrouve l'œuvre, notamment par les variations de chaleur engendrées par la présence humaine. *Condensation Cube* est une œuvre conceptuelle. Le Museu d'Art Contemporani de Barcelone, où elle est exposée, décrit ainsi la réflexion derrière le projet :

> This piece summarises Haacke's interest in closed physical systems, biological growth and random movement, while emphasising the idea of art that has lost its representative and referential ability to emerge as a fact or state of affairs. … A physical process as basic as water condensation allows Haacke to redefine not only the work of art as a living system, but, most significantly, the role of the viewer or user of art. While the patterns of water trails within the cube have to do with the conditions of their immediate surroundings, the human presence is also part of this environment. The artwork depends on the physical presence of the viewers who, by their proximity, modify the work unwittingly (MACBA 2018).

Similairement, Paglen et Appelbaum s'interrogent sur l'environnement de l'art, rappellent l'impossibilité de s'isoler définitivement des infrastructures de surveillance. Dans ce contexte, la modulation de l'espace muséale et la participation des spectateurs à réseau Tor est indispensable à la réussite de la protection de l'anonymat. Si l'on ne peut échapper entièrement à la société de contrôle, au moins est-il possible de créer collectivement certains havres favorables à l'autodétermination.

Ni l'art ni les individus ne peuvent prétendre être extérieurs au monde dans lequel ils vivent. L'autonomie et la liberté, propose l'anarchisme, ne se limitent pas à des bulles de protection contre les autres ou contre l'État. Ces deux valeurs fondamentales s'exercent ensemble, et par l'ensemble des individus. Mais si les structures de pouvoir sont inévitables et insèrent l'individu dans un cadre politique, cela signifie également que chaque action peut avoir une portée politique préfigurant un monde différent qui ne sera pas soumis à la surveillance. *Autonomy Cube* politise ainsi le geste de plus en plus anodin de naviguer sur Internet et, prenant une perspective matérialiste, les infrastructures de communication. Tant pour les individus que pour les institutions muséales exposant l'œuvre, la participation Internet devient une opportunité de créer à travers le réseau Tor

un collectif de protection de l'anonymat. Tor et tous ceux qui y contribuent agissent directement sans attendre l'intervention de l'État ou des acteurs dominants de l'économie numérique et sans attendre l'autorisation de qui que ce soit comme le démontre la pression exercée contre le réseau. *Autonomy Cube* préfigure, à travers l'espace du réseau et des musées, un monde différent qui protège, par l'effort de tous, l'anonymat de chacun. L'œuvre fragilise les fondations économiques des entreprises qui monopolisent le numérique et réaffirme Internet comme un lieu de rencontre, de découverte et de transformation individuelle et collective.

6.4 Participation numérique : entre complicité et résistance

En parallèle à la critique matérielle et spatiale des infrastructures de communication et des institutions muséales, la conscientisation à la surveillance numérique menée par *Autonomy Cube* critique l'autonomie de l'utilisateur Internet. Celui-ci ne peut échapper à la surveillance ni se déresponsabiliser de ses effets. En même temps, les opportunités de participer à l'univers numérique sont rapidement appropriées par les structures économiques et sécuritaires du pouvoir. Dans une perspective tant économique que sécuritaire, la possibilité d'interaction qu'offrent les technologies numériques est perçue positivement. « [P]articipation, » écrit Julie E. Cohen, « is framed as the result of uncoordinated, autonomous, inherently democratic choices made by free-market actors » (J. E. Cohen 2016, 207). Pourtant, suggère Cohen, la valorisation de la participation est trompeuse, soumise à l'appropriation marchande des données. Contrairement à ce que peut suggérer le mythe du sujet néolibéral, l'espace numérique semble difficilement réconciliable avec l'autonomie promue par Paglen et Appelbaum alors qu'il détermine davantage qu'il permet l'autodétermination. « The neoliberal framework of the cloud purposely confuses economic intimacy with personal intimacy, » explique Hu.

> … In doing so, the cloud monetizes users through implicit incentives to "use." Through this system, users are continually asked to engage in ever more online activity; to participate in constructing themselves as autonomous subjects; and even to misread economic incentives (such as free disk space) as personal freedoms. … [O]nline expression of any sort is … constrained by this implicit injunction to continually "use more"—and the profits of active use typically accrue to the companies who own online platforms for expression. … Power in the age of postindustrial capitalism, political theorist Maurizio Lazzarato reminds us, is "a technology for creating and controlling the 'subjective processes' … one *has* to express oneself, one *has* to speak" (Hu 2015, 121–122).

Pour Hu, cet appel à la participation de l'utilisateur rend complice d'une structure économique et de pratiques de violences souveraines qui dépassent largement le monde numérique. Même les pratiques de résistance des pirates et autres férus d'informatique sont prises dans ce processus de détournement.

> Seen correctly, a hacktivist's freedom most closely resembles that of a free laborer who contributes online reviews, forum moderation, and source code. Free laborers volunteer their services out of their love for the game, even as they are aware that their labor generates value for others. … [T]o volunteer as a hacker … is to work within a neoliberal system of free labor (Hu 2015, 122).

L'activisme numérique se distance ainsi difficilement de la portée de cette structure du pouvoir. Le réseau Tor illustre à l'avis de Hu la proximité entre résistance et pouvoir. On le rappelle : Tor a été développé à l'origine par des chercheurs associés à la défense américaine. Le réseau devait rendre anonymes les communications gouvernementales et les opérations de surveillance américaines en les camouflant dans une masse de communication civile. Le projet Tor rappelle ainsi que les services policiers utilisent le réseau pour exécuter la surveillance en ligne et visiter des sites Web suspects sans laisser de trace. Dans la même veine, les militaires recourent au réseau pour masquer les activités des agents sur le terrain et surveiller les mouvements insurrectionnels (Tor 2018e). Devenu symbole de résistance contre la NSA, Tor est ironiquement un outil d'invisibilité étroitement surveillé au point de compromettre selon certains une partie de ses efforts d'anonymisation (Ridgway 2017, 383-384). « Reasoning that an anonymous backchannel such as TOR has a higher rate of illicit traffic than public Internet browsing, » résume Hu, « the NSA has even used searches for TOR as a way of targeting potential suspects … leading many cypherpunks to describe TOR as a "NSA honeypot" (i.e., trap) » (Hu 2015, 119). Plus significatif, Hu suggère que Tor ne peut être une solution systémique aux structures de pouvoir numérique. « Using TOR may successfully encrypt an individual user's network traffic, but it does little to solve the larger problem of state surveillance, » écrit-il (Hu 2015, 119). L'individu demeure notamment pris dans une logique d'utilisateur. Au mieux, cela confère-t-il un espace d'évitement, mais encore faudrait-il que le réseau assure ses promesses d'anonymat et maintienne le lien de confiance entre les utilisateurs et Tor.

La sousveillance, autre forme de résistance, n'arrive pas plus à offrir une critique non complice que Tor. La sousveillance, analyse Hu, retourne le regard des subordonnés vers les figures d'autorité dans l'objectif de rééquilibrer les structures de pouvoir (Mann & Ferenbok 2013). Steve

Mann, à l'origine du concept, pratique la sousveillance avec des caméras portatives qui filment le quotidien et la présence invisible de la surveillance. Toutefois, pour Hu, la volonté de rendre visible l'invisible se comprend au-delà des caméras, comme une pratique de l'image. Dénonçant le mensonge et la propagande des images officielles, les pratiques de sousveillance scrutent ces images et les connectent entre elles afin d'établir une réalité de l'image qui serait plus authentique, plus vraie : un réseau d'amateurs surveillant les radios et plans de vols des avions de chasse occidentaux pendant la mission de l'OTAN en Libye pour contourner la propagande de guerre ; des journalistes du Washington Post offrant dans Top Secret America une visualisation de données agrégées sur les entrepreneurs privés pour contourner le secret d'État. Ainsi définie, la sousveillance reproduit le mode de visualisation paranoïaque de la rationalité de réseau. « Portraying themselves as iconoclasts—literally, destroyers of icons or images—» suggère l'auteur,

> hacktivists seek to establish a parallel and alternate ecology of media that is supposedly less prone to manipulation or censorship. If any given image can be duplicitous, the only way to find the truth … is to correlate and situate that image within a network of other images, to look through its duplicitous surface and decode and decrypt the hidden network within the network (Hu 2015, 124).

La recherche de connexions entre les images reproduit, plutôt qu'elle ne conteste, les structures du pouvoir numérique. Les efforts de résistance sont menés par des utilisateurs avides d'action. Alors qu'ils tentent de briser le spectre d'un pouvoir qui s'imposerait sur les individus, les activistes numériques retombent dans la dichotomie commune dans l'imaginaire d'avant-garde qui oppose la lutte masculinisée à la passivité d'une consommation féminisée (Hu 2015, 120). Ces activistes sombrent en outre dans la fièvre du réseau et la croyance que l'interconnectabilité infinie mènera vers la vérité. La fièvre du réseau, rappelle Hu, « is a paranoid epistemology that offers to reveal meaning buried beneath the surface, but also serves to lubricate the market mechanisms by which that meaning was created » en produisant, à travers l'activité numérique, toujours de plus de données nécessaires à l'économie numérique (Hu 2015, 122). Ultimement, pour Hu, l'activisme numérique témoigne d'un désir d'être vu et reconnu nécessaire au sentiment d'existence des utilisateurs (Hu 2015, 130). Le regard inversé ne fragilise pas les structures de pouvoir en place, mais les renforce : « a gaze often confirms and reciprocates. When we gaze at a control society in the hopes of exposing its structures, our gaze ends up acknowledging its right to power » (Hu 2015, 143).

Les efforts de résistance deviennent en définitive complices d'une structure de pouvoir qui, si elle se veut numérique, agit dans le « réel », à travers les frappes de drone ou les blackouts numériques au cours desquels l'armée syrienne multiplie les attaques contre les forces rebelles (Hu 2015, 137). Pour Hu, un problème plus fondamental empêche de comprendre la violence réelle du numérique. La violence numérique n'est pas exclusivement le fait d'actions militaires d'envergure. Elle se situe dans l'action de dividuation des utilisateurs. Les individus devenus utilisateurs sont réduits à des fragments d'eux-mêmes à partir desquels des politiques d'exclusion sont menées. La violence numérique n'est pas exceptionnelle. Au contraire, elle est normalisée au cœur des processus de collecte de données et d'opérationnalisation du savoir de sécurité. « The cloud is a subtle weapon that translates the body into usable information, » écrit Hu.

> Despite this violence, it functions primarily as a banal ideology that convinces us that usability is, in Agamben's words, "'normal' and economical," or that identifying ourselves is the "normal way of registering into the mechanism and transmission of the state."… The mistake is to believe that warlike acts are temporary exceptions to the normal operations of the cloud. … To explain away the brutality of militarized spaces as black sites outside the rule of law—to understand them as exceptions within an economy primarily interested in selling and buying information—is to miss a crucial point. The information economy traffics in bare life, and indeed is only possible through it (Hu 2015, 142).

La souveraineté du code soumet tant les autorités économiques, sécuritaires que les forces qui tentent de s'y opposer. « [T]he sovereignty of data is what enables any user to use the cloud » (Hu 2015, 135). C'est aussi ce qui les contraint et les rend complices.

La critique formulée par Hu à l'encontre de l'activisme numérique est démobilisatrice, sapant l'espace d'autonomie. Pourtant, Hu n'abandonne pas complètement l'idée d'une résistance aux structures du pouvoir numérique. Il propose toutefois qu'elle reconnaisse l'extraordinaire difficulté d'en sortir, la complicité de l'utilisateur et le désir d'être surveillé, mais aussi les inégalités et l'absence de réciprocité entre les surveillants et le surveillés (Hu 2015, 143). Pour ce faire, il suggère de mettre de côté le scepticisme ambiant vis-à-vis des images. À l'instar du travail (auto-)ethnographique que l'on retrouve dans les projets documentaires *How Little We Know of Our Neighbors* (2005) de Rebecca Baron et *Workers Leaving the Googleplex* (2009-2011) d'Andrew Norman Wilson, l'observation des structures de pouvoir permet de recomposer une histoire critique du présent à partir de l'image. « To capture our own sensuous investment in digital culture—where … the digital cloud properly lies—we might begin by mapping the images we see in it » (Hu 2015, 144). D'une certaine façon, des projets comme *Citizen Ex* de James Bridle et

Secret Power de Simon Denny s'inscrivent dans cette démarche d'observation et de visualisation où l'image est porteuse, investie de sens. Ces projets ne cherchent pas à visualiser une réalité cachée, mais reproduisent les images à travers lesquelles les structures de pouvoir s'attribuent un sens. Elles ouvrent en outre un espace de réciprocité le temps d'un instant, permettant aux spectateurs de voir les rouages de la surveillance et les processus de pouvoir.

Toutefois, l'histoire critique du présent que propose Hu demeure, d'une certaine façon, extérieure au monde numérique. Elle l'observe sans vouloir y prendre part. Est-ce donc dire qu'une participation numérique non complice est impossible ? Qu'il faille abandonner le navire-Internet ? La participation est pourtant au cœur de la condition contemporaine. Elle demeure associée à un idéal démocratique. « Participation is not only a concept and a set of practices; » écrivent Barney et coll.,

> fundamentally, it is the promise and expectation that one can be actively involved with others in decision-making processes that affect the evolution of social bonds, communities, systems of knowledge, and organizations, as well as politics and culture. Tied to this promise and belief, as well as to the structures of the media technologies (Internet forums, blogs, wikis, podcasts, smartphones, etc.) that appear to facilitate increased participation, are the possibilities of communication linked to social change. But while possibilities represent desire, they can also be understood as rhetoric, as a set of empty habits, or as failed opportunities (Barney et coll. 2016, viii).

Condamner irrémédiablement la participation serait l'abandon de la voie contemporaine vers l'autodétermination individuelle et collective. Elle est une solution aussi insatisfaisante que l'idée d'être complice d'une structure de pouvoir économique et sécuritaire discriminatoire.

> This is the political agony of the participatory condition: It can be neither embraced nor disavowed without considerable loss. We are not happy with participation, but were we to lose it, we would be sad. It is thus the name of our collective melancholy… Under the participatory condition, democratic politics turns against itself, fulfilling the diagnosis made by Rancière in On the Shores of Politics: "Depoliticization is the oldest task of politics, the one which achieves its fulfillment at the brink of its end, its perfection on the brink of the abyss." What the participatory condition finally demands of us is that we struggle to think and act our way beyond this abyss (Barney et coll. 2016, xxxii).

Pour Andrejevic, penser la participation, c'est-à-dire une action impliquant temps, effort et intentionnalité, à l'ère numérique demande la constitution d'un nouvel imaginaire. Adaptant la distinction entre participation et interactivité proposée par Henry Jenkins, Andrejevic voit dans la notion de participation la possibilité de participer à l'élaboration des codes sociaux, là où

l'interactivité limiterait l'action à l'intérieur de codes technologiques. « Participation carries connotations of collaborative construction of the protocols themselves, » écrit-il.

> Technically, participation simply means "to take part" in… However, there is an underlying promise connoted in the offer to participate. Framed in these terms, the invitation to participate carries with it the implication that this activity will be meaningful for the user, a form of self-expression and, simultaneously, a participation in the greater good. … Interactivity takes place according to coded protocols; participation carries the implied promise of intervening in the code (Andrejevic 2016, 188-189).

Or, le contexte actuel masque des relations d'interactivité sous le vernis de la participation. La présence numérique génère des données qui sont appropriées et exploitées par les fournisseurs de services. Comme il a été précédemment question, ces mégadonnées sont associées de façon à découvrir des inférences corrélatives, souvent contre-intuitives, entre des variables. Pour Andrejevic, penser une participation à l'intérieur de ces structures de pouvoir qui permettrait d'en changer les codes, il est nécessaire de développer un « database imaginary adequate to the capabilities and uses of the machinic "gaze" » (Andrejevic 2016, 202). Cet imaginaire doit rendre visibles les mécanismes de collecte de données intégrés au sein même des technologies numériques, l'imprévisibilité des analyses des mégadonnées, et enfin le rapport de propriété sur les données et l'opacité des processus de surveillance. « The implementation of a data-driven machinic gaze … confounds conventional expectations regarding how surveillance and information processing works, » écrit-il.

> Since much of the conceptual and regulatory apparatus related to questions of privacy and forms of participation still operates within the scope of these expectations, it needs to be updated to reflect and anticipate emerging data mining practices. Absent such an update, we may find that active forms of participation online are redoubled by increasingly passive ones, amounting to automated participation in data-driven control systems (Andrejevic 2016, 204).

Peut-être devrait-on aussi reconnaître que malgré la prise de conscience de l'environnement de surveillance qui structure les sociétés occidentales contemporaines et qui doit guider la participation, et la reconnaissance de notre complicité et de nos désirs, il n'y aura vraisemblablement pas de moment de sortie complète du monde numérique ni de participation pure. Rita Raley invite à penser la contestation en terme moins dichotomique : exit les notions simplistes de complicité ou de résistance. « [D]ataveillance and counterveillance coexist not in dialectical struggle but rather are so fundamentally entangled that the line separating the one from the other is unstable, » rappelle-t-elle.

> Positioned as we are within the dataveillance regime, we cannot but employ the tactics of immanent critique, which depends not on an overstatement or overarticulation of totalizing control system nor on a hyperbolized romance of the exploitation of these systems, but rather depend simply on ordinary action itself (Raley 2013, 139).

Si aucune institution, malgré les tentatives des Google et de la NSA, n'est en mesure de collecter la totalité des données numériques, pour l'individu la possibilité de s'extraire de la surveillance numérique est naïve. « The flip side of the fantasy of total information awareness, » martèle l'auteur, « … is the fantasy of breach » (Raley 2013, 138). Dans ce contexte, il est nécessaire, pour Raley, de chercher des avenues de résistance intérieures, en émulant par exemple les pratiques de surveillance, plutôt que de postuler une impossible extériorité.

Adoptant une perspective moins pessimiste sur l'agentivité dans le monde numérique, Cheney-Lippold défend, à l'instar de Raley, l'occupation de ce territoire. Il faut profiter, suggère-t-il de la performativité numérique pour contrer la définition de nos identités numériques. Les formes de contrôle provenant de la visibilité numérique sont différentes de l'interpellation traditionnelle, rappelle-t-il. Selon le concept d'interpellation de Louis Althusser, « we become the subjects we are by responding to the hail of ideological formations that structure our social environments » (Barney et coll. 2016, ix-x). En se retournant à l'interjection « Hé, vous, là-bas ! » du policier en patrouille, l'individu se reconnaît exister en tant que sujet soumis à une structure de pouvoir (Monahan 2017, 3). Pour Cheney-Lippold, la particularité de l'interpellation numérique est son invisibilité. Si l'on peut reconnaître l'appel à la participation numérique, il est impossible de reconnaître l'identité algorithmique qui nous est assignée puisque celle-ci demeure un secret commercial ou d'État. « While we may theoretically acknowledge our algorithmic identities, » écrit-il,

> jus algorithmi's black boxed opacity means we won't immediately encounter the hail of 'citizenship.' Yet algorithmic identifications like jus algorithmi rarely hail users directly. They instead structure users' conditions of possibility, be it their access to privacy rights, social relations, or knowledge itself. In this way, the process of making subject is indirect (Cheney-Lippold 2017a, 169).

Pour l'auteur, l'interpellation numérique produit par conséquent une subjectivité différente, mais non moins réelle. Il poursuit :

> As digital theorist Seb Franklin argues, "the dividual is the subject digitized," not only positing an ontology of subject relations functionally distinct from our nondigital lives but founding a productive framework to think of how the specific, lived complexity of one's

> individuality is divided from within. It is decontextualized, dehistoricized, and thus modular in operation and application (Cheney-Lippold 2017a, 173).

Certes, les utilisateurs dividualisés sont soumis, à travers l'interpellation numérique, à des structures de pouvoir au-delà de leur contrôle, mais Torin Monahan rappelle que la constitution identitaire des individus n'est pas monopolisée par le pouvoir. D'autres nous interpellent, nous demandent d'être différemment, et souvent d'être en contradiction avec les identités prescrites par les structures de pouvoir (Monahan 2017, 3-4).

Dans ce contexte, s'il est possible de reconnaître un espace navigable, performatif, à travers la multiplicité des interpellations, peut-être est-il possible de résister à la surveillance numérique par ces propres termes ? « Our datafied subject relations are only practiced through data… While we can certainly resist relations of power outside data through direct action against Google or legal reform of the NSA, that resistance must exist on data's terms if it wants to defy our algorithmic identifications, » suggère Cheney-Lippold.

> Of course, this is not because we are literally made of data … but rather because data is the only thing legible to these algorithmic systems of power. … We're algorithmically assessed, not personally disciplined through observation. And that datafied subject relation adds another layer onto who we are, a localized instance of algorithm connecting our data to emergent meaning (Cheney-Lippold 2017a, 197–198).

Pour Cheney-Lippold, cette ontologie du sujet numérique constitué par l'addition a une performativité qui ouvre la porte à la résistance par le numérique. L'identité numérique est formée par l'accumulation infinie de connexions : avec qui l'on communique, avec ce que l'on recherche, avec les espaces Web que l'on traverse. La logique algorithmique est une logique du « et ». L'identité de chaque utilisateur est établie à l'aide de calculs algorithmiques qui le comparent à une population. Cette comparaison permettra de déterminer l'identité de genre, de classe, de race, etc. de l'utilisateur. « It is precisely due to the associative quality of these terms that the decenteredness of datafied subject relations comes to the fore, » explique-t-il.

> We are who we are *because* of our connections to people, places, and things—not despite them. And without a stable, centered identity, both algorithms and our responses to their identifications must attend to the intensive interrelationality of our associative connections. … As with the idea that our algorithmic identities add yet another layer to ourselves, "and … and … and…" rejects any semblance of static being as we indefinitely barrel through time, producing more data that algorithms then use to modulate that data's meaning en masse (Cheney-Lippold 2017a, 190).

La détermination spéculative des identités à l'aide d'algorithmes engendre comme conséquence la fluidité et la perte de contrôle sur l'identité numérique de plus en plus importante dans les nouvelles formes de contrôle social (Cheney-Lippold 2017a; Cheney-Lippold 2011). En même temps, puisque l'identité algorithmique n'est jamais parfaitement exacte par rapport à l'identité réelle ni définitive, il devient possible de jouer avec cette identité. Une identité algorithmique ne rend jamais entièrement justice à l'individu qu'elle recrée. Cheney-Lippold nomme le décalage entre les identités réelles et virtuelles le « else », terme difficilement traduisible qui invoque la présence au-delà de l'image numérique de quelque chose d'autre, quelque chose de plus, dans l'identité réelle. « The else is the lever that our subjectivity uses to address and account for these inescapable slippages of algorithmic life, » propose-t-il. « … This else, or the fact that something "else" is up that we sense or indirectly know about, reifies the contemporary impossibility to perfectly transcode life/control into a digital form » (Cheney-Lippold 2017a, 179–180). Pour l'auteur, l'existence de ce décalage offre un espace d'intervention et de résistance : « [t]o be aware of how we are algorithmically spoken for is to give us administration over what is left to say. The else offers a possibility for deviance, mobility, and ultimately unincorporability according to the conceptual space between algorithms and us » (Cheney-Lippold 2017a, 193).

Profitant de ce décalage pour contourner les modes de contrôle, Cheney-Lippold propose, reprenant ici l'idée d'obscurcissement (« obfuscation ») d'Helen Nissenbaum, de noyer notre identité numérique dans une mer d'information impertinente. L'extension TrackMeNot (Howe, Nissenbaum & Toubiana 2015) que Nissenbaum a mise au point avec une équipe de la New York University génère du bruit : toutes les six secondes, l'application lance des recherches aléatoires sur les moteurs de Google, Bing, Yahoo! et AOL. Ce bruit obscurcit l'identité numérique, non pas en rendant l'identité illisible, cachée par le chiffrement, mais en contribuant à créer une identité aléatoire qui serait donc inutilisable. « [I]n terms of pattern of recognition, in terms of making 'you' on the basis of your dividual queries, TrackMeNot can produce enough noise in the channel that a single, identifiable, measurable-typed essence would be statistically onerous, » écrit Cheney-Lippold.

> … TrackMeNot hides your dividualities in plain sight but overloads what might become meaningful with layers upon layers of extradividual nonsense… Obfuscation creates layers of data incoherency, further upholding our dividual privacy. … [It] avoid incorporation, and thus discursive effect, within the Googleverse's … array of measurable types. Obfuscation is the practice by which the world, as organized through data, can be messed with on data's

> terms. A privacy that relies on a "don't look at this, it's private!" liberal-rights-based approach will always fall vulnerable to people, inside and outside the government, who break and/or ignore the law. Instead, we can view dividual privacy praxis as a "try to look, but I doubt you will find anything useful" invitation to our surveilling others (Cheney-Lippold 2017a, 231).

L'obscurcissement apparaît comme une approche intéressante de résistance à la participation numérique. Elle permet de se réapproprier la présence numérique pour protéger l'identité réelle sans devenir une proie docile de la surveillance. Lue à la lumière du « else » et du décalage entre le réel et le virtuel, la tactique laisse toutefois un goût amer : l'impression d'assister au retour d'une vaine dichotomie entre le vrai et la simulation. Premièrement, cette dichotomie nous ramènerait à la critique formulée par Hu à l'endroit des entreprises de sousveillance. Deuxièmement, elle postulerait sur une base indéfinie l'existence d'une identité qui serait plus réelle que les autres. Troisièmement, en apparente contradiction avec l'essentiel de l'argument de l'auteur à l'endroit du contrôle algorithmique, cette dichotomie inciterait à négliger l'effet des structures de pouvoir au profit d'une illusoire quête ou préservation de l'authenticité. Plus près de mon argument, l'obscurcissement ne résout pas le problème de l'opérationnalisation du savoir de sécurité. Si pour l'auteur, la tactique permet d'une part de masquer le véritable soi et de rendre le double numérique statistiquement inutilisable, cela n'empêche néanmoins pas les acteurs économiques ou sécuritaires de spéculer et d'agir. Pour Cheney-Lippold, qui repend ici l'analogie de Nissenbaum, l'obscurcissement se compare à l'histoire de Spartacus (Cheney-Lippold 2017a, 232). Dans le film paru en 1960, lorsque les soldats romains demandent au groupe d'esclaves qu'ils viennent de capturer lequel est Spartacus, chef de l'insurrection des esclaves, tous se lèvent. Par cette mobilisation, le nom Spartacus est vidé de son sens. Tout le monde et en même temps personne n'est Spartacus. En devenant visibles tous ensemble, il n'y a plus de chef insurrectionnel, mais une insurrection à laquelle les soldats doivent faire face. En définitive, tous sont néanmoins crucifiés.

Pour Hu, un des problèmes de la résistance numérique et des efforts de visualisation est qu'en rendant visibles les structures de pouvoir, ils reconnaissent leur existence. « When we gaze at a control society in the hopes of exposing its structures, » écrit-il, « our gaze ends up acknowledging its right to power » (Hu 2015, 143). D'une certaine façon, c'est ce que fait *PRISM: The Beacon Frame* qui s'arroge le droit de surveiller. Dans sa volonté critique, l'œuvre reconnaît à celui qui contrôle les moyens technologiques la légitimité de surveiller pour le bien commun : ici

la prise de conscience des pratiques de sécurité. *Data Detox Kit* dont il a été brièvement question s'inscrit également dans cette reconnaissance et validation du système. Le projet reproduit l'individualisme sur lequel la société de contrôle est établie. L'objectif demeure individuel : la protection de la vie privée de l'individu afin, comme il est écrit, que ses primes d'assurance automobile ne soient pas plus dispendieuses que celles de ses amis (MozillaTactical Technology Collective 2017). Résilient face à un environnement sur lequel il n'a aucun contrôle, *Data Detox Kit* propose une solution individuelle s'apparentant sur une bonne hygiène numérique, « a healthy, balanced digital lifestyle » (MozillaTactical Technology Collective 2017). Comme le suggère Hu, cette hygiène plutôt que de contribuer à la critique du système fait partie de ses mécanismes de préservation. La tâche d'assurer un Internet libre et sécuritaire, où les utilisateurs consciencieux n'auront pas à subir les affres de pirates mal intentionnés, est impartie à l'individu qui doit se responsabiliser et prendre en charge d'assurer la protection de ses données. Ainsi, plutôt que de s'intéresser aux structures sécuritaires et néolibérales de la société de contrôle, *Data Detox Kit* se présente comme la diète numérique saine, le jogging et la salade verte, de la participation numérique. Si sur le plan individuel, la démarche de *Data Detox Kit* peut être salutaire, sa portée politique est, au mieux, réduite.

Malgré ces exemples, le pas demeure grand entre regard et reconnaissance. Si, comme le propose Althusser, la réponse à l'interpellation ou le retour du regard signifie la reconnaissance de notre position dans une structure de pouvoir, est-ce dire que l'on reconnaît du même coup d'œil le droit et la légitimité de ce système ? Mirzoeff rappelle au contraire comment le regard, par exemple celui de l'esclave noir à l'endroit d'une femme ou d'une personne en position d'autorité blanche sous les Lois Jim Crow, ou encore celui des détenus de la fameuse prison d'Abu Ghraib vers leurs geôliers et tortionnaires, peut constituer un geste de défi (Mirzoeff 2011, 482-483). Ce regard souligne l'existence d'un tort, conteste la hiérarchie établie et revendique une redistribution des parts. Il ne légitime pas les structures de pouvoir, mais rappelant aux puissants l'invisibilité du sort des laissés pour compte, il bouscule l'ordre établi. Cheney-Lippold fait de la révolte des esclaves qui se sont tous identifiés comme Spartacus, la possibilité de protéger la vie privée et l'intégrité individuelle, mais en occupant la scène publique, ces esclaves ne protègent personne, ni physiquement ni éthiquement, ils réclament l'existence d'un nouvel ordre.

Ainsi, la visibilité que réclame le mouvement spontané #myNYPDfile, apparu dans la foulée des révélations sur les pratiques de surveillance de la communauté musulmane par le NYPD,

est un refus des hiérarchies sociales et une revendication d'égalité, d'existence politique. Le mouvement #myNYPDfile mené principalement depuis la plateforme de microblogage Twitter par des membres de la communauté musulmane des Tri-States contestait certes le profilage racial auquel ils étaient soumis. Avant tout, les participants à #myNYPDfile clamaient à coup de gazouillis humoristiques leur place dans la société américaine et leur égalité par rapport aux autres citoyens de la nation que la police new-yorkaise niait (Hogue 2016). Si l'acte de visibilité peut à première vue sembler naïf, il n'en demeure pas moins un geste profondément politique qui conteste leur statut de subordonné par la revendication d'une présence publique.

Le moment politique, suggère Jacques Rancière, provient précisément dans cet acte d'apparition, dans ce moment de réorganisation sociale provoquée par la présence de ce qui devrait être invisible. Pour Rancière si les asymétries de pouvoir peuvent servir de fondement à l'affirmation politique, l'énonciation d'un tort ne peut se formuler uniquement en termes de justice sociale. L'affirmation politique revendique un droit de présence, un droit à l'égalité, qui bouscule les hiérarchies existantes. « What many regard as the sphere of politics—the spaces from which policy is implemented—Rancière regards as mere policing, » explique Michael J. Shapiro.

> For Rancière, politics—as opposed to policing—is itself an event. The domain of 'the political' is not a pre-existing space; it emerges through action that is addressed to a wrong. There are no political parties with an existence prior to 'the declaration of a wrong.'… Instead of seeing the political as emerging from collective responses to events, Rancière sees the political *as* an event, an event of dissensus. And, instead of mapping a world of political and non-political spaces, Rancière identifies acts that reorder spaces and reconstitute identities, rendering persons as political subjects (Shapiro 2013, 140).

« [T]he real challenge posed by surveillance is the re-articulation of the public domain, » suggère Andrea Brighenti (Brighenti 2010b, 52). Tant les hacktivistes, Mann, Hu, Andrejevic que Cheney-Lippold et Nissenbaum sont à la recherche d'un rééquilibrage du pouvoir entre surveillants et surveillés. Cela passe par une intervention consciente de la mainmise économique et sécuritaire sur les données numériques, de l'absence de réciprocité et de contrôle sur les données produites, et du désir de participation à l'entreprise numérique. C'est aussi ce que propose Paglen et Appelbaum avec *Autonomy Cube*. L'œuvre des artistes-activistes engage chacun de ces enjeux, conférant à ceux qui désirent participer activement à l'entreprise numérique un espace d'autonomie relative à travers le réseau Tor. Certes, la surveillance du réseau Tor et les tentatives de percer ses mécanismes d'anonymat le fragilisent. Mais ils rappellent surtout l'impossibilité de s'exclure définitivement des structures de pouvoir comme le suggérait Foucault. Cela ne justifie pas pour

autant d'abandonner la lutte à travers les technologies numériques. « [C]ontemporary participation has become a pharmakon of sorts, to borrow one of the key concepts from Bernard Stiegler's philosophy of technology: both a poison and a remedy, a benefit and a problem, a promise of emancipation as well as a form of subjection, » écrivent Barney et coll. (Barney et coll. 2016, ix-x). *Autonomy Cube* propose de rééquilibrer les rapports de pouvoir numérique à travers la mise en place d'une infrastructure d'anonymat.

Certes, l'anonymat de Tor n'est pas sans faille. Quoique les conclusions sur ces failles du réseau ne concordent pas entièrement avec l'analyse, certes datée, de la NSA, il ne fait pas de doute que Tor ne peut assurer à lui seul un anonymat parfait. Les concepteurs du projet sont d'ailleurs les premiers à le reconnaître (Tor 2018c, So I'm totally anonymous if I use Tor?). Tor attire également l'attention sur l'utilisateur, l'invisibilité étant suspecte, et comme la connexion au réseau est publique, à moins d'utiliser un pont, cette publicité permet de cibler les utilisateurs pour qui voudrait exploiter des brèches dans le réseau ou les données d'un utilisateur. Pourtant, Tor, et plus encore sous la forme d'*Autonomy Cube*, n'est pas uniquement une tentative ratée d'éviter la surveillance. *Autonomy Cube* n'est pas simplement une œuvre de contre-surveillance, d'évasion, incapable de répondre à l'enjeu global de la surveillance. *Autonomy Cube* est une réappropriation, plutôt qu'une preuve de complicité, des technologies de sécurité développées par l'armée américaine, un acte de piraterie en bonne et due forme, qui permet désormais à tous d'émuler les pratiques secrètes de surveillance. Elle se réapproprie les infrastructures internationales de communication mondiale que la NSA et ses partenaires exploitent. Sans attendre que l'État assure la protection du droit à la vie privée de ses citoyens et de tous au-delà de l'appartenance à la communauté politique, *Autonomy Cube* le fait de sorte que la mobilité numérique devienne un outil pour brouiller les pistes. Plus significativement toutefois, *Autonomy Cube* est une œuvre de préfiguration qui performe un espace d'autonomie Internet concurrençant la tendance oligopolistique du capitalisme numérique actuel. « Participation is not a quality added to some other thing or activity, not one hailing process among others, » écrivent Barney et coll., « but a condition that is constitutive of the social itself » (Barney et coll. 2016, ix-x). *Autonomy Cube* crée un espace de participation constitutif d'une réalité sociale numérique alternative et amène la discussion sur l'anonymat au-delà de l'individualisme vers l'enjeu plus large de l'égalité sociale dans la société de contrôle.

6.5 Moi-et-l'autre : une communauté de rupture pour performer l'égalité sociale

Avec *Autonomy Cube*, Paglen et Appelbaum ne sombrent pas dans le technofétichisme ambiant, mais refusent l'appropriation du numérique en proposant des infrastructures alternatives. En ce sens, le projet partage un éthos commun avec Monahan, David J. Phillips et David Murakami Wood. Plutôt que de penser la surveillance uniquement en termes négatifs, ces derniers suggèrent de faire des technologies de surveillance des instruments d'autonomisation individuelle et collective (« empowerment »). Reconnaissant la nature controversée du concept, les auteurs défendent néanmoins leur utilisation :

> the idea of empowerment [refers to] a progressive process rather than an end state. As with all progressive social change, it can never be achieved once and for all because the world is dynamic, justice is emergent, and social problems are tenacious. If we accept that technologies and techniques of surveillance can assist with processes of empowerment, the questions then become: empowerment for whom, toward what ends, under which circumstances, and within which structural contexts? …
>
> This approach recognizes that because surveillance is socially constructed, the design of surveillance infrastructures is a contingent and underdetermined process, which means that alternative—and more power-equalizing—designs are possible. The focus on infrastructures is intentional. Whereas technologies function as tools that enable certain practices, infrastructures establish contexts for practice (Monahan, Phillips & Murakami Wood 2010, 108–109).

Le design d'*Autonomy Cube* vise l'égalisation du pouvoir numérique par la création d'un espace d'anonymat. L'effet immédiat de l'œuvre est d'offrir aux individus un plus grand contrôle sur leurs données numériques. Ce contrôle n'est pas le fait d'une invisibilité pure et simple de l'utilisateur, mais de la constitution d'une collectivité hétéroclite qui conteste l'individualisation du néolibéralisme numérique et les modes de contrôle qui y sont associés.

S'intéressant, dans le cadre d'un projet auto-ethnographique, à la personnalisation des recherches Internet par Google et les moteurs de recherche similaires, Renée Ridgway observe une faille dans l'utopie démocratique entourant les premiers moments Internet. Internet offrait l'opportunité à tout curieux d'explorer les richesses du savoir et de découvrir de nouvelles idées. Citant, Lucas D. Introna et Helen Nissenbaum, elle rappelle que, pour plusieurs, Internet

> was a new medium, a democratizing force that will give voice to diverse social, economic, and cultural groups, [and] to members of society not frequently heard in the public sphere. It will empower the traditionally disempowered, giving them access both to typically

> unreachable nodes of power and to previously inaccessible troves of information (Introna et Nissenbaum cités par Ridgway 2017, 393).

Cette promesse démocratique était fondée sur une conception individualiste d'Internet où chaque utilisateur se trouverait à naviguer à travers le Web au fil des hyperliens. La démocratie Internet dans toute sa diversité était ainsi spontanée, le reflet du hasard des clics, de la liberté de sauter d'une idée à l'autre, pour venir au terme de cette exploration à une rationalisation du savoir.

> The web was thought of as emerging out of myriads of individualised website creators and surfers, whose joint activities would then add up miraculously to a new structured yet democratic and open space. What was absent was a systematic approach to the need of organising collectives to systematise the processes that enables us to navigate this space (Ridgway 2017, 394).

Face à l'absence de structure d'organisation des idées, les moteurs de recherche ont entrepris de guider le hasard en personnalisant les recherches. Cette personnalisation, qui suggère la détermination de préférence et donc de l'identification de l'utilisateur, est dépendante de la comparaison des utilisateurs avec une population. Paradoxalement, même si chaque utilisateur est constamment individualisé et présenté comme l'acteur de ses succès économiques et de sa sécurité, il faut penser le contrôle Internet en termes collectif plutôt qu'individuel. Les algorithmes et les mégadonnées qui définissent de plus en plus Internet suggèrent une structure de contrôle associative plutôt qu'individualisante vers laquelle l'interconnectabilité de la rationalité de réseau pointait déjà. La logique de l'interconnectabilité algorithmique qui construit l'identité numérique montre ainsi, à l'avis de Cheney-Lippold, l'impossibilité de sujet néolibéral.

> Associations are the lingua franca of our datafied life, the source of its fetters as well as the nourishment for its growth. Because a single piece of data means nothing on its own, the fetishized autonomy of the liberal subject would starve without the other. Patterns are made from a population, not a person. How algorithms interpret us necessarily connects us to the lives of others (Cheney-Lippold 2017a, 199).

Ridgway voit dans Tor un instrument pour combattre l'individualisation de l'utilisateur. Alors que les moteurs de recherche et autres services Internet intègrent l'utilisateur à un collectif — qui servira de point de départ pour déterminer son identité — sur lequel il n'a aucun contrôle, Tor crée un collectif alternatif qui protège l'utilisateur contre les pratiques d'individualisation. Il est vrai qu'un utilisateur ne contrôle pas le collectif Tor, mais il accepte néanmoins, comme le suggère Ridgway, d'y participer et, par sa participation, contribue à le modeler à son image, même si cette modulation est infinitésimale.

> When I use Tor I am part of an anonymity p2p network, which increases in strength the more users use it. Exactly and only because I am anonymous and unknown, I have a small voice in a choir of the manifold decisions that make up the p2p-*collective* of Tor users, whereas I would lose this voice if I were to join in the constant flux of algorithmic clustering of personalisation. To partake anonymously in a p2p-collective individuates me more than personalisation does. At stake is an *individuation* in the sense of Bernard Stiegler's reading of Simondon—an individuation that is marked by being collective and psychic alike, which forms the opposite to the *individualisation* of the pseudo-autonomous objects of Google's personalization (Ridgway 2017, 393).

Autonomy Cube imagine le collectif Internet en créant une communauté d'utilisateurs qui protège l'autonomie individuelle de chacun. Cette communauté est peut-être limitée en nombre, quelque quatre millions d'utilisateurs quotidiens (Tor 2018a), mais le réseau Tor défend sa légitimité en montrant la diversité de ses utilisateurs (Tor 2018e), Appelbaum rappelant que le réseau est « [a] reflection of the larger Internet » (Paglen & Appelbaum 2016). Tous peuvent bénéficier de l'anonymat offert par Tor, tant les minorités ciblées, les activistes, que les gens d'affaires, et les autorités. Du même coup, tous contribuent, à travers une infrastructure bénévole et libre plutôt que cannibale, à la mise en place de la communauté numérique représentative de la diversité sociale.

Le duo d'artistes-activistes ne prétend pas trouver dans la technologie, une solution à tous les problèmes du monde moderne. « [W]e are not going to engineer our way out of a totalitarian future. Technology won't save us, » expliquent-ils en entrevue. Après tout, *Autonomy Cube* n'empêche pas Google ni la NSA d'utiliser à leur guise les données recueillies — soit celles produites par la collectivité Tor ou celles identifiant un individu comme un utilisateur Tor. *Autonomy Cube* n'offre pas de contrôle ni sur les données ainsi produites ni sur les inférences générées de l'analyse des mégadonnées. « Tor will not save us, but it can help » (Paglen & Appelbaum 2016). Même si les artistes ne se revendiquent pas explicitement du courant, à l'instar des médias tactiques (« tactical media »), *Autonomy Cube* aide à contrer la surveillance numérique en créant un espace, le temps d'un moment, pour mettre en œuvre et imaginer un monde différent.

Comme les médias tactiques, Paglen et Appelbaum recherchent avec *Autonomy Cube* la création d'une rupture avec les structures du pouvoir numériques. Raley suggère que la destruction créative associée à l'acte de refus des médias tactiques s'apparente à la notion d'événement proposée par Gilles Deleuze. Celui-ci insiste, les suites d'un événement sont imprévisibles. Si le sens du monde se cristallise par la répétition et l'accumulation de couches sémitiques, l'événement vient rompre cette accumulation et ouvre la possibilité d'un futur imprévisible (Shapiro 2013, xv-

xvii). « To precipitate an event is to act without knowing the situation into which one will be propelled, to change things as they exist, » résume Raley, avant de citer Deleuze

> For a while, they have a real rebellious spontaneity. … Events can't be explained by the situations that give rise to them, or into which they lead. They appear for a moment, and it's that moment that matters, it's the chance we must seize. … If you believe in the world you precipitate events, however inconspicuous, that elude control (Deleuze cité par Raley 2009, 26).

Sémantiquement, l'événement se comprend en association avec la rupture, l'indétermination, la mobilité. Les médias tactiques exploitent l'événement pour créer des moments d'instabilité dans les structures de pouvoir et d'ouverture vers un autre monde possible.

Dans un retour réflexif sur leurs propres pratiques, Geert Lovink et Ned Rossiter s'interrogent néanmoins sur la pertinence d'une résistance momentanée qui, d'une certaine façon, reproduit l'obsession postfordiste pour la courte durée. La nature momentanée de la déstabilisation des médias tactiques épargnerait les structures profondes du pouvoir en plus de révéler les failles existantes du système (Raley 2009, 28). Pour Raley toutefois, la courte durée n'invalide en rien la pertinence des médias tactiques. « From the perspective of a tactical media practitioner, » rapporte-t-elle,

> the belief in this temporal opening to a better tomorrow makes the question of immediate efficacy less pronounced. A skeptic might wonder what difference a temporary disturbance makes, but for tactical media there is a certain power in the spontaneous eruption, the momentary evasion of protocological control structures, the creation of temporary autonomous zones, that surely play their part in making possible the opening for political transformations (Raley 2009, 27).

Pour Raley, la création d'un événement aux conséquences imprévisibles situe les médias tactiques dans un rapport au temps qui va au-delà du présent. L'activisme de ces artistes-activistes ne vise pas l'établissement immédiat d'un ordre social émancipé, mais la création d'un moment de rupture permettant de faire apparaître un autre futur qui défie néanmoins l'idée d'utopie. Citant le théoricien de l'art Nicolas Bourriaud, Raley précise :

> "the role of artworks is no longer to form imaginary and utopian realities, but to actually be ways of living and models of action within the existing real, whatever the scale chosen by the artist." With the recognition that there is no getting outside the global techno-military-economic world order, tactical media thus performs a sociopolitical intervention by gesturing only obliquely toward a better world in the future (Bourriaud cité par Raley 2009, 27).

Résistance à l'intérieur des structures de pouvoir, sans possible échappée sinon que par un refus temporaire d'obtempérer, l'éphémérité de la performance esthétique des médias tactiques incite Raley à penser le rapport entre l'artiste, l'œuvre, le moment et les spectateurs. Les médias tactiques vivent dans la mémoire de leurs spectateurs et dans les secousses créées par l'événement de rupture. L'objet des médias tactiques, s'il y en a un, n'est que prétexte à la performance de destruction créatrice. En ce sens, les médias tactiques sont à l'image de l'acte de virtuosité : « [an] activity which finds its own fulfillment (that is, its own purpose) in itself, without objectifying itself into an end product, without settling into a 'finished product,' or into an object which would survive the performance » (Paolo Virno cité par Raley 2009, 29). Puisque la performance vertueuse ne se concrétise pas dans la réalisation d'un objet, elle nécessite un public pour la voir et lui attribuer une longévité. « [T]actical media projects share with performing artists and political actions a sense of contingency in that they too are performed "on the fly" and require the presence and response of a user to complete their signifying fields, » écrit Raley.

> It is in this respect that we can understand the foregrounding of technique and technological expertise, which might initially appear to frustrate attempts to situate these works in relation to a social context and which also seems instead to invest in what Pierre Bourdieu calls a "pure aesthetic" (Raley 2009, 29).

À première vue, la proximité entre les médias tactiques et *Autonomy Cube* est forcée. D'une part, Paglen rejette l'autonomie artistique supposée par l'esthétique pure. Comme l'analyse Bourdieu, « [t]he invention of the pure gaze [and pure aesthetic] is realized in the very movement of the field toward autonomy. In fact, … the autonomy of the principles of production and evaluation of artwork is inseparable from the affirmation of the autonomy of the producer, that is, the field of production » (Bourdieu 1987, 207). Or, Paglen conteste cette prétention à l'autonomie. Il rappelle au contraire l'impossibilité des individus et institutions culturelles à s'extraire définitivement de la surveillance numérique et presse les musées à reconnaître leur position privilégiée dans la société contemporaine afin d'en faire des havres de démocratie, de liberté d'expression et d'exploration. La vocation utilitaire d'*Autonomy Cube* cadre également mal avec l'essentialisme de l'esthétique pure. Alors que la déstabilisation créatrice des médias tactiques cherche avant tout la création d'une brèche dans l'ordre social, l'œuvre de Paglen et Appelbaum assure une fonction d'anonymisation des utilisateurs et de renforcement des infrastructures du réseau Tor. D'autre part, contrairement à la virtuosité immatérielle de Virno à laquelle Raley associe les médias tactiques, *Autonomy Cube* se matérialise dans un produit fini, en l'occurrence

des composantes informatiques enfermées dans un cube de Plexiglas. À cela s'ajoute la critique formulée par Raley à l'endroit du cyberactivisme et de l'hacktivisme parmi lesquels le réseau Tor peut compter. « The models of resistance, dissent, and "being-against" articulated by tactical media, » explique-t-elle, « do not adhere … to the ideology of the cyberlibertarians, who have been active in public policy debates about censorship, privacy, and intellectual property and tend to focus on individual freedom rather than social justice » (Raley 2009, 25).

Pourtant, malgré les apparentes incompatibilités entre les médias tactiques et *Autonomy Cube*, davantage les unissent. Il ne s'agit pas ici de faire d'*Autonomy Cube* une œuvre des médias tactiques à tout prix, mais de bien distinguer le réseau Tor du projet de Paglen et Appelbaum. Si le second fait la promotion de la première, elle ne s'y limite pas. *Autonomy Cube* est une œuvre politique, là où Tor a une vocation d'abord utilitaire. Comme les médias tactiques, elle crée un moment de rupture. Plutôt que d'insister uniquement sur la dimension temporelle de la perturbation de l'ordre social, *Autonomy Cube* rompt l'espace-temps de la surveillance numérique. Notant l'aspect profondément matériel et spatial des infrastructures de communication, Paglen et Appelbaum proposent dans le réseau Tor et plus encore dans le sanctuaire muséal la création d'un espace de rupture. Cet espace joue avec la permanence et l'éphémérité de l'anonymat Tor. Il renforce l'ensemble du réseau assurant à tous la possibilité de s'y connecter en tout temps. En même temps, l'œuvre reconnaît la limitation de l'espace du musée à partir duquel les spectateurs se connectent directement au réseau. Implicitement, l'œuvre reconnaît aussi que la navigation sur le réseau Tor n'occupera pas l'ensemble de la présence Internet qui perd toute pertinence lors de l'utilisation de services personnalisés. Comme le suggère Cheney-Lippold, « even if we used Netflix.com through Tor, we'd still be connected to our users accounts—we'd still be ordered according to the logics of Netflix's genre-defining algorithms and how those algorithms profile, and thus delimit, our lives » (Cheney-Lippold 2017a, 240). Les artistes-activistes ne prétendent pas assurer une sortie définitive de la surveillance numérique. Si *Autonomy Cube* s'attarde à l'espace, c'est pour offrir une agora, limitée dans l'espace et le temps, pour penser à une alternative à la surveillance numérique similaire à ces « temporary autonomous zones … [that] mak[e] possible the opening for political transformations » qu'identifie Raley (Raley 2009, 27).

Dans la création d'un havre se concrétise également la réflexion sur l'émancipation et l'utopie, le présent et le futur d'*Autonomy Cube*. Les médias tactiques relèvent la naïveté des discours d'émancipation et d'utopie à la recherche du renversement des structures de pouvoir, et

préconisent des alternatives vécues dans le présent ouvrant vers un futur inconnu plutôt que prédéterminé. De son côté, *Autonomy Cube* propose à travers le réseau Tor une plus grande maîtrise de la présence numérique dans le présent qui pourrait être associée à une forme de sortie émancipatrice des contrôles de la surveillance. Pourtant, reconnaissant les limites de la solution technologique aux enjeux de surveillance, l'œuvre ne peut se limiter à cette sortie temporaire. De même que Tor ne peut se résumer à une entreprise de chiffrement, mais protège l'anonymat individuel en créant un collectif, *Autonomy Cube* ne peut se résumer à Tor. L'œuvre offre un moment de rupture pour imaginer un monde alternatif. *Autonomy Cube* est tout à la fois une exploitation des failles des présentes structures de pouvoir et une marche vers un futur incertain qui, s'il est à l'image du réseau Tor, est bien loin d'être utopique. *Autonomy Cube* offre au mieux la possibilité de garder en vie le rêve certes utopique, voire romantique, d'un Internet libre et créatif. Mais ce rêve, comme le reconnaissent Paglen et Appelbaum, ressemble aujourd'hui davantage à une chimère. Entre l'horreur d'une société de contrôle totalitaire et l'impossibilité d'une liberté parfaite, *Autonomy Cube* pose la question du futur d'Internet.

Une partie de la réponse, assurément incomplète, que proposent Paglen et Appelbaum à cette question se retrouve dans la collectivité spontanée créée sur le réseau Tor. Dans la démocratie radicale de Springer, la contestation de l'espace public n'est pas une fin en soi, mais un moyen vers la redécouverte du pouvoir transformateur de la contestation (Springer 2010). Similairement, le havre temporaire créé par *Autonomy Cube* n'est pas le futur d'Internet, mais un moyen vers l'affirmation du pouvoir de transformation de la collectivité numérique. Plus qu'un objet, *Autonomy Cube* vit de la participation des spectateurs. Sans cette participation, Tor perd son efficacité d'anonymisation, le rêve des artistes-activistes d'un Internet alternatif s'estompe. Car, ce qu'Autonomy Cube propose, c'est la constitution d'une collectivité numérique égalitaire et autonome. Cheney-Lippold reconnaît également le caractère social de Tor, mais pour l'auteur, c'est à titre de véhicule de socialisation. En même temps que Tor permet de protéger la vie privée d'un individu, il oblige celui-ci à penser la vie privée des autres. « You are, at the level of infrastructure, forced to engage with questions of privacy at square one, both for the sake of yourself and also for the sake of the server and other users » (Cheney-Lippold 2017a, 240). *Autonomy Cube* ne se limite pas à la question de la vie privée, mais est politique : elle rend visible une force collective qui refuse la surveillance numérique.

Contrairement à la lecture traditionnelle de Tor, le réseau, et l'œuvre à travers lui, ne cherche pas à faire disparaître l'individu, ils invitent chaque utilisateur à constituer une multitude hétéroclite, spontanée et modulable permettant d'aplanir, aux vues de la surveillance numérique, les différences individuelles. L'individu se dissout dans l'ensemble. Cette dissolution ne se comprend toutefois pas en terme moderne où l'individu est forcé de se conformer à une identité prédéterminée. L'utilisateur du réseau Tor module l'identité numérique de la collectivité. C'est en ce sens que l'on peut parler avec Michael Hardt et Antonio Negri d'une multitude composée de singularités. « The multitude … is not unified but remains plural and multiple, » écrivent-ils. « … The multiple is composed of a set of *singularities*—and by singularity here we mean a social subject whose difference cannot be reduced to sameness, a difference that remains different » (Hardt & Negri 2004, 99). Un ensemble devient une multitude par sa volonté d'agir : « [t]he multitude, designates an active social subject, which acts on the basis of what the singularities share in common » (Hardt & Negri 2004, 100). C'est ce qui la distingue de la masse ou de la foule. Si ces dernières peuvent produire des effets très réels, on ne peut pour les auteurs en parler comme une multitude, car elles n'agissent pas d'un commun accord. L'accord qui donne vie à la multitude Tor provient de la volonté de participer au réseau ; l'action commune qu'elle mène est l'anonymisation de chacun et l'aplanissement des inégalités sociales.

L'anonymat consenti par la multitude offre à tous, tant aux privilégiés qu'aux petits, un outil de contrôle et de participation dans la création d'une collectivité numérique. Pour la surveillance numérique, chaque utilisateur est un membre de la communauté Tor indissociable de son voisin. Pour chacun, Tor offre la possibilité de participer à l'entreprise numérique en contournant, pour un moment, les mécanismes d'individualisation, de catégorisation et de contrôle de la surveillance.

Autonomy Cube est une œuvre politique qui offre une visibilité à cette multitude. Rompant avec l'obsession du cyberactivisme pour la liberté individuelle que note Raley, *Autonomy Cube* conjugue, dans une aspiration anarchiste, la recherche de l'autonomie individuelle et collective à la poursuite de l'égalité sociale et s'inscrit dans une politique de contre-visibilité. Paradoxalement, comme le pointent les critiques, si le réseau empêche de tracer les détails de la navigation Internet, Tor laisse paraître, en amont, la participation individuelle au réseau et en aval, la force de Tor. L'anonymat est donc partiel, un problème d'ailleurs soulevé par les concepteurs du projet et qui peut être lourd de conséquences pour les activistes qui tentent de contourner la répression de

régimes autoritaires. Pour ces derniers, se connecter à Tor est une geste politique, de contestation du régime. Pour les autres, notamment les privilégiés parmi lesquels on peut me compter, se connecter à Tor reste néanmoins un geste compromettant, une association avec les quatre cavaliers de l'apocalypse numérique. Au-delà des risques, la participation au réseau Tor revendique un droit individuel et collectif d'exister sans être soumis au contrôle de la surveillance numérique. *Autonomy Cube* est une intervention politique qui clame l'existence d'un tort et revendique une redistribution des parts entre d'un côté les grands joueurs du numérique et le dispositif de sécurité, et de l'autre les utilisateurs d'Internet. L'œuvre contribue à la mise en place de ce droit. Elle redistribue les parts en créant des espaces qui brouillent les opérations de ciblage nécessaire à l'attribution de contraintes et de privilèges. Elle politise la présence Internet en créant une multitude qui conteste le processus de dividuation de la surveillance numérique et qui oppose à l'individualisme policé, une identité collective à laquelle tous qui partagent la critique de la société de contrôle peuvent se joindre et qui refusent les divisions au cœur de l'organisation sociale entre bons et mauvais sujets moraux, économiques et sécuritaires.

6.6 Conclusion : pour une politique de contre-visibilité

Pour Hardt et Negri, « [t]he multitude is the only social subject capable of realizing democracy, that is, the rule of everyone by everyone » (Hardt & Negri 2004, 100). *Autonomy Cube* ne promet pas la mise en place d'un régime démocratique. La notion de démocratie demeure néanmoins essentielle au projet de Paglen et Appelbaum, l'antithèse de la société de contrôle. En transformant Internet en espace surveillé à partir duquel des données nécessaires à la gestion des populations sont collectées, la surveillance numérique menace l'autonomie des individus et les encourage à adopter des comportements conformes aux exigences de l'ordre social néolibéral. Pour les artistes-activistes, la démocratie se comprend en termes d'autonomie individuelle et collective, de liberté d'explorer de nouvelles idées sans craindre la répression, et d'autodétermination. Paglen et Appelbaum se situent dans la tradition anarchiste pour laquelle l'absence de contraintes est essentielle pour assurer la liberté et l'égalité de tous. En même temps, la conception de la démocratie derrière *Autonomy Cube* s'aligne avec celle de Rancière qui voit dans celle-ci une lutte pour le maintien d'une sphère publique. « The spontaneous practice of all government, » écrit-il

> tends to shrink this public sphere, to make it into its private affair and, for that purpose, to consign the interventions and the places of intervention of non-state actors to the side of

> private life. Democracy, then, far from being the form of life of individuals dedicated to their private happiness, is the process of struggle against this privatization, the process of enlarging the public sphere (Rancière cité par Brighenti 2010b, 66).

Dans la tradition arendtienne, la sphère publique assure pour Rancière un espace de visibilité permettant d'exprimer les doléances et de revendiquer une réorganisation de l'ordre social. Pour cette raison, son maintien est indispensable à la poursuite de l'égalité sociale.

Autonomy Cube s'inscrit dans cette défense de la sphère publique numérique comme espace de revendication, d'égalisation et d'autodétermination. Car contrairement à ce qui peut paraître à première vue, et à ce qui est véhiculé à propos de Tor, *Autonomy Cube* n'est pas une œuvre individualiste, mais un projet collectif. Si Tor est avant tout fonctionnel, tourné vers la défense de la vie privée à travers l'anonymat numérique, le projet de Paglen et Appelbaum politise le réseau et plus généralement les infrastructures numériques. Elle sort Tor de l'isolement pour mieux l'insérer dans son contexte politique afin de penser les effets de la surveillance numérique et proposer un moment de rupture, de destruction créatrice. Parallèlement, alors que Tor peut se lire comme un réseau ouvert à qui recherche l'anonymat numérique, *Autonomy Cube* est un acte de contre-visibilité créant, à travers le réseau Tor, une multitude dont le point commun est la volonté de repenser les infrastructures de communication mondiale, la surveillance numérique et la sécurisation du monde.

L'œuvre évite, sinon conteste si l'on s'attarde à la critique institutionnelle du milieu artistique, la dépolitisation et le technofétichisme des entreprises d'anonymat et de chiffrement qui reproduisent, comme l'ont relevé tant Hu que Raley, l'individualisme de la culture numérique. Prenant à contre-pied des projets comme *PRISM: The Beacon Frame* ou *Data Detox Kit*, *Autonomy Cube* rappelle que la surveillance n'est pas une pratique à prendre à la légère, que l'invisibilité n'est pas une fin en soi. À la lumière des ressources investies dans le déchiffrement, notamment à travers la recherche sur les ordinateurs quantiques qui promettent une efficacité de cryptanalyse encore inégalée (Bourque 2016), l'invisibilité numérique ressemble à une utopie bien peu viable, si elle ne nous ramène pas directement vers une course aux armements numériques.

Similairement, *Autonomy Cube* n'est pas seule dans sa volonté de se réapproprier les infrastructures numériques. Le festival transmediale a été l'hôte de rencontre promouvant la création de réseaux de communication autonomes (Wilk 2015; Garrett 2016; voir aussi Antoniadis 2016). Ces réseaux fabriqués collectivement dans la logique du DIY (« Do It Yourself ») cherchent

à créer des espaces refuges. De façon générale, ces réseaux utilisent les composantes Wi-Fi de chaque ordinateur participant pour créer un réseau qui devient en même temps une communauté. Partant de ce principe de base, les entreprises sont diverses. Certains, comme PirateBox (PirateBox 2017), Post Cyberwar Series de Philipp Ronnenberg (Ronnenberg 2017) et Backslash Router de P. Olivera et X. Chen (Hertz 2018, 27), proposent des réseaux hors-ligne, non connectés à Internet, pour favoriser l'activisme, ou encore pour contourner la censure d'État (Garcia Martinez 2017; Wachter & Jud 2018). D'autres comme freifunk.net (freifunk.net 2018) ont mis en place des réseaux autonomes pour sortir Internet de la logique marchande ou pour assurer une connexion Internet à des zones négligées par les opérateurs comme le projet Sarantoporo en Grèce (Garrett 2016). Ensemble, ils proposent de contourner la surveillance numérique et le monopole que les grands acteurs économiques du numérique possèdent sur l'accès Internet, et recentrent la logique du réseau de communication autour d'une communauté plus restreinte.

Dans la diversité des démarches ressort la volonté commune d'établir un espace de communication en marge des grandes structures de l'Internet marchand et sécuritaire. Leur sortie permet la mise en place de petites communautés autogérées. Face à ces refuges qui se veulent parallèles à Internet et au contrôle de la surveillance numérique, *Autonomy Cube* joue avec les différents registres de l'invisibilité et de la visibilité numérique pour établir un espace protégé qui n'est pas fermé sur lui-même ni en marge d'Internet. *Autonomy Cube* se situe au sein même des mécanismes du pouvoir numérique et affirme la volonté d'établir un monde différent. La visibilité que se forge la multitude d'*Autonomy Cube* et, à travers elle, le devenir politique de l'œuvre, est collective. Rappelant la réciprocité des autonomies individuelle et collective, *Autonomy Cube* masque dans la communauté les inégalités et brouille les processus discriminatoires. L'œuvre de Paglen et Appelbaum est ainsi à la fois un instrument de protection, une critique sociale et un vecteur d'autodétermination. Contrairement aux projets de réseaux autonomes, l'œuvre ne se situe pas dans une logique de fuite vers un univers homogène, mais devient un outil d'autonomisation permettant à tous de naviguer la toile à l'abri de la surveillance numérique et globalement de rééquilibre les inégalités.

La double apparition, celle d'abord de l'utilisateur membre de la communauté Tor, celle ensuite de la communauté dans son ensemble, performe une politique de contre-visibilité qui préfigure une collectivité marquée par un aplanissement des inégalités sociales. Cette communauté est en lui-même un espace de dissensus face à la société profilée. Tor offre à chacun le même outil

d'anonymat, sans poser la question du mérite. La communauté accueille tous ceux qui désirent participer, peu importe qui il est ou ce qu'il a fait. La possibilité de voir s'y joindre des individus mal intentionnés est régulièrement soulevée comme critique, critique que le projet Tor écarte immédiatement. Tor est-il coupable d'un relativisme moral niant les violences que l'anonymat peut générer ? Peut-être, mais il semble plutôt s'agir d'une volonté de décloisonner les enjeux. Le vice est présent dans la société, avec ou sans Tor. D'une part, il serait réducteur de ramener une communauté à cette seule réalité, de la même façon que l'on ne résume pas une société entière, qu'elle soit québécoise, canadienne ou américaine, à sa criminalité. D'autre part, à l'image du dogme judiciaire qui assure l'innocence de chacun jusqu'à preuve du contraire, Tor protège tout le monde au risque de faciliter des actes répréhensibles. Or, cette innocence est de plus en plus battue en brèche par la logique sécuritaire qui cherche à empêcher les événements de survenir pour assurer le statu quo social. C'est donc sans grande surprise que l'universalité de l'anonymat offert par Tor apparaît dangereuse à l'entreprise de catégorisation nécessaire au contrôle des sociétés occidentales. Le jeu entre invisibilité et visibilité auquel joue *Autonomy Cube* n'est pas parfait ; il est même probablement naïf. Pourtant, cette naïveté est nécessaire pour contrer l'excès de sérieux d'un monde formaté par l'aveuglement volontaire face aux mégadonnées et la paranoïa sécuritaire.

7 Conclusion : De l'esthétique de la visibilité à la réappropriation de l'univers numérique : fissurer l'ordre sécuritaire de la surveillance algorithmique

Appreciating complexity is surely a virtue, but being immobilized by it is not.
Gary T. Marx[1]

L'omniprésence de la surveillance algorithmique peut apparaître déstabilisante, son contrôle sur les populations au nom de l'ordre social et de la sécurité nationale, inquiétante. Pourtant, les multiples interventions critiques de l'art numérique montrent plutôt sa fragilité. Assemblage complexe, la surveillance algorithmique des dispositifs de sécurité occidentaux est formée d'un ensemble hétéroclite de parties : institutions de sécurité, culture du secret, infrastructures de communication, nouvelles technologies de l'information, conventions informatiques, interchangeabilité des données numériques, frontières internationales, cadres législatifs, assemblées législatives sympathiques aux arguments sécuritaires, partenariats intergouvernementaux, ententes commerciales, modèle économique néolibéral échangeant services numériques contre données d'utilisateur, individualisation de la société, percée dans l'intelligence artificielle, normes sociales accélérant la pénétration des médias numériques, contexte sécuritaire obsédé par le terrorisme, sécurisation du quotidien, rationalité de risque, volonté d'intervenir de façon préemptive, etc. Si la surveillance algorithmique semble totalisante, c'est qu'elle réussit à donner une cohérence à toutes ces parties pour former un tout. Rien n'indique cependant que cette cohérence saura perdurer. Déjà, des fissures se forment, des tensions se manifestent. À la suite des révélations Snowden, les partenariats intergouvernementaux entre les agences de renseignement se sont ébranlés (Bauman et coll. 2014, 127-128). Les entreprises numériques ont augmenté le niveau de chiffrement de leurs communications (Hattem 2015). Des groupes activistes comme Privacy International et ACLU ont lancé des actions légales dans le but de faire invalider certains pans des lois qui circonscrivent les pratiques de surveillance des agences de renseignement (ACLU 2015a). D'autres organisations, comme les groupes canadiens OpenMedia, Citizen Lab et Crypto.Québec, s'organisent pour faire pression sur les gouvernements

[1] (Marx 2006, 50)

et favoriser l'alphabétisation numérique. Des hérauts comme Snowden, Greenwald et les journalistes d'enquête de The Intercept brisent le secret d'État et alertent la population contre les pratiques de surveillance étatique. Des artistes nous provoquent et nous invitent à réimaginer le monde. Indépendamment, chacun s'avèrera peut-être insuffisant pour transformer l'assemblage de surveillance ; qui sait, néanmoins, les points de fracture qu'ils pourront à terme créer. Ils démontrent, minimalement, que toute résistance n'a pas encore été assujettie.

7.1 Résumé de la thèse

La participation ou la complicité de l'art numérique à la surveillance algorithmique et la visibilité se situent au cœur de cette thèse qui posait la question de l'agentivité face à une structure de pouvoir omniprésente et inévitable. Plus précisément, les questions de recherche se déclinaient comme suit :

1) Comment l'art de surveillance, pensé comme une forme particulière de participation citoyenne numérique, peut-il constituer un espace de résistance à la surveillance algorithmique et à la sécurisation du quotidien ?
2) Comment l'art de surveillance s'insère-t-il dans le régime de visibilité de la surveillance algorithmique ?
3) Comment l'art de surveillance peut-il proposer une forme alternative de visibilité à l'ère numérique ?

Les artistes issus de la culture numérique ont fortement réagi aux révélations Snowden. En mettant en œuvre une surveillance de masse, en s'octroyant un pouvoir d'interprétation sur les données collectées, en créant un impératif de visibilité, la surveillance menée par les dispositifs de sécurité occidentaux est intrusive et met en danger la démocratie occidentale. Pour plusieurs artistes, la surveillance algorithmique n'est toutefois pas intrinsèquement condamnable. Ces artistes explorent la relation technologie-culture-pouvoir pour comprendre et contester les structures de pouvoir associées à ces pratiques de surveillance. Contestant le régime de visibilité de cette surveillance algorithmique, ils revendiquent un droit de regard sur l'assemblage de surveillance qui met en lumière les rouages de la surveillance algorithmique, et permet de reprendre le contrôle sur nos données.

Dans un premier temps, je retourne aux littératures sur la sécurité, la sécurisation et la surveillance. Les études critiques de sécurité contestent la naturalité du concept de sécurité. Constatant l'impossibilité d'une sécurité absolue malgré l'extension du dispositif de sécurité et un glissement de la notion de menace vers celle de risque, elles abordent la sécurité, dans la tradition foucaldienne, comme une technologie de gouvernement. Le dispositif de sécurité assure le contrôle des circulations d'objets et de populations et veille à intercepter les événements déstabilisateurs afin de maintenir l'ordre social nécessaire à la profitabilité économique. La surveillance algorithmique participe à ce dispositif de sécurité permettant un contrôle plus précis et en temps réel. En même temps, plusieurs ont remis en question l'interprétation manichéenne des technologies de surveillance. La surveillance est une pratique culturelle qui peut aussi bien servir à contrôler les populations qu'à promouvoir son autodétermination. Cela ouvre la porte à la réappropriation des technologies de surveillance à des fins de résistance.

Le chapitre 3 part de cette ouverture vers la résistance pour penser la contestation artistique de la surveillance algorithmique. L'esthétique a acquis, avec l'art moderne particulièrement, une portée critique importante. Dans le chapitre, j'explore la façon dont les études critiques de sécurité et le tournant esthétique en Relations internationales définissent l'art et l'esthétique. Inspiré par ces auteurs et le théoricien de l'art Jacques Rancière, je propose d'identifier la politique de l'art dans la critique du régime de visibilité. L'art est à la fois un objet et une performance qui crée une rupture dans l'intelligibilité du monde, permettant de revendiquer une présence et un monde différent. Dans ce chapitre, je présente également la méthodologie qui me permet de reconstituer une communauté d'artistes numériques et de sélectionner certaines œuvres au sein de celle-ci.

Dans le chapitre 4, j'explore, à travers l'analyse des œuvres *Citizen Ex* de James Bridle et *IXmaps* de l'équipe pluridisciplinaire d'Andrew Clement, l'exploitation des infrastructures internationales de communication mondiale par les dispositifs de sécurité occidentaux, au premier chef la NSA. Ces œuvres illustrent les mécanismes de collecte de données de la NSA révélés par Snowden. Elles soulèvent en parallèle les limites des cadres juridiques du droit à la vie privée consenti par les États à leurs ressortissants. Les infrastructures de communication et la mobilité des données qui en résulte facilitent la surveillance algorithmique et normalisent un droit d'exception. Plutôt que de chercher l'exception dans l'anti-constitutionnalité de certaines pratiques, ces œuvres montrent que l'exception est inscrite dans l'infrastructure matérielle et légale du dispositif de sécurité américain.

Le chapitre suivant se penche sur l'opérationnalisation du savoir de sécurité. Le chapitre 4 montre les mécanismes de surveillance de masse qui universalisent la surveillance. Approfondissant l'œuvre *Secret Power* de Simon Denny, le chapitre 5 poursuit la réflexion décrivant cette fois comment les données collectées sont transformées en savoir permettant d'entreprendre des actions de sécurité. La rationalité de sécurité promeut une logique d'interconnectabilité où le réel et le virtuel deviennent des mondes fongibles et où les données peuvent être associées et réassociées indéfiniment dans l'objectif de générer des structures de suspicion à partir desquelles il sera possible d'intervenir pour intercepter les risques identifiés. Cette obsession pour l'interconnectabilité insère le savoir de sécurité dans une logique paranoïaque et spéculative aux effets contradictoires. D'une part, tous les individus deviennent la cible potentielle du dispositif de sécurité. D'autre part, la surveillance algorithmique cible certains individus et groupes contribuant à leur marginalisation. En définitive, tous perdent le contrôle sur la signification de leurs données qui peuvent être interprétées librement par les dispositifs de sécurité occidentaux.

Dans le chapitre 6, il n'est plus uniquement question de s'attribuer un droit de regard sur des structures de pouvoir invisible, mais de reprendre le contrôle sur sa propre visibilité. Pour contrer les mécanismes de contrôle de la surveillance algorithmique, Trevor Paglen et Jacob Appelbaum proposent avec leur œuvre *Autonomy Cube* de créer des havres de protection en offrant un accès au réseau d'anonymisation Tor. Si Tor est généralement associée à la criminalité, aux cyberlibertariens et à la protection d'une vie privée individualisée, Paglen et Appelbaum insufflent une dimension sociale et politique au réseau. Tor/*Autonomy Cube* permet une participation à l'univers numérique qui évite, pour un instant, la complicité avec les structures de pouvoir de la société de contrôle. Pour rendre la navigation individuelle anonyme, Tor/*Autonomy Cube* crée une collectivité d'utilisateurs. L'image de cette collectivité hétéroclite remplace l'individu aux yeux de la surveillance. Ce faisant, elle brouille les mécanismes de catégorisation et de ciblage de la surveillance. En revanche, Tor/*Autonomy Cube* rend la participation au réseau visible. La dimension sociale et politique de l'œuvre réside dans l'ambiguïté de cette visibilité : l'utilisateur est identifiable comme partie de la collectivité résistante, mais son identité est masquée par la collectivité. Tor/*Autonomy Cube* performe une visibilité politique qui revendique un monde numérique égalitaire.

Devant la complicité volontaire et involontaire des entreprises numériques aux efforts antiterroristes et l'incapacité du droit à la vie privée à protéger les individus contre la surveillance algorithmique des communications mondiales, ces artistes proposent une cartographie alternative du pouvoir qui éclaire et politise les structures de pouvoir rendues invisibles par le secret d'État et la banalisation des technologies. Ils permettent de voir les mécanismes de collecte de données qui soumettent toute présence numérique au regard possible de la sécurité et la liberté d'interprétation des dispositifs de sécurité qui fragilise le contrôle sur la signification de nos données. S'appropriant les technologies numériques, ils contestent en outre l'existence d'un sujet numérique néolibéral décentré et les pratiques de catégorisation sociale pour repenser la résistance à la surveillance algorithmique en termes collectifs : constitutif d'une collectivité politique égalitaire.

7.2 Contributions de la thèse : avancement du savoir sur la sécurité, la surveillance et la résistance esthétique

La thèse offre quatre contributions à l'avancement du savoir en lien avec les trois grandes littératures sur lesquelles elle se fonde et avec lesquelles elle établit des dialogues : les études critiques de sécurité, les études de surveillance et la théorisation de l'esthétique et de la culture populaire en Relations internationales. La thèse démontre la pertinence de l'art et de l'esthétique comme forme de résistance, propose une méthode pour étudier l'art et l'esthétique en RI, dessine une cartographie du pouvoir à l'ère numérique, et propose une forme de résistance collective à la fois technologique et normative.

Premièrement, la thèse démontre la pertinence de l'art comme forme de résistance ou de contre-pouvoir, en particulier face à la surveillance algorithmique des communications mondiales. Traditionnellement, l'esthétique est reconnue comme une forme importante de résistance dans la pensée critique, au point de souffrir à l'occasion d'une certaine fétichisation. Ainsi, pour les Adorno, Debord et Baudrillard, figures emblématiques de cette pensée, l'art permet de démystifier les représentations du monde qui empêchent tout un chacun de le voir tel qu'il est et de connaître ses intérêts réels. L'art jouit ainsi d'une force incontestée. Mais la pensée critique est incapable d'expliquer comment cette démystification procède au-delà de l'énonciation d'une dynamique d'inversion dont on comprend mal le point d'origine (Rancière 2008, 30-55).

Suivant Rancière (Rancière 2000) et Mirzoeff (Mirzoeff 2011), la thèse propose plutôt de faire de l'art une pratique qui s'insère dans le régime de visibilité, cette construction politique qui

normalise les hiérarchies sociales. En valorisant une forme visuelle créative, l'art permet de contourner l'invisibilité et de voir les structures de pouvoir, que celles-ci se trouvent masquées par le secret commercial ou d'État ou par la banalisation du quotidien. Jouer avec les formes visuelles permet de faire apparaître les rapports de force, première étape indispensable à leur politisation et à leur contestation. Ainsi, les œuvres analysées dans la thèse permettent-elles de rendre plusieurs piliers de la surveillance algorithmique des communications mondiales visibles. Elles permettent de voir la politique qui transcende les infrastructures de communication, l'opérationnalisation du savoir de sécurité et la participation numérique. Elles mettent en lumière la politique de la technique, de l'exceptionnel ou du normal. Moyen privilégié pour faire apparaître, l'art complète d'autres pratiques de résistance plus près de l'activisme classique qui cherche à transformer la norme sociale comme le lobbying d'élus et la mise en place de groupes de pression, l'activisme juridique, l'organisation communautaire et la mobilisation de mouvements sociaux. En plus de cet objectif pédagogique et normatif que la résistance esthétique partage, l'art encourage la production de formes déstabilisatrices potentiellement radicales qui invitent précisément à penser le monde à l'extérieur des cadres conceptuels conventionnels. Ainsi, les œuvres analysées proposent-elles ensemble la constitution d'une collectivité radicalement égalitaire de façon à stimuler la réflexion sur la dé-hiérarchisation et la désécurisation du monde (Aradau 2004), mais qui n'a pas à s'avérer une solution permenante aux problèmes soulevés.

Deuxièmement, poursuivant la démonstration de la pertinence de l'art tout en cherchant à dé-fétichiser son effet politique, la thèse développe une méthode pour étudier l'art et l'esthétique en RI. Je propose une voie médiane entre une approche entière sociologique de l'esthétique qui stipule la pertinence de l'art dans la sédimentation de ses représentations dans la société comme le proposent les théoriciens de la culture populaire en RI (Moore & Shepherd 2010) et une approche qui postule une ontologie déstabilisatrice à l'esthétique comme le suggère par exemple Bleiker (Bleiker 2009). Sise entre les deux, la thèse propose de concevoir l'esthétique sous l'angle de la pratique artistique (Rancière 2000) et pose les questions : qui se revendique de l'art résistant ? Que fait-on au nom de l'art résistant ? Quelle forme la critique artistique prend-elle ? Que dit-on à son propos ? Où cet art circule-t-il ?

Suivant cette méthode, l'art n'a pas d'existence ontologique préétablie, sinon celle de pratique revendiquée comme artistique. L'esthétique n'est pas par définition déstabilisante. L'art devient plutôt une performance, une prise de parole publique. Cette performance peut être, ou à

tout le moins peut se vouloir, déstabilisatrice : dans son texte, dans ses représentations visuelles, elle rend des structures de pouvoir visible, les remet en question. En ce sens, la performance artistique est résolument politique : pédagogique et contestatrice. Toutefois, étant publique, la performance appelle également la présence de spectateurs et d'un public qui interprètent l'œuvre. Celle-ci vit ainsi à travers son public. Cette publicité explique les limites de la déstabilisation, dépendante en partie de la réception de l'œuvre par ses spectateurs (Kear 2013), mais lui permet de s'insérer dans la durée. Le public devient, en d'autres mots, le médiateur de l'œuvre définissant son sens, l'insérant dans un contexte politique particulier et assurant sa pérennité dans le temps. Cette méthode préserve en définitive la dimension individuelle de la déstabilisation esthétique tout en démontrant sa pertinence collective. En proposant une lecture collective et publique de l'art, en portant attention aux réactions, critiques, lieux de circulation et contexte de diffusion notamment, elle permet de voir comment l'art agit sur l'espace social, conteste les structures sociales et construit un nouveau projet social.

Troisièmement, la thèse dessine, à travers les œuvres analysées, une cartographie du pouvoir à l'ère numérique. Mettant en lumière les trois piliers supportant la surveillance algorithmique des communications mondiales, ces œuvres démontrent le fonctionnement de la surveillance et ses conséquences : le potentiel presque illimité de collecte de données, la nature discriminatoire de la surveillance et l'impératif de visibilité. Interprétée dans un contexte de résistance, cette cartographie du pouvoir éclaire les limites et contraintes que la surveillance algorithmique impose à la surveillance. Elle permet en outre une entrée dans le débat public soulevé par les révélations Snowden. Les critiques au cœur de ce débat ont pour l'essentiel porté sur la menace que représentait la surveillance algorithmique contre la vie privée. Se greffaient à ces critiques des considérations légalistes sur les limites au pouvoir de surveillance des institutions de sécurité américaines à l'endroit des citoyens américains — ou des institutions nationales à l'endroit de leurs ressortissants. Conformément à cette définition individualisante du débat, les solutions proposées se résumaient au chiffrement et, de façon plus généralement, à la promotion de l'invisibilité numérique (Gurses, Kundnani & Van Hoboken 2016). Or, la cartographie du pouvoir révèle que ces critiques évitent de s'attaquer au cœur du problème de la surveillance algorithmique des communications mondiales. Cette dernière ne peut se réduire à son déploiement technologique et à son potentiel de collecte des données, aussi énorme soit-il. La surveillance menée par les dispositifs de sécurité occidentaux participe à la sécurisation du quotidien en normalisant les

mesures d'exception et en s'octroyant une liberté d'interprétation des données qui constituent pour tous une perte de contrôle sur notre présence numérique, une perte de contrôle particulièrement significative pour les individus membres de communautés ciblées par les appareils de sécurité. La surveillance et les pratiques de sécurité qu'elle supporte sont discriminatoires. La résistance doit prendre acte de la réalité du pouvoir et dépasser les réponses individuelles au profit d'une intervention collective plus à même de porter une critique sur la hiérarchie sociale que la surveillance rend possible.

Utilisant comme tremplin les observations sur les limites et contraintes à la résistance à la surveillance algorithmique des communications mondiales, la quatrième contribution de la thèse est précisément la proposition d'une avenue de contestation à la fois technologique et collective permettant la mise en place, aussi éphémère soit-elle, d'une collectivité radicalement égalitaire. Prenant acte qu'à travers ses pratiques de surveillance, les dispositifs de sécurité occidentaux agissent directement à partir des infrastructures du réseau Internet, les œuvres analysées proposent ensemble une forme de résistance qui intervient au même niveau, qui se déploie à partir des technologies numériques. Elle ne s'y limite toutefois pas. Les dispositifs de sécurité collectent des données afin d'en tirer du savoir sur les risques à la stabilité nationale. Les données numériques sont ainsi interprétées, insérées dans des scénarios de risque qui reproduisent et accentuent des tendances discriminatoires. De ce fait, la surveillance algorithmique contribue doublement à la sécurisation du quotidien. Elle transforme tout événement, toute routine et toutes données qui en résultent en savoir de sécurité potentiel. Rien du social ne doit échapper aux impératifs d'ordonnancement, de stabilisation et de maximisation de la logique sécuritaire, avec les risques d'exclusion que ces processus de contrôle impliquent. Là se situe la seconde dynamique de sécurisation portée par la surveillance algorithmique menée par les dispositifs de sécurité occidentaux. En ciblant certains individus et certaines populations davantage perçus comme des vecteurs de risque à la stabilité nationale, les appareils de sécurité stimulent et normalisent les effets discriminatoires de la politique et le recours aux mesures d'exception par le souverain.

Les œuvres analysées, *Autonomy Cube* des artistes-activistes Trevor Paglen et Jacob Appelbaum en particulier, proposent de résister à la sécurisation du quotidien en s'appropriant les technologies numériques afin de transformer les modes de visibilité de la surveillance algorithmique. À travers *Autonomy Cube*, la visibilité numérique n'est plus seulement une interpellation du pouvoir fortifiant les structures de pouvoir et les hiérarchies sociales. Amalgamant

des millions de présences à travers le réseau Tor, l'œuvre construit une nouvelle forme de collectivité radicalement égalitaire. *Autonomy Cube* masque dans la communauté les inégalités et brouille les processus de catégorisation sociale. L'œuvre performe ainsi une politique de contre-visibilité qui préfigure une collectivité marquée par un aplanissement des inégalités sociales, collectivité qui se veut en elle-même un espace de dissensus face à la société profilée et sécurisée de la surveillance algorithmique.

7.3 Limites de la thèse et projections : vers le développement d'un programme de recherche

Trois limites, qui constituent autant de projets de recherche, sont identifiables dans la thèse : l'approfondissement des composantes de l'assemblage de surveillance de sécurité, l'exploration des stratégies des artistes pour assurer la durée de l'effet esthétique et la diversification de la résistance artistique.

L'analyse d'œuvres critiques de la surveillance algorithmique des communications mondiales permet de dessiner une cartographie du pouvoir à l'ère numérique. Pourtant, si elle éclaire le fonctionnement des pratiques de surveillance des dispositifs de sécurité occidentaux, la gravité des enjeux soulevés par celles-ci justifie un approfondissement individuel de chacune des composantes de l'assemblage de surveillance. Ainsi, la thèse montre les transformations qu'entraînent les technologies numériques sur la gestion de la sécurité. Le premier coup d'œil permet de constater qu'elles offrent notamment de nouveaux instruments aux acteurs sécuritaires. Les technologies de collecte de données permettent de capter des flots de données en temps réel, de pénétrer les appareils des personnes d'intérêt et de décoder les programmes de chiffrements. La surveillance algorithmique donne ainsi accès, à travers des montagnes de données, à des informations révélatrices des comportements des utilisateurs, de leurs réseaux, mêmes aux contenus de leurs communications. Ces informations peuvent être couplées aux scénarios de risque pour évaluer les dangers auxquels la société fait face. En ce sens, les technologies offrent un outil d'une extrême précision pour contrer les risques d'attentats terroristes ou, plus généralement, de déstabilisation sociale.

Toutefois, la surveillance algorithmique ne peut se réduire à cet outil de sécurité. Elle est performative. Les technologies numériques transforment l'exercice de la souveraineté. Prolongeant la réflexion sur la surveillance comme pratique culturelle, la surveillance algorithmique peut être

interprétée comme une pratique de souveraineté : l'exercice du regard d'exception, de la détermination des frontières de la collectivité et du droit de vie et de mort. La mobilité des données rendue possible par l'internationalisation des infrastructures de communication permet au souverain d'étendre sa sphère d'intervention et de capturer les données même si l'origine et la destination sont au-delà de son territoire. Non protégées par ce qui pourrait être un pendant numérique de la liberté de navigation, les données sont sujettes à l'autorité de chaque État qu'elles croisent, à l'avantage de ceux dont les infrastructures sont les plus développées et les centrales aux communications mondiales. Les infrastructures numériques redécoupent ainsi les catégories de mobilité et de territoire. Elles deviennent l'espace d'action du souverain (Easterling 2016).

Les technologies numériques dédoublent la mobilité de l'utilisateur. Alors que celui-ci demeure immobile, ses données circulent à travers le monde, franchissant les frontières. Cette circulation peut lui être invisible, elle n'en est pas moins significative permettant la collecte des données par la surveillance algorithmique. Internet, espace supposément virtuel et mondial, apparaît à l'utilisateur comme un espace détaché de la configuration territoriale mondiale. Toutefois, les infrastructures numériques participent à la reterritorialisation de l'espace numérique permettant au souverain de revendiquer un droit d'action. Ce droit d'action s'exerce à travers les infrastructures, directement par les commis de l'État travaillant pour les agences de renseignement, ou à travers la délégation de pouvoir vers leurs partenaires économiques. Il s'exerce localement ou à travers le monde. Cette territorialité s'inscrit ainsi dans la lignée de l'expansion du Homeland américain que Medovoi analysait comme le penchant sécuritaire de la mondialisation économique (Medovoi 2007). Elle permet d'étendre la sphère d'intervention du souverain américain au-delà de son territoire national. Le territoire national conserve une pertinence dans la surveillance algorithmique, mais, plus encore, c'est l'accès au nouveau territoire façonné par les infrastructures numériques qui importent. C'est ce nouveau territoire que le souverain voudra cartographier.

Poursuivre l'analyse de l'exercice de la souveraineté à travers les infrastructures est important pour comprendre l'extension du pouvoir d'intervention des dispositifs de sécurité américains et occidentaux. À cet effet, il pourrait être intéressant de faire une contre-cartographie des infrastructures numériques, des points d'accès et des partenariats de la surveillance algorithmique, ou encore de chercher à approfondir les fonctionnements d'un centre de collecte spécifique afin de voir la performance souveraine en action. Toutefois, de tels projets font inévitablement face aux problèmes d'accès à l'information dans le monde ultrasecret de la sécurité

nationale. Pour contourner ce problème, il pourrait alors être intéressant de tourner l'attention, dans une perspective de résistance, vers les entreprises de construction d'infrastructures alternatives, qu'elles soient gouvernementales, brésiliennes ou européennes (Bauman et coll. 2014), populaires ou artistiques (Antoniadis 2016).

Du même souffle, la surveillance algorithmique complique l'identification du souverain, responsable de l'exception. Pour la NSA, seules les données analysées par un agent sont dites collectées ou surveillées (EFF 2012). Or, vu la somme de données ingérées, les analystes ne manipulent pas toutes les données acquises. La distinction de la NSA est établie sur la base d'une division nette entre le travail humain et celui des algorithmes. On en déduit que le caractère intrusif de la surveillance proviendrait uniquement du fait du regard humain. Comme le soulignent Claudia Aradau et Tobias Blanke,

> [Theresa] Shea [former Director of Signals Intelligence Directorate at NSA] and other intelligence experts invoke an analogy between NSA bulk data processing and targeted surveillance. Ultimately, the assumption is that there is no surveillance where data in not 'seen' by a human being. The human/machine distinction, with humans supposedly only coming in at the end of the data processing, aims to render these practices of data collection and processing legitimate by enacting a strong separation between humans and machines (Aradau & Blanke 2015, 5).

Pour Aradau et Blanke, cette justification de la surveillance de masse sur la base d'une séparation nette entre humain et machine est fausse et témoigne d'un refus de problématiser le caractère social des technologies. L'attention portée vers une personne d'intérêt générée par les algorithmes, expliquent-ils, est indissociable du processus de construction des algorithmes d'abord, et des multiples étapes de validation de résultats subséquemment. Les acteurs humains écrivent et confirment les conclusions des algorithmes. En même temps, les algorithmes relèvent et accentuent certains résultats et phénomènes, corroborant les perceptions initiales codées lors de l'écriture de l'algorithme (Amoore 2009b; Aradau & Blanke 2015). Cette étroite relation cyclique entre humains et machines, que Tarleton Gillespie nomme le « recursive loop between the calculations of the algorithm and the "calculations" of people » (Amoore & Raley 2017, 5), rend d'autant plus difficile la tâche d'identifier clairement qui de l'analyste ou de l'algorithme est le surveillant, qui est responsable en cas d'erreur. Dans ce contexte, certains appellent à repenser l'éthique de responsabilité de la prise de décision avec algorithme. « The critical and political responses to these kinds of questions have overwhelmingly sought to reinstate the human as the proper figure of

sovereignty, its executive decisions bound by juridical and ethical codes of conduct, » explique Louise Amoore et Rita Raley.

> Thus the 'human in the loop' often functions as a fail-safe for the speculative imaginary of driverless cars, autonomous weapons and robotic surgery. However, taking seriously the generative and world-making capacities of algorithms means troubling the human as the sole locus of security decision, authorship, interpretation and ethico-political responsibility (Raley, 2016). After all, humans and algorithmic systems can be said to have co-evolved in complex processes of technogenesis, with human knowledge and logical structures migrating between people and software agents (Hayles, 2012) (Amoore & Raley 2017, 5)

Refuser de reconnaître que l'accès et le filtrage des données constituent une forme de surveillance, comme le fait le dispositif de sécurité sur la base d'une prétendue objectivité du support technologique, mène à nier le caractère politique des algorithmes, à ignorer les effets discriminatoires de la boucle récursive de la surveillance de sécurité, rationalisés dans un contexte de profilage et de catégorisation, et ramenés au statut de dommage collatéral ou de faux positif. À travers les algorithmes, le pouvoir d'exception se diffuse une fois de plus sans que l'on soit en mesure d'établir les responsabilités ni de prévoir les décisions (Amoore 2011; Zwitter 2014; Aradau & Blanke 2017). Une réflexion éthique s'impose donc sur la responsabilité du souverain algorithmique. La surveillance algorithmique transforme donc les enjeux de la souveraineté et de la normalisation de l'exceptionnalisme, et de la responsabilité politique, mais son impact se fait aussi sentir sur d'autres questions notamment la construction de l'identité nationale et de l'ennemi, et la transformation de la citoyenneté. Tous ces enjeux méritent d'être étudiés à part entière si ce n'est, dans une perspective de résistance, que pour pouvoir identifier de nouveaux points de faille à exploiter.

En adoptant les révélations Snowden comme moment de référence artistique et politique, la thèse pose également la question de la durée. Si une partie de la réponse à cette question se trouve dans la méthode d'analyse des œuvres conçues comme performances publiques médiées par des spectateurs et des publics, un approfondissement des stratégies artistiques mises de l'avant pour assurer la permanence de l'effet esthétique est pertinent. L'esthétique se veut déstabilisatrice, mais plusieurs artistes se posent également en pédagogues et cherchent une transformation à long terme de la société. Si d'aucuns prétendent pouvoir mener cette transformation par le seul biais de son art, celui-ci est néanmoins parti d'une transformation normative qui s'inscrit dans la durée. Comment les artistes assurent-ils cette inscription dans le temps ? Quelles stratégies mettent-ils en œuvre ? La question est d'autant plus criante que les événements politiques et les réponses

artistiques à ceux-ci se succèdent au risque de s'éclipser l'un et l'autre. Comment les artistes naviguent-ils cette fluctuation tout en demeurant pertinent au regard du moment et des phénomènes sociaux associés ?

Une analyse plus pointue et spécifique à chaque œuvre que celle effectuée dans le cadre de cette thèse pourrait permettre d'approfondir ces stratégies artistiques et la pénétration des œuvres dans l'espace public. Au-delà de l'incursion au cœur du champ artistique pour étudier de près les relations de pouvoir internes pouvant jouer sur la circulation et la sédimentation d'œuvres, d'autres cadres analytiques pourraient permettre de mieux comprendre le rapport entre œuvre et durée. L'analyse des publics matériels et la sociologie des scandales (de Blic & Lemieux 2005; Boltanski et coll. 2007; Latour 2003) apparaissent comme des repères théoriques intéressants. Ces approches s'intéressent autant aux démarches intentionnelles des acteurs pour assurer la circulation de leurs idées qu'à l'autonomie des textes et de leur circulation une fois émis, deux éléments indispensables pour comprendre comment les œuvres atteignent leur public et s'imposent dans un espace social. S'intéresser aux stratégies notamment numériques des artistes permettrait en outre de voir si les nouveaux médias, notamment sociaux, permettent aux œuvres de briser la niche artistique (Gat 2015).

Enfin, dépasser le moment Snowden signifie également étudier la contestation artistique d'autres formes de surveillance et celle provenant d'autres milieux artistiques. La diversité de l'art numérique témoigne d'une fascination et d'une angoisse à l'endroit du monde numérique et des mécanismes de contrôle social qu'il permet. Explorant cet enjeu sous une multitude d'angles, proposant autant d'avenues pour l'éclairer, la mettre en échec ou la contourner, cette diversité esthétique témoigne de la pluralité des pratiques et des contextes de surveillance. S'il faut reconnaître l'étroite proximité entre la production, la collecte et l'analyse des données commerciales et la surveillance sécuritaire, il faut aussi reconnaître leurs spécificités techniques, stratégiques et sociales. Les pratiques de surveillance de Google, celles de la NSA et celles de GCHQ ne suivent pas les mêmes règles, peu importe que celles-ci soient issues d'un protocole informatique, d'une directive interne, ou d'un cadre législatif. Pourtant, la tentation est grande de généraliser les pratiques de l'un pour permettre de brosser le tableau unique d'un univers immensément vaste et raturé, en même temps qu'il est si étroitement connecté. La diversité des interventions artistiques rappelle donc la richesse de cet univers et met en garde contre le piège de

cette universalisation. Universaliser les pratiques de surveillance triche inévitablement laissant hors cadre certains phénomènes et détails.

L'hétérogénéité de l'assemblage de surveillance confirme plutôt la nécessité de penser et d'approfondir la diversité de la résistance artistique à la surveillance algorithmique. Dans la thèse, j'approfondis quelques œuvres qui éclairent et contestent à leur façon la surveillance de sécurité. Les contraintes d'espace et de cohérence m'obligent toutefois à laisser en pan un grand nombre de projets auxquels j'aurais souhaité pouvoir consacrer davantage de temps[2]. Or, si cette limitation se comprend dans la perspective d'une thèse, elle ne fait aucun sens face à un phénomène dont la portée sociale est aussi grande. L'univers numérique, la surveillance algorithmique et les régimes de visibilité qui en résultent s'insèrent et/ou transforment une multitude de sphères sociales que ce soit la définition du sujet, le rapport à l'autre, la présence publique, la participation politique, l'économie, les conditions de genre ou, bien entendu, la sécurité qui fut l'angle retenu ici. Pourtant, au risque de reproduire la logique paranoïaque du savoir de sécurité, il est difficile d'approfondir une seule dimension isolément. Analyser l'aspect sécuritaire amène sur le terrain de l'économie, de la subjectivité, de l'autre, de la politique. Étudier les structures économiques pourrait nous amener à discuter les rapports de genre et la présence publique. Restreindre le sujet d'étude risque de reproduire les silos que l'analyse interdisciplinaire tente de percer. Afin d'éviter ce piège, poursuivre l'étude de l'art résistant en croisant les thèmes pourrait permettre d'illustrer les multiples interconnexions et les différences entre les pratiques de surveillance. Il serait intéressant de voir, par exemple, quelles formes de visibilité du sujet les critiques de la surveillance de sécurité, économique et de genre proposent. Cette comparaison permettrait d'identifier les points de convergence, les contradictions et rappellerait, si besoin est, la nécessité d'analyser la résistance dans son contexte de production et d'éviter les jugements dichotomiques. Résister la discrimination sécuritaire par la revendication d'une présence publique s'explique peut-être difficilement face à

[2] Mentionnons, sans ordre particulier, la cartographie de *Submarine Cable Taps* d'Ingrid Burrington, les photographies de Trevor Paglen et les projets *AdNauseam*, *Data Selfies* et *Data Detox* que j'ai pu survolé, ainsi que d'autres qui se sont mérité au mieux une mention tels que *Tracking Transience* d'Hasan Elahi (Elahi 2013), *Karen* du collectif Blast Theory (Blast Theory 2018), *Internet Cache Self-Portrait Series* d'Evan Roth (Roth 2015), *JLM, Inc.* de Jennifer Lyn Morone (Morone 2015), *pplkpr* de Kyle McDonald et Lauren McCarthy (McDonald and McCarthy 2014), *Webcam Venus* de Pablo Garcia (Garcia 2015), *High retention, slow delivery* de Constant Dullaart (Dullaart 2015b), *Overexposed* de Pablo Cirio (Cirio 2015), *Seeing Networks* de Ingrid Burrington (Burrington 2017), *ScareMail* de Benjamin Grosser (Grosser 2015), les expositions *Body Anxiety* (Schrager and Chan 2015b) et *The Glass Room* (The Glass Room 2017), l'espace de diffusion *Ars Electronica*.

l'enjeu de la vie privée. Cela ne signifie pas pour autant qu'elle soit complice de la surveillance. Elle déstabilise une des facettes de l'assemblage.

Il importe néanmoins, dans l'étude de ces diverses facettes, de ne pas oublier la nature discriminatoire de la surveillance. L'étendue de la collecte de données pointe vers l'existence de pratiques de surveillance de masse qui soumettraient la population entière à la surveillance. D'un autre côté, l'opérationnalisation du savoir de sécurité suggère l'existence d'une surveillance discriminée, caractérisée par des pratiques de ciblage et de catégorisation contribuant à la marginalisation de certains segments de la population. Ce dédoublement de la surveillance pourrait peut-être expliquer l'incompréhension, voire l'incommensurabilité, entre les évaluations des pratiques de surveillance de sécurité proposées par les acteurs de la société civile qui insiste sur la nature indiscriminée de la surveillance et par le dispositif de sécurité qui prétend au contraire restreindre la portée de la surveillance en ciblant uniquement les individus représentant une menace à la société. Pourtant, les deux coexistent, ayant chacun des effets distincts, mais non moins significatifs.

La surveillance de masse sécurise l'ensemble de l'espace numérique. À travers cette sécurisation, tout et tous peuvent devenir l'objet d'attention. Cela est possible parce que le double numérique mène une vie indépendante de l'individu auquel il est rattaché. Les données, une fois générées, circulent d'une institution à l'autre où elles sont interprétées en fonction des besoins de l'institution en question. Les données ne disparaissent pas, au mieux, elles dorment. La durée des données permet ainsi aux institutions de sécurité de revenir dans les temps pour donner un nouveau sens à des données qui auraient pu être écartées au départ (Snowden, Poitras & Greenwald 2013). La liberté d'interprétation des données couplée à la volonté d'intercepter les risques à la sécurité nationale de façon préemptive accroît la possibilité de surinterprétation des données ciblant erronément certains individus (Aradau & Blanke 2015). Dans la terminologie algorithmique, cette surinterprétation s'appelle un faux positif, dans celle de la sécurité, elle engendre un dommage collatéral. On comprend alors qu'à travers le processus d'interprétation des données, la surveillance de masse devient également discriminée, avec une économie de l'attention inégalement distribuée (Amoore 2009b).

Cette double nature de la surveillance soulève plusieurs enjeux. La sécurisation de l'univers numérique encourage la peur de l'autre et la suspicion généralisée, posant la question de l'identité

des membres de la communauté politique. Cette dualité a également des conséquences sur la résistance à la surveillance. Quoiqu'en disent les critiques, la surveillance numérique ne peut se résumer à la pratique universelle et indifférenciée d'une collecte de masse de données. La surveillance numérique est ciblée et discriminatoire. Or, le biais universaliste est très présent dans l'esthétique de la communauté d'artistes explorée ici. *Citizen Ex*, *IXmaps*, les photographies de Trevor Paglen, *Secret Power*, *Data Detox*, *TrackMeNot* visualisent tous la surveillance de masse sans jamais réellement attirer l'attention sur son effet discriminatoire. Dans une moindre mesure, *Autonomy Cube* tombe aussi dans le piège de la surveillance universelle. Si l'œuvre reconnaît les processus de stratification sociale permis par la surveillance algorithmique, elle propose néanmoins une avenue unique pour y échapper, peu importe que l'utilisateur soit ou non une personne d'intérêt. D'un côté, cette unicité permet l'égalisation sociale qui brouille le ciblage de la surveillance algorithmique. De l'autre, elle ne reconnaît pas les revendications particulières que pourraient entretenir certains groupes marginalisés.

Dans ce contexte, il serait tentant de leur adresser la critique formulée par Torin Monahan à l'endroit de l'art de camouflage. « Although anti-surveillance camouflage and fashion designs may offer creative forms of resistance that resonate with artists and their audiences, » écrit-t-il,

> … they fail to achieve countervisuality. … [T]he works enact a play of individual avoidance, rather than asserting a collective right to look back and challenge authority. Many of them reproduce discourses of universalism that elide difference as well as the marginalizing and discriminatory effects of surveillance. As such, these forms of aestheticized resistance identify vital areas of concern but address them in ways that may fetishize, trivialize, and normalize larger structural conditions of inequality and danger (Monahan 2015, 4).

Si l'esprit de la critique demeure pertinent, deux constats s'imposent en défense des œuvres analysées ici. D'abord, dans la diversité des pratiques de surveillance, la surveillance de masse a un effet particulier et non négligeable qu'il convient de contester. Ensuite, ces œuvres partagent une démarche collective de résistance à la surveillance. Les projets de contre-visibilité de Bridle et Denny, par exemple, promeuvent une plus grande connaissance et sensibilité vis-à-vis des mécanismes de pouvoir de la surveillance algorithmique au sein de la population. Celui de Paglen et Appelbaum préfigurent dans le réseau Tor une nouvelle collectivité égalitaire.

Le problème n'est pas d'offrir une contre-visibilité à la surveillance de masse, mais de négliger l'effet discriminatoire. La question de cette négligence se pose. Le regard post-Snowden adopté afin de baliser la thèse explique peut-être en partie le biais pour la surveillance de masse.

Toutefois, à la lumière du statut social des artistes, si l'on se rappelle l'hypothèse de David Lyon sur le retour en force du discours sur la vie privée (Lyon 2001, 22), ce biais n'est pas très surprenant. À forte majorité, les artistes étudiés sont des hommes blancs éduqués qui démontrent leurs privilèges par leur grande mobilité internationale. James Bridle détient une maîtrise de l'University College, London. Son art a voyagé en Europe, dans les Amériques, en Asie et en Australie (Bridle 2018). Simon Denny, artiste néo-zélandais domicilié à Berlin, possède un diplôme de la Städelschule de Frankfort. Son art a aussi abondamment voyagé en Europe et en Amérique du Nord (Leonard 2017). Trevor Paglen détient des diplômes de l'Art Institute of Chicago et de l'University of California, Berkeley. Similairement, son art a fait le tour du monde et a été présenté dans certaines des plus grandes institutions mondiales (Paglen 2018). Dans ce contexte, leurs critiques de la surveillance numérique et de la société de contrôle acquièrent une dimension paradoxale : eux-mêmes bénéficient des opportunités offertes par le système qu'ils dénoncent — démontrant une fois de plus, si cela est nécessaire, la porosité de la frontière entre participation et résistance.

Penser différemment les contours de la communauté d'artistes étudiée aurait laissé voir une autre facette de la résistance à la surveillance. Étudier, à la suite de Susan Cahill, une communauté canadienne par exemple aurait offert un portrait d'artiste différent (Cahill 2018). Peut-être cela souligne-t-il la nécessité d'approfondir le champ artistique et de s'intéresser à la distribution des fonctions et pouvoirs entre les institutions muséales, aux laboratoires de création, aux lieux de formation, aux médias, aux partenaires et bailleurs de fonds, aux professionnels de l'art, aux codes esthétiques… Une analyse de champ permettrait de mettre en lumière les rapports de pouvoir au sein de cette communauté, les véhicules de circulation, les espaces de diffusion et les barrières d'entrée. Dans tous les cas, il existe un véritable besoin de consacrer davantage d'attention aux préoccupations et aux demandes des groupes marginalisés par la surveillance algorithmique et sous-représentés dans la communauté artistique (Morgner 2017; P. J. Burke & McManus 2011), même si celles-ci s'inscrivent en porte-à-faux avec les thèmes dominants de la résistance à la surveillance comme la vie privée, l'anonymat et l'invisibilité.

Une œuvre comme *Tracking Transience* d'Hasan Elahi (Elahi 2013), par exemple, discute d'anonymat. Pourtant, elle revendique également le droit d'apparaître sans que le corps (foncé), la religion (musulmane) ou le double numérique de l'artiste ne soulèvent la suspicion. L'artiste démontre dans son projet d'autosurveillance qu'il n'est rien de plus qu'un citoyen « normal ». Elahi n'est pas un terroriste, il n'est pas une menace à l'ordre social, il est un citoyen américain tout ce

qu'il y a de plus banal. *Tracking Transience* est en ce sens une intervention publique et politique, la mise en visibilité de l'artiste qui refuse les hiérarchies sociales en place qui font du « musulman » une menace à la sécurité nationale américaine (et occidentale) et revendique un droit à être différent et normal. En ce sens, cette visibilité est choquante : elle bouscule les préjugés courants qui associent l'invisibilité de la communauté au complot terroriste. La visibilité de *Tracking Transience* contraint en définitive à redistribuer les parts sociales, à reconnaître la position sociale d'Elahi et, à travers lui, celle des communautés marginalisées.

En ce sens, la visibilité d'Elahi rejoint celle d'artistes féministes qui réclament que leurs corps et leur présence numérique cessent d'être associés à un objet de désir sexuel ou à l'industrie pornographique. L'exposition en ligne *Body Anxiety* se veut une réappropriation de la visibilité du corps de la femme et une contestation de la chosification produite par Internet et le monde artistique. Leah Schrager et Jennifer Chan, commissaires de *Body Anxiety*, écrivent ainsi :

> [t]hroughout art and film history, the female body and nude has been an ongoing subject in male-authored work. More often than not, the woman's body is capitalized on in these works while their voice is muted. … Today, artists use the internet as a platform to create and share their own imagery. While appropriation might be a common practice in contemporary art, using the internet as gender-queer performative space allows artists to question contemporary attitudes towards feminity (Schrager & Chan 2015a).

Paradoxalement, ces artistes résistent le régime de visibilité par la nudité et une reproduction des codes de la pornographie. À l'antipode d'une logique d'anonymat, elles choisissent d'apparaître, de se mettre littéralement à nue, pour se réapproprier le droit de déterminer leur image. La question de la complicité ou de l'efficacité de la tactique de résistance peut se poser — comme avec toute autre œuvre d'ailleurs —, mais il semble surtout important de reconnaître le besoin de visibilité, plutôt que d'invisibilité, exprimé par ces groupes minorisés. Pourquoi ces artistes revendiquent-elles une visibilité que plusieurs autres acteurs de l'art résistant tentent, au contraire, d'éviter ?

7.4 Visibilité créative, visibilité créatrice : vers une réimagination collective du monde

L'étendue des infrastructures de collecte de données, la volonté affichée de tout collecter et l'impératif de visibilité auquel nous sommes soumis montrent la difficulté d'apparaître dans l'espace numérique sans devenir complice de l'économie politique de la surveillance algorithmique. Celle-ci restreint la possibilité d'une présence numérique autodéterminée, c'est-à-

dire une présence qui ne serait ni l'objet de contrôle ni utilisée pour contrôler les autres. L'impossibilité de s'émanciper des contraintes du contrôle est inscrite autant dans les codes numériques que dans les stratégies de pouvoir de la surveillance algorithmique. Pourtant, s'il est illusoire de penser sortir entièrement des structures de pouvoir, l'art numérique permet des espaces temporaires de déstabilisation. La réduction ou le brouillage des données, notamment, offrent un certain contrôle sur notre présence numérique.

Il convient cependant d'apporter quelques bémols à ses espoirs de contrôle. La spéculation sécuritaire rappelle qu'aucun contrôle ne saura être parfait et nous force à accepter une part d'arbitraire. En outre, le désir de contrôle nous isole dans une logique individualiste où l'objectif est la création d'un espace clos au cœur duquel le soi pourra aller se conforter dans sa propre authenticité. L'authenticité détient pourtant peu de valeur aux yeux de la surveillance algorithmique pour qui l'utilité des profils et catégories assignés aux individus pour faire mousser les ventes ou préempter des attentats terroristes prime sur la justesse de la reconstitution biographique. L'entreprise de la surveillance algorithmique est créative et créatrice d'un monde néolibéral et sécuritaire. Plutôt que de s'isoler l'un de l'autre dans une pluralité d'espaces privés séparés par les cloisons de l'unicité individuelle et de la peur de l'autre, la résistance à la surveillance algorithmique doit s'aventurer sur le même terrain que la surveillance algorithmique et réimaginer la collectivité.

Le paradigme actuel qui informe notre rapport au monde numérique valorise l'individualité de l'utilisateur. Les services sont personnalisés, garantissent à travers le nuage un espace unique pour le soi, offrent la possibilité d'afficher sa personnalité et permettent de mieux se connaître et de s'épanouir. Le participant-utilisateur reproduit en ce sens le moi entrepreneur-consommateur néolibéral. Pourtant, cette individualité est aussi réelle que fantasmée. Réelle dans la société atomisée, elle est vite contestée par la volonté de « relier les points » de la surveillance algorithmique. Les mécanismes de collecte de données soumettent l'individu à la surveillance sur la base de ses apparitions dans les communications d'autres personnes. Une analyse du Washington Post citée par l'EFF évaluait ainsi que 90 % des individus surveillés ne sont pas directement visés par les sélecteurs (EFF 2012). Ils apparaissent dans la boîte de réception d'un service de messagerie, font partie du carnet d'adresses, partagent des amis communs. Le processus de construction du savoir algorithmique montre également que l'individu est indissociable de son environnement. Découpé, recomposé, comparé, catégorisé, l'individu acquiert un sens — une

identité, un potentiel de profitabilité, ou un niveau de risque — en fonction de ses liens avec les autres. Il est en lui-même vide de sens s'il ne peut être inséré dans une population qui permet de contextualiser ses actions et de le projeter dans l'avenir. Paradoxalement, les mégadonnées contredisent la prédominance que le néolibéralisme attribue à l'individu sur le social. Elles invitent du coup à ramener le collectif au cœur de la réflexion sur le sujet.

D'une certaine façon, le lien entre numérique et collectivité est bien établi, au point de devenir même banale, comme le pointent Barney et coll. :

> A gloss of dominant terms used to convey the nature of online sharing—ad hoc, the commons, peer-to-peer, prosumer, user-driven innovation, spontaneity, creativity, empowerment, crowd-sourcing, and especially openness—bolsters a now-entrenched notion that the Internet is ideal for "organization without organizations," to cite the subtitle of Clay Shirky's influential book *Here Comes Everybody*, a de facto bible for this sort of thinking. What is ostensibly distinct today is how the Internet allows humans to bypass institutions and hierarchies while encouraging direct connection and participation (Barney et coll. 2016, xxiii).

Toutefois, du même souffle, les auteurs rappellent que cette prétention à la radicalité est prématurée ; la cooptation ou l'institutionnalisation sont des processus qui affectent également les collectivités numériques. Il ne s'agit donc pas de tenir pour acquise la radicalité des relations numériques, mais de s'y intéresser afin de comprendre comment elles pourraient être porteuses de nouveauté.

Autonomy Cube propose une communauté radicale. Pour Paglen et Appelbaum, d'inspiration anarchiste, la liberté individuelle est indissociable de celle de l'autre, d'où la nécessité d'assurer l'autonomie et l'égalité de chacun et de tous. Convertissant cet objectif politique en termes numériques, les artistes proposent dans leur œuvre de masquer l'utilisateur Internet, sans égard à son identité, dans la communauté qui compose le réseau Tor. Chacun y garantissant l'anonymat de l'autre, l'œuvre brouille les mécanismes de contrôle de la surveillance algorithmique qui fonctionne par la catégorisation. *Autonomy Cube* aplanit les différences sociales qui permettent à la surveillance d'attribuer un sens aux données collectées et aplanit les inégalités sociales que la surveillance renforce dans sa distribution des privilèges et de la suspicion. *Autonomy Cube* constitue en outre un geste de visibilité : la revendication numérique d'une appartenance à une communauté égalitaire.

La revendication de ce droit d'apparaître est doublement significative, politique. D'abord, elle met en échec — le temps d'un instant — la surveillance algorithmique, au grand dam des autorités qui fustigent et ciblent le réseau pour cette raison. En ce sens, elle suggère le besoin de rompre avec la segmentation et l'ordonnancement social par le moyen des algorithmes. Tor/*Autonomy Cube* rejette ainsi la prédétermination individuelle et collective que la société de contrôle exerce, encourageant l'autonomie et la liberté de devenir. Ensuite, elle préfigure une société alternative et inclusive — au risque, comme le souligneront les détracteurs, d'y accueillir des individus socialement dangereux ou moralement condamnables. Pourtant, la question du vice dépasse la portée de l'œuvre, suggère-t-on. Tor/*Autonomy Cube* n'est pas à l'origine du vice qui habite la société. Plutôt que de contrôler sur la base de probabilité statistique, il faut revaloriser la présomption d'innocence pour protéger ceux qui pourraient y être associés sans fondement. Ainsi, rejetant l'argument selon lequel le réseau permet à certains de mener leurs basses œuvres, Tor/*Autonomy Cube* devient à travers cette société alternative un projet de visibilité, de réimagination d'une communauté qui refuserait la stratification sociale. Cet espace de visibilité, aussi momentané soit-il, contient le potentiel politique de déstabiliser l'ordre social en place en réécrivant de nouvelles normes où l'autre n'est pas directement associé à suspicion.

De la même manière que Tor/*Autonomy Cube* ne peut être tenu responsable de tous les torts, la surveillance algorithmique n'a pas inventé la peur de l'autre. Elle amplifie les dynamiques en place, lui offrant la précision et l'abondance des données numériques, et les inférences de l'analyse des mégadonnées qu'elle couple à une logique paranoïaque déjà portée vers la spéculation. La persistance de la peur de l'autre incite à réfléchir sur le rôle que peut jouer l'art numérique dans la réimagination de la collectivité. Si l'on ne peut pas empêcher la surveillance algorithmique de spéculer sur l'identité du monde, l'objectif, ou du moins un des objectifs de la résistance, devrait être l'écriture d'un autre monde que l'on pourra lui opposer. Dans le contexte de la surveillance algorithmique menée par les NSA et consœurs et de leur entreprise d'*ubër*-sécurisation, réimaginer la collectivité, lutter contre la discrimination demande de reconnaître, comme l'écrit Eric Stoddart, « [that h]ow we act has consequences for how more or less visible others might be—at a cost to them and possibly also to us. … Resistance will mean re-narrating immigrant and foreigner categories deployed by those whose fear of the Other has become enmeshed in a perverted patriotism » (Stoddart 2014, 48). *Autonomy Cube* propose une nouvelle forme de narration. Cette écriture pourra aussi prendre la forme de la mise en place d'infrastructures de communication

alternatives (MAZI 2018), de structures de partage (Cammaerts 2016), de campagnes d'activisme numérique (M. Brown et coll. 2016), de mèmes (Gal, Shifman & Kampf 2016), d'art numérique proposant ensemble un monde où l'autre n'est pas une menace, n'a pas à nier sa différence ou à se soumettre à un impératif d'hypervisibilité. La visibilité n'est pas qu'un processus de soumission, elle est aussi, peut-être avant tout, un processus de création.

Bibliographie

Aas, Katja Franko. 2006. "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture." *Crime, Media, Culture: An International Journal* 2 (2): 143–58. doi:10.1177/1741659006065401.

AccessNow. 2017. "Global Coalition from Five Nations Demands 'Five Eyes' Respect Encryption." *AccessNow*. June 30. https://www.accessnow.org/83-organizations-experts-5-nations-demand-five-eyes-respect-strong-encryption/.

Ackerman, Spencer. 2013. "James Clapper: Obama Stands by Intelligence Chief as Criticism Mounts." *The Guardian*. June 12. http://www.theguardian.com/world/2013/jun/12/james-clapper-intelligence-chief-criticism.

Ackerman, Spencer, and James Ball. 2014. "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ." *The Guardian*. February 28. http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

ACLU. 2015a. "ACLU Sues NSA to Stop Mass Internet Spying." *American Civil Liberties Union*. March 10. https://www.aclu.org/national-security/aclu-sues-nsa-stop-mass-internet-spying.

ACLU. 2015b. "Wikimedia v. NSA: Challenge to Mass Surveillance Under the FISA Amendment Act." *American Civil Liberties Union*. Accessed March 11. https://www.aclu.org/national-security/wikimedia-v-nsa.

Adams, Tim. 2017. "Trevor Paglen: Art in the Age of Mass Surveillance." *The Guardian*. November 25. http://www.theguardian.com/artanddesign/2017/nov/25/trevor-paglen-art-in-age-of-mass-surveillance-drones-spy-satellites.

Adey, Peter. 2006. "'Divided We Move': the Dromologics of Airport Security and Surveillance." In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 195–208. New York: Routledge.

Adey, Peter. 2009. "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body." *Environment and Planning D: Society and Space* 27 (2): 274–95. doi:10.1068/d0208.

Adey, Peter, and Ben Anderson. 2012. "Anticipating Emergencies: Technologies of Preparedness and the Matter of Security." *Security Dialogue* 43 (2): 99–117. doi:10.1177/0967010612438432.

Agamben, Giorgio. 1998. *Homo Sacer: Sovereign Power and Bare Life*. Stanford: Stanford University Press.

Agamben, Giorgio. 2013. "For a Theory of Destituent Power." In. Athens.

Aguiton, Christophe, and Nicolas Haeringer. 2012. "(S')occuper (de) la gauche, ou l'ignorer ?." *Mouvements* 69 (1) : 116–27.

Aikens, Nick, and Trevor Paglen. 2016. "Autonomy Cube." *L'internationale*. June 16. http://www.internationaleonline.org/research/alter_institutionality/71_autonomy_cube.

Ainsley, Julia Edwards, Dusting Volz, and Kristina Cooke. 2017. "Exclusive: Trump to Focus Counter-Extremism Program Solely on Islam Sources." *Reuters*. February 1. https://www.reuters.com/article/us-usa-trump-extremists-program-exclusiv/exclusive-trump-to-focus-counter-extremism-program-solely-on-islam-sources-idUSKBN15G5VO.

Albrechtslund, Anders, and Lynsey Dubbeld. 2005. “The Plays and Arts of Surveillance: Studying Surveillance as Entertainment.” *Surveillance & Society* 3 (2/3): 216–21.
Albrechtslund, Anders, and Peter Lauritsen. 2013. “Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation.” *Geoforum* 49 (C): 310–16. doi:10.1016/j.geoforum.2013.04.016.
Aldis, William. 2008. “Health Security as a Public Health Concept: a Critical Analysis.” *Health Policy and Planning* 23 (6): 369–75. doi:10.1093/heapol/czn030.
Altman Siegel. 2015. “Trevor Paglen-Press Release.” *Altman Siegel*. San Francisco.
Amicelle, Anthony. 2011. “Towards a ‘New’ Political Anatomy of Financial Surveillance.” *Security Dialogue* 42 (2): 161–78. doi:10.1177/0967010611401472.
Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. “Questioning Security Devices: Performativity, Resistance, Politics.” *Security Dialogue* 46 (4): 293–306. doi:10.1177/0967010615586964.
Amoore, Louise. 2006a. “‘There Is No Great Refusal’: The Ambivalent Politics of Resistance.” In *International Political Economy and Poststrutural Politics*, edited by Marieke de Goede, 255–74. Basingstoke: Palgrave MacMillan.
Amoore, Louise. 2006b. “Biometric Borders: Governing Mobilities in the War on Terror.” *Political Geography* 25 (3): 336–51. doi:10.1016/j.polgeo.2006.02.001.
Amoore, Louise. 2007. “Vigilant Visualities: The Watchful Politics of the War on Terror.” *Security Dialogue* 38 (2): 215–32. doi:10.1177/0967010607078526.
Amoore, Louise. 2009a. “Algorithmic War: Everyday Geographies of the War on Terror.” *Antipode* 41 (1). Blackwell Publishing Ltd: 49–69. doi:10.1111/j.1467-8330.2008.00655.x.
Amoore, Louise. 2009b. “Lines of Sight: on the Visualization of Unknown Futures.” *Citizenship Studies* 13 (1): 17–30. doi:10.1080/13621020802586628.
Amoore, Louise. 2011. “Data Derivatives: on the Emergence of a Security Risk Calculus for Our Times.” *Theory, Culture & Society* 28 (6): 24–43. doi:10.1177/0263276411417430.
Amoore, Louise. 2013. *The Politics of Possibility*. Durham; London: Duke University Press.
Amoore, Louise. 2014. “Security and the Claim to Privacy.” *International Political Sociology* 8 (1): 108–12.
Amoore, Louise, and Alexandra Hall. 2010. “Border Theatre: on the Arts of Security and Resistance.” *Cultural Geographies* 17 (3): 299–319. doi:10.1177/1474474010368604.
Amoore, Louise, and Marieke de Goede. 2005. “Governance, Risk and Dataveillance in the War on Terror.” *Crime, Law and Social Change* 43 (2–3): 149–73. doi:10.1007/s10611-005-1717-8.
Amoore, Louise, and Marieke de Goede. 2008a. “Introduction: Governing by Risk in the War on Terror.” In *Risk and the War on Terror*, 5–19. New York: Routledge.
Amoore, Louise, and Marieke de Goede. 2008b. “Transactions After 9/11: the Banal Face of the Preemptive Strike.” *Transactions of the Institute of British Geographers* 33 (2): 173–85.
Amoore, Louise, and Marieke de Goede, eds. 2008c. *Risk and the War on Terror*. New York: Routledge.
Amoore, Louise, and Rita Raley. 2017. “Securing with Algorithms: Knowledge, Decision, Sovereignty.” Edited by Louise Amoore and Rita Raley. *Security Dialogue* 48 (1): 1–8. doi:10.1177/0967010616680753.
Amoore, Louise, ed. 2005. *The Global Resistance Reader*. New York: Routledge.
Andersen, Rune Saugmann, Juha A Vuori, and Can E Mutlu. 2015. “Visuality.” In *Critical Security Methods: New Frameworks for Analysis*, edited by Claudia Aradau, Jef Huysmans, Andrew W Neal, and Nadine Voelkner, 85–117. London; New York: Routledge.

Anderson, Ben. 2010. “Security and the Future: Anticipating the Event of Terror.” *Geoforum* 41 (2): 227–35. doi:10.1016/j.geoforum.2009.11.002.
Anderson, Chris. 2008. “The End of Theory: The Data Deluge Makes the Scientific Method Obsolete.” *Wired*. June 23. https://www.wired.com/2008/06/pb-theory/.
Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence: University Press of Kansas.
Andrejevic, Mark. 2016. “The Pacification of Interactivity.” In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 187–206. Minneapolis: University of Minnesota Press.
Angelotti, Martina. 2015. “Secret Power.” *Domus*. May 15. http://www.domusweb.it/en/art/2015/05/15/simon_denny_secret_power.html.
Angwin, Julia, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras, and James Risen. 2015. “AT&T Helped U.S. Spy on Internet on a Vast Scale.” *The New York Times*. August 15. https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.
Antoniadis, Panayotis. 2016. “Local Networks for Local Interactions: Four Reasons Why and a Way Forward.” *First Monday* 21 (12): 150–65. doi:10.1016/j.comnet.2015.07.009.
Appelbaum, Jacob, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer, and Christian Stöcker. 2014. “Prying Eyes: Inside the NSA’s War on Internet Security.” *Spiegel Online*. December 28. http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.
Appelbaum, Jacob, and Laura Poitras. 2013. “Edward Snowden Interview: the NSA and Its Willing Helpers.” *Spiegel Online*. July 8. http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.
Appelbaum, Jacob, Judith Horchert, and Christian Stöcker. 2013. “Shopping for Spy Gear: Catalog Advertises NSA Toolbox.” *Spiegel Online*. December 29. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.
Apuzzo, Matt, Adam Goldman, and Linda Sarsour. 2013. “From Mosques to Soccer Leagues: Inside the NYPD’s Secret Spy Unit Targeting Muslims, Activists.” *Democracy Now*. September 17. http://www.democracynow.org/2013/9/17/from_mosques_to_soccer_leagues_inside.
Aradau, Claudia. 2004. “Security and the Democratic Scene: Desecuritization and Emancipation.” *Journal of International Relations and Development* 7 (4). Palgrave Macmillan UK: 388–413. doi:10.1057/palgrave.jird.1800030.
Aradau, Claudia. 2008. *Rethinking Trafficking in Women*. Palgrave Macmillan.
Aradau, Claudia. 2010. “Security That Matters: Critical Infrastructure and Objects of Protection.” *Security Dialogue* 41 (5): 491–514. doi:10.1177/0967010610382687.
Aradau, Claudia, and Rens Van Munster. 2007. “Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future.” *European Journal of International Relations* 13 (1): 89–115. doi:10.1177/1354066107074290.
Aradau, Claudia, and Rens Van Munster. 2008. “Taming the Future: the *Dispositif* Of Risk in the War on Terror.” In *Risk and the War on Terror*, edited by Louise Amoore and Marieke de Goede, 23–40. New York: Routledge.

Aradau, Claudia, and Tobias Blanke. 2015. “The (Big) Data-Security Assemblage: Knowledge and Critique.” *Big Data & Society* 2 (2): 1–12. doi:10.1177/2053951715609066.
Aradau, Claudia, and Tobias Blanke. 2017. “Governing Others: Anomaly and the Algorithmic Subject of Security.” *European Journal of International Security* 11 (October): 1–21. doi:10.1017/eis.2017.14.
Aradau, Claudia, Jef Huysmans, Andrew W Neal, and Nadine Voelkner. 2015. “Introducting Critical Security Methods.” In *Critical Security Methods: New Frameworks for Analysis*, edited by Claudia Aradau, Jef Huysmans, Andrew W Neal, and Nadine Voelkner, 1–22. London; New York: Routledge.
Art Hack Day. 2017. “Art Hack Day.” *Art Hack Day*. http://arthackday.net/.
Ashley, Richard K. 1986. “The Poverty of Neorealism.” In *Neorealism and Its Critics*, edited by Robert O Keohane, 255–300. New York: Columbia University Press.
Ashley, Richard K. 1988. “Untying the Sovereign State: a Double Reading of the Anarchy Problematique.” *Millennium-Journal of International Studies* 17 (2): 227–62.
Associated Press. 2014. “Everyone Is Under Surveillance Now, Says Whistleblower Edward Snowden.” *The Guardian*. May 3. http://www.theguardian.com/world/2014/may/03/everyone-is-under-surveillance-now-says-whistleblower-edward-snowden.
Azoulay, Ariella. 2011. “Getting Rid of the Distinction Between the Aesthetic and the Political.” *Theory, Culture & Society* 27 (7–8): 239–62. doi:10.1177/0263276410384750.
Baldwin, David A, ed. 1993. *Neorealism and Neoliberalism: the Contemporary Debate*. New York: Columbia University Press.
Ball, James. 2013. “Xbox Live Among Game Services Targeted by US and UK Spy Agencies.” *The Guardian*. December 9. http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.
Ball, James. 2014. “Angry Birds and ‘Leaky’ Phone Apps Targeted by NSA and GCHQ for User Data.” *The Guardian*. January 28. http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data.
Ball, James, Bruce Schneier, and Glenn Greenwald. 2013. “NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users.” *The Guardian*. October 4. http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.
Ball, James, Julian Borger, and Glenn Greenwald. 2013. “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security.” *The Guardian*. September 6. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
Ball, Kristie, Kevin D Haggerty, and David Lyon, eds. 2012. *The Routledge Handbook of Surveillance Studies*. New York: Routledge.
Balzacq, Thierry. 2005. “The Three Faces of Securitization: Political Agency, Audience and Context.” *European Journal of International Relations* 11 (2): 171–201. doi:10.1177/1354066105052960.
Bamford, James. 2012. “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say).” *Wired*. March 15. http://www.wired.com/2012/03/ff_nsadatacenter/all/.
Barnard-Wills, Katherine, and David Barnard-Wills. 2012. “Invisible Surveillance in Visual Art.” *Surveillance & Society* 10 (3/4): 204–14.
Barney, Darin, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck. 2016. “The Participatory Condition.” In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, vii—xxxix. An Introduction. Minneapolis: University of Minnesota Press.

Bartholl, Aram. 2014. “Killyourphone.com.” *Killyourphone.com*. http://killyourphone.com/.
Baudrillard, Jean. 1981. *Simulacres et Simulation*. Paris : Galilée.
Bauman, Zygmunt, and David Lyon. 2013. *Liquid Surveillance: A Conversation*. Cambridge; Malden, MA: Polity.
Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R B J Walker. 2014. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8 (2): 121–44. doi:10.1111/ips.12048.
Beck, Ulrich. 2009. *World at Risk*. Translated by Ciaran Cronin. Malden, MA: Polity.
Bell, Colleen. 2012. “Hybrid Warfare and Its Metaphors.” *Humanity: an International Journal of Human Rights, Humanitarianism, and Development* 3 (2): 225–47. doi:10.1353/hum.2012.0014.
Bell, Colleen. 2015. “The Police Power in Counterinsurgencies: Discretion, Patrolling and Evidence.” In *War, Police and Assemblages of Intervention*, edited by Jan Bachman, Colleen Bell, and Caroline Holmqvist, 17–35. London.
Bellanova, Rocco, and Gloria González Fuster. 2013. “Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices.” *International Political Sociology* 7 (2): 188–209. doi:10.1111/ips.12017.
Biermann, Kai. 2011. “Data Protection: Betrayed by Our Own Data.” *Zeit Online*. March 10. http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.
Big Brother Awards, Privacy International. 2017. “Big Brother Awards International.” *Big Brother Awards*. http://www.bigbrotherawards.org/.
Bigo, Didier. 1998. “Sécurité et Immigration : Vers une gouvernementalité par l’inquiétude ?” *Cultures & Conflits* 31-32 : 1–17.
Bigo, Didier. 2005. “La mondialisation de l’(in)sécurité ?” *Cultures & Conflits*, no. 58. Centre d’études sur les conflits : 53–101.
Bigo, Didier. 2016. “The Möbius Strip of National and World Security.” *Mapping Security*. June 21. doi:10.1111/ips.12048/abstract.
Bilal, Wafaa. 2014. “Wafaa Bilal.” *Wafaabilal.com*. http://wafaabilal.com/#&panel1-3.
Bishop, Ryan. 2012. “Project ‘Transparent Earth’ and the Autoscopy of Aerial Targeting: The Visual Geopolitics of the Underground.” *Theory, Culture & Society* 28 (7–8): 270–86. doi:10.1177/0263276411424918.
Blas, Zach. 2014. “Facial Weaponization Suite.” *Zach Blas*. Accessed July 8. http://www.zachblas.info/projects/facial-weaponization-suite/.
Blast Theory. 2018. “Karen.” *Blast Theory*. https://www.blasttheory.co.uk/projects/karen/.
Bleiker, Roland. 2000. *Popular Dissent, Human Agency, and Global Politics*. Cambridge, New York: Cambridge University Press.
Bleiker, Roland. 2001. “The Aesthetic Turn in International Political Theory.” *Millennium-Journal of International Studies* 30 (3): 509–33.
Bleiker, Roland. 2009. *Aesthetics and World Politics*. Houndsmills, Basingstoke, New York: Palgrave Macmillan.
Bloomberg. 2017. “Qwest Corp.: Private Company Information.” *Bloomberg.com*. July 18. https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=3028457.
Blum, Andrew. 2012. *Tubes*. Toronto: HarperCollins.
Boltanski, Luc, Elisabeth Claverie, Nicolas Offenstadt, and Stéphane Van Damme, eds. 2007. *Affaires, Scandales et Grandes Causes*. Paris : Stock.
Booth, Ken. 1991. “Security and Emancipation.” *Review of International Studies* 17 (4). JSTOR: 313–26.

Booth, Ken, ed. 2005. *Critical Security Studies and World Politics*. Boulder: Lynne Rienner.
Borger, Julian. 2013. "NSA Files: Why the Guardian in London Destroyed Hard Drives of Leaked Files." *The Guardian*. August 20. http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.
Bourdieu, Pierre. 1987. "The Historical Genesis of a Pure Aesthetic." *The Journal of Aesthetics and Art Criticism* 46: 201—10.
Bourdieu, Pierre. 2002. *Questions de Sociologie*. Paris : Les Éditions de Minuit.
Bourque, Brad. 2016. "MIT's Newest Quantum Computer Puts Us One Step Closer to Defeating Modern Encryption." *Digital Trends*. March 8. https://www.digitaltrends.com/computing/mit-five-atom-quantum-rsa/.
Brandis, Lucas. 1475a. "Rudimentum Novitiorum." *Lübeck Stadtbibliothek*. Lukas Brandis (Drucker). http://digital.stadtbibliothek.luebeck.de/viewer/resolver?urn=urn:nbn:de:gbv:48-1-83070.
Brandis, Lucas. 1475b. "Rudimentum Novitorum." *Rudimentum Noviciorum Sive Chronicarum Et Historiarum Epitome*. Lübeck. https://commons.wikimedia.org/wiki/File:1475_Rudimentum_Novitorum_Lucas_brandis.jpg .
Bridle, James. 2012. "#Sxaesthetic." *Booktwo.org*. March 15. http://booktwo.org/notebook/sxaesthetic/.
Bridle, James. 2013. "The New Aesthetic and Its Politics." *Booktwo.org*. June 12. http://booktwo.org/notebook/new-aesthetic-politics/.
Bridle, James. 2015a. ".Cymru." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015b. ".Io." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015c. ".Ly." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015d. ".Scot." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015e. "Algorithmic Citizenship." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015f. "Citizen Ex." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2015g. "Five Eyes / Hyperstacks." *Jamesbridle.com*. http://jamesbridle.com/works/five-eyes-hyperstacks.
Bridle, James. 2015h. "Stories." *Citizen Ex*. http://citizen-ex.com/.
Bridle, James. 2018. "About." *Jamesbridle.com*. http://jamesbridle.com/about.
Bridle, James. 2017. "Algorithmic Citizenship." *Exposingtheinvisible.org*. Accessed July 6. http://exposingtheinvisible.org/films/algorithmic-citizenship/.
Brighenti, Andrea Mubi. 2010a. "Artveillance: at the Crossroads of Art and Surveillance." *Surveillance & Society* 7 (2): 175–86.
Brighenti, Andrea Mubi. 2010b. "Democracy and its Visibilities." In *Surveillance and Democracy*, edited by Kevin D Haggerty and Minas Samatas, 51–68. New York: Routledge-Cavendish.
Brown, Melissa, Rashawn Ray, Ed Summers, and Neil Fraistat. 2016. "#SayHerName: A Case Study of Intersectional Social Media Activism." *Ethnic and Racial Studies* 40 (11). Taylor & Francis: 1831–46. doi:10.1080/01419870.2017.1334934.
Brown, Wendy. 2010. *Walled States, Waning Sovereignty*. Cambridge, MA: MIT Press.
Brucker-Cohen, Jonah. 2014. "Welcome to Your New NSA Partner Network: Report from Transmediale 2014." *Rhizome*. February 6. http://rhizome.org/editorial/2014/feb/6/report-transmediale-2014/.
Brucker-Cohen, Jonah. 2016. "Jonah Brucker-Cohen, PH.D." *Coin-Operated.com*. Accessed June 22. http://www.coin-operated.com/2016/04/04/lively-2016/.

Burke, Anthony. 2002. “Aporias of Security.” *Alternatives* 27 (1): 1–27.
Burke, Penny Jane, and Jackie McManus. 2011. “Art for a Few: Exclusions and Misrecognitions in Higher Education Admissions Practices.” *Discourse: Studies in the Cultural Politics of Education* 32 (5): 699–712. doi:10.1080/01596306.2011.620753.
Burke, Redmond A. 1982. “Review: Bessarion’s Library and the Biblioteca Marciana: Six Early Inventories by Lotte Labowsky.” *The Library Quarterly Information, Community, Policy* 52 (2): 163–65.
Burrington, Ingrid. 2014a. “Submarine Cable Taps.” *Lifewinning.com*. http://lifewinning.com/projects/submarine-cable-taps/.
Burrington, Ingrid. 2014b. “The Cloud Is Not the Territory.” *Creative Time Reports*. May 20. http://creativetimereports.org/2014/05/20/ingrid-burrington-the-cloud-is-not-the-territory-wnv/.
Burrington, Ingrid. 2017. “Seeing Networks.” *Seeingnetworks.in*. Accessed June 26. http://seeingnetworks.in/.
Burrington, Ingrid, and Meredith Whittaker. 2016. “The Realm of Rough Telepathy.” *Grimoire.computer*. Accessed June 20. http://grimoire.computer/.
Burtch, Allison. 2015. “Allison Burtch.” *Allisonburtch.Net*. Accessed November 5. http://www.allisonburtch.net/.
Buzan, Barry. 1991. *People, States and Fear: An Agenda for International Security Studies in Post-Cold War Era*. 2nd ed. Boulder: Lynne Rienner.
Buzan, Barry, and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.
Buzan, Barry, David Held, and Anthony McGrew. 1998. “Realism vs Cosmopolitanism.” *Review of International Studies* 24: 387—98.
Buzan, Barry, Ole Waever, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.
Cahill, Susan. 2018. “Art and Surveillance.” *Art and Surveillance*. http://www.artandsurveillance.com/.
Cammaerts, Bart. 2016. “Internet-Mediated Mutual Cooperation Practices.” In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 145–66. The Sharing of Material and Immaterial Resources. Minneapolis: University of Minnesota Press.
Campbell, David. 1998. *Writing Security: United States Foreign Policy and the Politics of Identity*. Rev. Ed. Minneapolis: University of Minnesota Press.
Campbell, David. 2003. “Cultural Governance and Pictorial Resistance: Reflections on the Imaging of War.” *Review of International Studies* 29 (S1).
Campbell, David. 2013. “Poststructuralism.” In *International Relations Theories: Discipline and Diversity, Third Edition*, edited by Tim Dunne, Milja Kurki, and Steve Smith, 223–46. Oxford: Oxford University Press.
Campbell, David, and Michael J Shapiro. 2007. “Guest Editors’ Introduction.” *Security Dialogue* 38 (2): 131–37. doi:10.1177/0967010607080596.
Canadian Journalists for Free Expression, Politics of Surveillance Project. 2018. “Snowden Surveillance Archive.” *Snowdenarchive.Cjfe.org*. Accessed February 9. https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi.
Caquard, Sébastien. 2011. “Cartography I: Mapping Narrative Cartography.” *Progress in Human Geography* 37 (1): 135–44. doi:10.1177/0309132511423796.
Carrillo, Jesus, and Hans Haacke. 2006. “Hans Haacke.” *REvista*, no. 2: 1–3.

Carter, Sean, and Derek P McCormack. 2006. “Film, Geopolitics and the Affective Logics of Intervention.” *Political Geography* 25 (2): 228–45. doi:10.1016/j.polgeo.2005.11.004.
Carter, Sean, and Derek P McCormack. 2010. “Affectivity and Geopolitical Images.” In *Observant States: Geopolitics and Visual Culture*, edited by Fraser MacDonald, Rachel Hughes, and Klaus Dodds, 103–22. London: I.B. Tauris.
Carter, Sean, and Klaus Dodds. 2011. “Hollywood and the ‘War on Terror’: Genre-Geopolitics and “Jacksonianism” in the Kingdom.” *Environment and Planning D: Society and Space* 29 (1): 98–113. doi:10.1068/d7609.
CASE Collective. 2006. “Critical Approaches to Security in Europe: A Networked Manifesto.” *Security Dialogue* 37 (4): 443–87. doi:10.1177/0967010606073085.
Caso, Federica, and Caitlin Hamilton, eds. 2015. *Popular Culture and World Politics*. Bristol: E-International Relations.
Chamayou, Grégoire. 2013. *Théorie du Drone*. Paris : La fabrique.
Chambers, Samuel A. 2009. “A Queer Politics of the Democratic Miscount.” *Borderlands* 8 (2): 1–23.
Chan, Stephen, Peter Mandaville, and Roland Bleiker, eds. 2001. *The Zen of International Relations Theory: IR Theory from East to West*. Houndmills: Palgrave Macmillan.
Cheney-Lippold, John. 2011. “A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control.” *Theory, Culture & Society* 28 (6): 164–81. doi:10.1177/0263276411424420.
Cheney-Lippold, John. 2016. “Jus Algoritmi: How the National Security Agency Remade Citizenship.” *International Journal of Communication* 10: 1721—42.
Cheney-Lippold, John. 2017a. *We Are Data*. New York: New York University Press.
Cheney-Lippold, John. 2017b. “Who We Are as Data Might Soon Become More Important Than Who We Are as People.” *Quartz*. May 4. https://qz.com/975231/google-and-the-nsa-probably-dont-think-youre-the-age-gender-or-nationality-you-really-are-and-thats-dangerous/.
Chernega, Jennifer. 2016. “Black Lives Matter: Racialised Policing in the United States.” *Comparative American Studies an International Journal* 14 (3–4). Routledge: 234–45. doi:10.1080/14775700.2016.1267322.
Christl, Wolfie. 2017. *Corporate Surveillance in Everyday Life*. Vienna: Cracked Labs.
Churchill, Ward. 1998. *Pacifism as Pathology: Reflections on the Role of Armed Struggle in North America*. Oakland, CA: AK Press.
Cinnamon, Jonathan. 2017. “Social Injustice in Surveillance Capitalism.” *Surveillance & Society* 15 (5): 609–25.
Cirio, Paolo. 2015. “Overexposed—HD Stencils.” *Paolocirio.Net*. Accessed August 25. http://paolocirio.net/work/hd-stencils/overexposed/.
Clapper, James R. 2009. *Cryptological School Course on Legal Compliance and Minimization Procedures*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH26d3/53b51a5c.dir/doc.pdf.
Clarke, Richard A, Michael J Morell, Geoffrey R Stone, Cass R Sunstein, and Peter Swire. 2013. *Liberty and Security in a Changing World*. Washington, DC. https://www.nsa.gov/about/civil-liberties/resources/assets/files/liberty_security_prgfinalreport.pdf.
Clement, Andrew, and Jonathan A Obar. 2015. *Keeping Internet Users in the Know or in the Dark*. IXmaps.ca & New Transparency Projects. https://www.ixmaps.ca/docs/DataPrivacyTransparencyofCanadianCarriers-2014.pdf.

Click. 2015. “The Art of Uncovering the USA’s Surveillance Culture.” *BBC World Service*.
Coaffee, Jon, Paul O’Hare, and Marian Hawkesworth. 2009. “The Visibility of (in)Security: The Aesthetics of Planning Urban Defences Against Terrorism.” *Security Dialogue* 40 (4–5): 489–511. doi:10.1177/0967010609343299.
Cockayne, James, and Adam Lupel. 2009. “Introduction: Rethinking the Relationship Between Peace Operations and Organized Crime.” *International Peacekeeping* 16 (1): 4–19. doi:10.1080/13533310802485567.
Cohen, Julie E. 2016. “The Surveillance-Innovation Complex.” In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 207–26. The Irony of the Participatory Turn. Minneapolis: University of Minnesota Press.
Cohen, Stanley. 1985. *Visions of Social Control: Crime, Punishment and Classification*. Cambridge: Polity Press.
Collier, Stephen J, and Andrew Lakoff. 2007. “Distributed Preparedness: Space, Security, and Citizenship in the United States.” In *War, Citizenship, Territory*, edited by Deborah Cowen and Emily Gilbert, 119–43. New York: Routledge.
Connolly, William. 1989. “Identity and Difference in Global Politics.” In *International/Intertextual Relations: Postmodern Readings of World Politics*, edited by James Der Derian and Michael J Shapiro, 323–343. New York: Lexington Books.
Contorno, Steve. 2014. “James Clapper’s Testimony One Year Later.” *PolitiFact*. March 11. http://www.politifact.com/truth-o-meter/article/2014/mar/11/james-clappers-testimony-one-year-later/.
Corry, Olaf. 2014. “From Defense to Resilience: Environmental Security Beyond Neo-Liberalism.” *International Political Sociology* 8 (3): 256–74. doi:10.1111/ips.12057.
Couldry, Nick. 2004. “Theorising Media as Practice.” *Social Semiotics* 14 (2): 115–32. doi:10.1080/1035033042000238295.
Coupe, James. 2017. “Watchtower (a Machine for Living).” *Jamescoupe.com*. http://jamescoupe.com/?p=2339.
Coward, Martin. 2009. “Network-Centric Violence, Critical Infrastructure and the Urbanization of Security.” *Security Dialogue* 40 (4–5): 399–418. doi:10.1177/0967010609342879.
Cowen, Deborah. 2010. “A Geography of Logistics: Market Authority and the Security of Supply Chains.” *Annals of the Association of American Geographers* 100 (3): 600–620.
Cox, Joseph. 2015. “This Database Gathers the Resumes of 27,000 Intelligence Workers.” *Motherboard*. May 7. http://motherboard.vice.com/read/this-database-gathers-the-resumes-of-27000-intelligence-workers?utm_source=mbfb.
Cox, Robert W. 1983. “Gramsci, Hegemony and International Relations: an Essay in Method.” *Millennium-Journal of International Studies* 12 (2): 162–75.
Crampton, Andrew, and Marcus Power. 2005. “Frames of Reference on the Geopolitical Stage: Saving Private Ryan and the Second World War/Second Gulf War Intertext.” *Geopolitics* 10 (2): 244–65. doi:10.1080/14650040590946575.
Crang, Mike, and Stephen Graham. 2007. “SENTIENT CITIES Ambient Intelligence and the Politics of Urban Space.” *Information, Communication & Society* 10 (6): 789–817. doi:10.1080/13691180701750991.
Cullen, Catherine, and Brigitte Bureau. 2017. “Someone Is Spying on Cellphones in the Nation’s Capital.” *CBC News*. April 3. http://www.cbc.ca/beta/news/politics/imsi-cellphones-spying-ottawa-1.4050049.

Currier, Cora, and Murtaza Hussain. 2017. “48 Questions the FBI Uses to Determine if Someone Is a Likely Terrorist.” *The Intercept*. February 13. https://theintercept.com/2017/02/13/48-questions-the-fbi-uses-to-determine-if-someone-is-a-likely-terrorist/.
Currier, Cora, and Peter Maass. 2015. “Firing Blind: Flawed Intelligence and the Limits of Drone Technology.” *The Intercept*. October 15. https://theintercept.com/drone-papers/firing-blind/.
D’Aoust, Anne-Marie. 2013. “In the Name of Love: Marriage Migration, Governmentality, and Technologies of Love.” *International Political Sociology* 7 (3). The Oxford University Press: 258–74. doi:10.1111/ips.12022.
da Costa, Beatriz, Jamie Schulte, and Brooke Singer. 2015. “Preemptive Media.” *Preemptivemedia.Net*. Accessed October 28. http://www.preemptivemedia.net/.
Dalby, Simon. 2002. *Environmental Security*. Minneapolis: University of Minnesota Press.
Danchev, Alex. 2009. *On Art and War on Terror*. Edinburgh: Edinburgh University Press.
Danchev, Alex, and Debbie Lisle. 2009. “Introduction: Art, Politics, Purpose.” *Review of International Studies* 35 (04): 775–79. doi:10.1017/S0260210509990179.
de Blic, Damien, and Cyril Lemieux. 2005. “Le Scandale comme Épreuve.” *Politix* 71 (3): 9–38. doi:10.3917/pox.071.0009.
de Goede, Marieke. 2005. “Carnival of Money: Politics of Dissent in an Era of Globalizing Finance.” In *The Global Resistance Reader*, edited by Louise Amoore, 379–91. New York: Routledge.
de Goede, Marieke. 2008a. “Risk, Preemption and Exception in the War on Terrorist Financing.” In *Risk and the War on Terror*, edited by Louise Amoore and Marieke de Goede, 97–111. New York: Routledge.
de Goede, Marieke. 2008b. “Beyond Risk: Premediation and the Post-9/11 Security Imagination.” *Security Dialogue* 39 (2–3): 155–76. doi:10.1177/0967010608088773.
de Goede, Marieke. 2012. *Speculative Security*. Minneapolis: University of Minnesota Press.
de Goede, Marieke. 2014. “The Politics of Privacy in the Age of Preemptive Security.” *International Political Sociology* 8 (1). Oxford University Press: 100–104. doi:10.1111/ips.12042.
de Tocqueville, Alexis. 1967. *L’ancien Régime et La Révolution*. Edited by JP Mayer. Paris : Gallimard.
DE-CIX. 2017. “Frankfurt— DE-CIX.” *De-Cix.Net*. https://www.de-cix.net/en/locations/germany/frankfurt.
Dean, Mitchell. 2010. *Governmentality*. Second Edition. London: SAGE Publications.
Death, Carl. 2010. “Counter-Conducts: a Foucauldian Analytics of Protest.” *Social Movement Studies* 9 (3): 235–51. doi:10.1080/14742837.2010.493655.
Debord, Guy. 1996. *La Société du Spectacle*. Paris : Gallimard.
Deleuze, Gilles. 1990. “Post-scriptum sur les sociétés de contrôle.” *L’autre Journal*, no. 1 (Mai). http://infokiosques.net/spip.php?article214.
Denny, Simon. 2015. *Secret Power*. *Biennale de Venise*. https://marciana.venezia.sbn.it/sites/default/files/dscf0351.jpg.
Der Derian, James. 1987. *On Diplomacy: A Genealogy of Western Estrangement*. Oxford; New York: Blackwell.
Der Derian, James. 2009. *Virtuous War: Mapping the Military-Industrial Media-Entertainment Network*. Second Edition. New York: Routledge.
Der Derian, James, and Michael J Shapiro, eds. 1989. *International/Intertextual Relations: Postmodern Readings of World Politics*. New York: Lexington Books.

Derr, Robert Ladislas. 2010. “Artist, Robert Ladislas Derr Uses Die Rolls and Cameras to Map His Walk Through Cities Worldwide.” Edited by A L Foglesong. *Surveillance & Society* 7 (2): 94–987.
Devereaux, Ryan, Glenn Greenwald, and Laura Poitras. 2014. “Data Pirates of the Caribbean: the NSA Is Recording Every Cell Phone Call in the Bahamas.” *The Intercept*. May 19. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.
Devetak, Richard. 2005. “The Gothic Scene of International Relations: Ghosts, Monsters, Terror and the Sublime After September 11.” *Review of International Studies* 31 (4): 621–43. doi:10.1017/S0260210505006662.
Dewey-Hagborg, Heather. 2015. “Heather Dewey-Hagborg.” *Deweyhagborg.com*. Accessed October 28. http://deweyhagborg.com/.
Digitalcourage. 2018. “What Are the Big Brother Awards?.” *BigBrotherAwards*. https://bigbrotherawards.de/en.
Dillon, Michael, and Andrew W Neal, eds. 2011. *Foucault on Politics, Security and War*. Palgrave Macmillan.
Dillon, Michael, and Julian Reid. 2001. “Global Liberal Governance: Biopolitics, Security and War.” *Millennium-Journal of International Studies* 30 (1). SAGE Publications: 41–66.
Dingwerth, Klaus, and Philipp Pattberg. 2006. “Global Governance as a Perspective on World Politics.” *Global Governance: A Review of Multilateralism and International Organizations* 12 (2). Lynne Rienner Publishers: 185–203.
Dittmer, Jason. 2011. “American Exceptionalism, Visual Effects, and the Post-9/11 Cinematic Superhero Boom.” *Environment and Planning D: Society and Space* 29 (1): 114–30. doi:10.1068/d4309.
Dodds, Klaus. 2015. “Popular Geopolitics and War on Terror.” In *Popular Culture and World Politics: Theories, Methods, Pedagogies*, edited by Federica Caso and Caitlin Hamilton, 51–62. Bristol: E-International Relations Publishing.
Doucet, Marc G. 2005. “Child’s Play: The Political Imaginary of International Relations and Contemporary Popular Children’s Films.” *Global Society* 19 (3): 289–306.
Duffield, Mark. 2010a. “The Liberal Way of Development and the Development—Security Impasse: Exploring the Global Life-Chance Divide.” *Security Dialogue* 41 (1): 53–76. doi:10.1177/0967010609357042.
Duffield, Mark. 2010b. “Risk-Management and the Fortified Aid Compound: Everyday Life in Post-Interventionary Society.” *Journal of Intervention and Statebuilding* 4 (4): 453–74. doi:10.1080/17502971003700993.
Dullaart, Constant. 2015a. “Constant Dullaart: 100,000 Followers for Everyone!” *Dismagazine.com*. Accessed October 30. http://dismagazine.com/dystopia/67039/constant-dullaart-100000-followers-for-everyone/.
Dullaart, Constant. 2015b. “✻✻✩✩.” *Constantdullaart.com*. Accessed October 30. http://constantdullaart.com/%E2%9D%8C%E2%9D%8C%E2%8C%98%E2%9B%94%E2%8F%B3%E2%9D%8C%E2%8C%BD%E2%8C%BD%F0%9F%90%92%E2%9A%AB%E2%9D%8C%E2%8C%98%F0%9F%94%8D%E2%9C%A8%E2%98%A0%E2%9C%8A%F0%9F%90%8D%20%E2%9C%8B%F0%9F%93%B1%F0%9F%90%87%E2%96%91%E2%9

C%93%E2%96%91%E2%96%91%E2%9C%A8%E2%9A%AB%E2%9D%8C%E2%9D%8C%E2%8C%98%E2%8F%8F%E2%9C%8A%F0%9F%90%80%E2%9C%93%E2%99%AA%E2%8C%AB/.
Duncombe, Constance, and Roland Bleiker. 2015. "Popular Culture and Political Identity." In *Popular Culture and World Politics: Theories, Methods, Pedagogies*, edited by Federica Caso and Caitlin Hamilton, 35–44. Bristol: E-International Relations Publishing.
Dunn Cavelty, Myriam, Mareile Kaufmann, and Kristian Soby Kristensen. 2015. "Resilience and (in)Security: Practices, Subjects, Temporalities." *Security Dialogue* 46 (1): 3–14. doi:10.1177/0967010614559637.
Easterling, Keller. 2016. *Extrastatecraft*. London: Verso.
Edith-Russ-Haus for Media Art. 2015. "Edith-Russ-Haus for Media Art—Trevor Paglen and Jacob Appelbaum: *Autonomy Cube*." *E-Flux*. October 20. http://www.e-flux.com/announcements/2916/trevor-paglen-and-jacob-appelbaumautonomy-cube/.
Edkins, Jenny, and Adrian Kear. 2013. "Introduction." In *International Politics and Performance: Critical Aesthetics and Creative Practice*, edited by Jenny Edkins and Adrian Kear. London; New York: Routledge.
Edkins, Jenny, Véronique Pin-Fat, and Michael J Shapiro, eds. 2004. *Sovereign Lives: Power in Global Politics*. New York: Routledge.
Edwards, Phil. 2015. "A Map of All the Underwater Cables That Connect the Internet." *Vox.com*. March 13. http://www.vox.com/2015/3/13/8204655/submarine-cables-internet.
EFF. 2012. "Word Games." *Electronic Frontier Foundation*. December 3. https://www.eff.org/fr/nsa-spying/wordgames.
EFF. 2017a. "HTTPS Everywhere." *Electronic Frontier Foundation*. https://www.eff.org/https-everywhere.
EFF. 2017b. "How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy." *Electronic Frontier Foundation*. June 8. https://www.eff.org/pages/tor-and-https.
Elahi, Hasan. 2013. "Trackingtransience.Net." *Trackingtransience.Net*. Accessed November 14. http://trackingtransience.net/.
Elbe, Stefan. 2005. "Sida, Un Enjeu Global de Sécurité." *Politique étrangère*, no. 1. IFRI : 163–75.
Ellerbrok, Ariane. 2010. "Empowerment: Analyzing Technologies of Multiple Variable Visibility." *Surveillance & Society* 8 (2): 200–220.
Ellerbrok, Ariane. 2011. "PLAYFUL BIOMETRICS: Controversial Technology Through the Lens of Play." *The Sociological Quarterly* 52 (4): 528–47.
Enloe, Cynthia. 1990. *Bananas, Beaches and Bases: Making Feminist Sense of International Relations*. Berkeley/Los Angeles: University of California Press.
Enloe, Cynthia. 2004. "Margins, Silences, and Bottom Rungs: How to Overcome the Underestimation of Power of Study of International Relations." In *The Curious Feminist: Searching for Women in a New Age of Empire*. Berkeley: University of California Press.
Ericson, Richard V. 2006. *Crime in an Insecure World*. Cambridge: Polity Press.
Eriksson, Johan. 1999. "Observers or Advocates? On the Political Role of Security Analysts." *Cooperation and Conflict* 34 (3): 311–30.
Eriksson, Magnus, and Evan Roth. 2015. "We Lost." *F.a.T. Free Art & Technology*. August 1. http://fffff.at/we-lost/.
Eyebeam. 2013. "PRISM Breakup." *PRISM Breakup*. October 4. http://prismbreakup.org/.
Falchetta, Piero. 2006. "Fra Mauro Map." *The Fra Mauro Map*. https://commons.wikimedia.org/wiki/File:FraMauroDetailedMap.jpg.

Fastly. 2017a. “Customers Stories.” *Fastly*. https://www.fastly.com/customers/.
Fastly. 2017b. “Network Map.” *Fastly*. https://www.fastly.com/network-map/.
Feenberg, Andrew. 1999. *Questioning Technology*. New York; London: Routledge.
Feinstein, Dianne. 2013. “Sen. Dianne Feinstein: Continue NSA Call-Records Program.” *USA Today*. October 20. http://www.usatoday.com/story/opinion/2013/10/20/nsa-call-records-program-sen-dianne-feinstein-editorials-debates/3112715/.
Ferguson, James. 2005. “Seeing Like an Oil Company: Space, Security, and Global Capital in Neoliberal Africa.” *American Anthropologist* 107 (3): 377–82.
Ferguson, Kennan. 1996. “Unmapping and Remapping the World: Foreign Policy as Aesthetic Practice.” In *Challenging Boundaries: Global Flows, Territorial Identities*, edited by Michael J Shapiro and Hayward R Alker, 165–91. Minneapolis: University of Minnesota Press.
Fisher, Jill A, and Torin Monahan. 2011. “The ‘Biosecuritization’ of Health Delivery: Examples of Post-9/11 Technological Imperatives.” *Social Science & Medicine* 72 (4): 545–52. doi:10.1016/j.socscimed.2010.11.017.
Foucault, Michel. 1975. *Surveiller et punir. Naissance de lapPrison*. Paris : Éditions Gallimard.
Foucault, Michel. 1976. *Histoire de la sexualité I. La volonté de savoir*. Paris : Éditions Gallimard.
Foucault, Michel. 1991. “Questions of Method.” In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 73–86. Chicago: University of Chicago Press.
Foucault, Michel. 1994a. “Est-il donc important de penser ?” In *Dits et Écrits, 1954–1988*, edited by Daniel Defert, François Ewald, and Jacques Lagrange. Paris : Gallimard.
Foucault, Michel. 1994b. “Qu’est-ce que les Lumières ?” In *Dits et Écrits, 1954–1988*, edited by Daniel Defert, François Ewald, and Jacques Lagrange, 562–78. Paris.
Foucault, Michel. 1997. *Il faut défendre la société. Cours au Collège de France (1976)*. Edited by François Ewald and Alessandro Fontana. Paris : Seuil/Gallimard.
Foucault, Michel. 2004a. *Naissance de la biopolitique. Cours au Collège de France (1978-1979)*. Paris : Seuil/Gallimard.
Foucault, Michel. 2004b. *Sécurité, Territoire, Population. Cours au Collège de France (1977-1978)*. Paris : Seuil/Gallimard.
freifunk.net, freifunk. 2018. “Freifunk.Net.” *Freifunk.Net*. https://freifunk.net/en/.
Froomkin, Dan. 2017. “NSA Backs Down on Major Surveillance Program That Captured Americans’ Communications Without a Warrant.” *The Intercept*. April 28. https://theintercept.com/2017/04/28/nsa-backs-down-on-major-surveillance-program-that-captured-americans-communications-without-a-warrant/.
Frost, Lola. 2010. “Aesthetics and Politics.” *Global Society* 24 (3): 433–43. doi:10.1080/13600826.2010.485560.
Fuller, Gillian. 2003. “Life in Transit: Between Airport and Camp.” *Borderlands* 2 (1).
Gal, Noam, Limor Shifman, and Zohar Kampf. 2016. “‘It Gets Better’: Internet Memes and the Construction of Collective Identity.” *New Media & Society* 18 (8): 1698–1714. doi:10.1177/1461444814568784.
Gallagher, Ryan. 2014. “Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide.” *The Intercept*. December 4. https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/.
Gallagher, Ryan. 2015a. “Inside the Secret World of NSA Art.” *The Intercept*. June 11. https://firstlook.org/theintercept/2015/06/11/secret-power-nsa-darchicourt-art-denny/.

Gallagher, Ryan. 2015b. “The Life and Death of Objective Peckham.” *The Intercept*. October 15. https://theintercept.com/drone-papers/the-life-and-death-of-objective-peckham/.
Galland, Jean-Pierre. 2010. “Critique de La Notion D’infrastructure Critique.” *Flux*, no. 81 (November) : 6–18.
Gandy, Oscar H, Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.
Gandy, Oscar H, Jr. 2012. “Statistical Surveillance.” In *The Routledge Handbook of Surveillance Studies*, edited by Kristie Ball, Kevin D Haggerty, and David Lyon, 125–32. Remote Sensing in the Digital Age. New York.
Gansing, Kristoffer, Daphne Dragona, Inga Seidler, and Florian Wüst. 2018. “Face Value | Transmediale Festival 2018.” *Transmediale*. Accessed March 2. https://2018.transmediale.de/program/text/face-value.
Garcia Martinez, Antonio. 2017. “Inside Cuba’s DIY Internet Revolution.” *Wired*. July 26. https://www.wired.com/2017/07/inside-cubas-diy-internet-revolution/.
Garcia, Pablo. 2015. “Pablo Garcia.” *Pablogarcia.org*. Accessed October 29. http://pablogarcia.org/.
Garrett, Marc. 2016. “Transmediale 2016: Necessary Conversations Off-the-Cloud.” *Furtherfield*. February 28. http://www.furtherfield.org/features/review-transmediale-2016-necessary-conversations.
Gat, Orit. 2015. “Global Audiences, Zero Visitors: How to Measure the Success of Museums’ Online Publishing.” *Rhizome*. March 12. http://rhizome.org/editorial/2015/mar/12/global-audiences-zero-visitors/?ref=nwslettr.
GCHQ. 2012. *Tempora*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH09dc.dir/doc.pdf.
Gellman, Barton. 2013. “Edward Snowden, After Months of NSA Revelations, Says His Mission’s Accomplished.” *The Washington Post*. December 23. https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html?utm_term=.c9a6e147903e.
Gellman, Barton, and Ashkan Soltani. 2013a. “NSA Collects Millions of E-Mail Address Books Globally.” *The Washington Post*. October 14. http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.
Gellman, Barton, and Ashkan Soltani. 2013b. “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.” *The Washington Post*. October 30. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
Gellman, Barton, and Ashkan Soltani. 2013c. “NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show.” *The Washington Post*. December 4. http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.
Gellman, Barton, and Ashkan Soltani. 2014. “NSA Surveillance Program Reaches ‘Into the Past’ to Retrieve, Replay Phone Calls.” *The Washington Post*. March 18. http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-

into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.
Gellman, Barton, and Laura Poitras. 2013. "U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post*. June 6. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.
George, Jim, and David Campbell. 1990. "Patterns of Dissent and the Celebration of Difference: Critical Social Theory and International Relations." *International Studies Quarterly* 34 (3): 269–93.
Giddens, Anthony. 1991. "The Self: Ontological Security and Existential Anxiety." In *Modernity and Self-Identity: Self and Society in Late Modern Age*. Cambridge: Polity Press.
Gill, Stephen. 2002. "Constitutionalizing Inequality and the Clash of Globalizations." *International Studies Review* 4 (2): 47–65.
Gillespie, Katherine. 2017. "This AI Creates Art from Instagram Posts with Zero Likes." *Vice*. May 10. https://creators.vice.com/en_au/article/z4jz3x/this-ai-creates-art-from-instagram-posts-with-zero-likes.
Gilliom, John, and Torin Monahan. 2013. *SuperVision*. Chicago: University of Chicago Press.
Goehr, Lydia. 2003. "Art and Politics." In *The Oxford Handbook of Aesthetics*, edited by Jerrold Levinson, 471–85. Oxford: Oxford University Press.
Goldman, Adam, and Matt Apuzzo. 2012. "NYPD Built Secret Files on Mosques Outside NY." *Associated Press*. February 22. http://www.ap.org/Content/AP-In-The-News/2012/NYPD-built-secret-files-on-mosques-outside-NY.
Gow, Andrew. 2007. "Review: Fra Mauro's World Map with a Commentary and Translations of the Inscriptions by Piero Falchetta and Marino Zorzi." *Imago Mundi* 59 (2): 235–36.
Gracyk, Theodore. 2013. "Adorno." In *The Routledge Companion to Aesthetics*, edited by Berys Gaut and Dominic McIver Lopes, Third Edition, 137–47. New York: Routledge.
Graeber, David. 2013. *The Democracy Project: A History, a Crisis, a Movement*. New York: Spiegel & Grau.
Graham, Gordon. 2005. *Philosophy of the Arts: An Introduction to Aesthetics*. Third Edition. London; New York: Routledge.
Graham, Stephen. 2009. "Cities as Battlespace: The New Military Urbanism." *City* 13 (4): 383–402. doi:10.1080/13604810903298425.
Grayson, Kyle, Matt Davies, and Simon Philpott. 2009. "Pop Goes IR? Researching the Popular Culture—World Politics Continuum." *Politics* 29 (3): 155–63.
Greenberg, Andy. 2016. "The Artist Using Museums to Amplify Tor's Anonymity Network." *Wired*. April 1. https://www.wired.com/2016/04/sculpture-lets-museums-amplify-tors-anonymity-network/.
Greenwald, Glenn. 2013a. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. June 6. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
Greenwald, Glenn. 2013b. "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'." *The Guardian*. July 31. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Random House.

Greenwald, Glenn. 2017. “Obama Killed a 16-Year-Old American in Yemen. Trump Just Killed His 8-Year-Old Sister.” *The Intercept*. January 30. https://theintercept.com/2017/01/30/obama-killed-a-16-year-old-american-in-yemen-trump-just-killed-his-8-year-old-sister/.
Greenwald, Glenn, and Ewen MacAskill. 2013. “NSA Prism Program Taps in to User Data of Apple, Google and Others.” *The Guardian*. June 7. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
Greenwald, Glenn, and James Ball. 2013. “The Top Secret Rules That Allow NSA to Use US Data Without a Warrant.” *The Guardian*. June 20. http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.
Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. 2013. “Microsoft Handed the NSA Access to Encrypted Messages.” *The Guardian*. July 12. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.
Grondin, David. 2010a. “Le poststructuralisme.” In *Théories des Relations Internationales*, edited by Alex Macleod and Dan O’Meara, 315–38. Montréal: Athéna Éditions.
Grondin, David. 2010b. “The New Frontiers of the National Security State: the US Global Governmentality of Contingency.” In *Security and Global Governmentality: Globalization, Governance and the State*, edited by Marc G Doucet and Miguel de Larrinaga, 78–95. London: Routledge, PRIO New Security Studies.
Grondin, David. 2014. “L’étude des Objets, Espaces et Sites de Sécurité de La Vie quotidienne.” *Études internationales* 44 (3) : 453–73. doi:10.7202/1021131ar.
Grondin, David, Anne-Marie D’Aoust, and Alex Macleod. 2010. “Les Études critiques de Sécurité.” In *Théories des Relations Internationales*, edited by Alex Macleod and Dan O’Meara. Montréal.
Gros, Frédéric. 2008. “Désastre humanitaire et Sécurité humaine. Le Troisième Âge de La Sécurité.” *Esprit* Mars/avril (3) : 51–66. doi:10.3917/espri.0803.0051.
Gros, Valentin, Marieke de Goede & Beste Isleyen. 2017. “The Snowden Files Made Public: a Material Politics of Contesting Surveillance.” *International Political Sociology* 11 (1): 73–89. doi:10.1093/ips/olw031.
Grosser, Benjamin. 2015. “ScareMail.” *Bengrosser.com*. http://bengrosser.com/projects/scaremail/.
Grove, Kevin. 2012. “Preempting the Next Disaster: Catastrophe Insurance and the Financialization of Disaster Management.” *Security Dialogue* 43 (2): 139–55. doi:10.1177/0967010612438434.
Gschrey, Raul. 2010. “Contemporary Closed Circuits—Subversive Dialogues. Artistic Strategies Against Surveillance.” *Surveillance & Society* 7 (2): 144–64.
Gurses, Seda, Arun Kundnani, and Joris Van Hoboken. 2016. “Crypto and Empire: the Contradictions of Counter-Surveillance Advocacy.” *Media, Culture & Society* 38 (4): 576–90. doi:10.1177/0163443716643006.
Gurses, Seda, Michelle Teran, and Manu Luksch. 2010. “A Trialogue on Interventions in Surveillance Space: Seda Gürses in Conversation with Michelle Teran and Manu Luksch.” *Surveillance & Society* 7 (2): 165–74.
Guyer, Paul. 2003. “History of Modern Aesthetics.” In *The Oxford Handbook of Aesthetics*, edited by Jerrold Levinson, 25–60. Oxford: Oxford University Press.
Haggerty, Kevin D, and Minas Samatas. 2010. “Introduction.” In *Surveillance and Democracy*, edited by Kevin D Haggerty and Minas Samatas, 1–16. New York: Routledge-Cavendish.

Haggerty, Kevin D, and Richard V Ericson. 2000. “The Surveillant Assemblage.” *British Journal of Sociology* 51 (4): 605–22. doi:10.1080/00071310020015280.
Hagmann, Jonas, and Myriam Dunn Cavelty. 2012. “National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity.” *Security Dialogue* 43 (1): 79–96. doi:10.1177/0967010611430436.
Hailey, Charlie. 2009. *Camps: A Guide to 21st Century Space*. Boston: The MIT Press.
Hansen, Lene. 2000. “The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School.” *Millennium-Journal of International Studies* 29 (2): 285–306. doi:10.1177/03058298000290020501.
Hansen, Lene. 2006. *Security as Practice: Discourse Analysis and the Bosnian War*. New York: Routledge.
Hansen, Lene. 2011. “Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply It.” *Review of International Studies* 38 (03): 525–46. doi:10.1017/S0260210511000581.
Harding, Luke. 2015. “The Node Pole: Inside Facebook’s Swedish Hub Near the Arctic Circle.” *The Guardian*. September 25. http://www.theguardian.com/technology/2015/sep/25/facebook-datacentre-lulea-sweden-node-pole.
Hardt, Michael, and Antonio Negri. 2000. *Empire*. Cambridge: Harvard University Press.
Hardt, Michael, and Antonio Negri. 2004. *Multitude: War and Democracy in the Age of Empire*. New York: Penguin Books.
Hardt, Michael, and Antonio Negri. 2009. *Commonwealth*. Cambridge: The Belknap Press of Harvard University Press.
Haro, Lia, and Romand Coles. 2014. “Journeys to Farther Shores: Intersecting Movements of Poetics, Politics, and Theory Beyond Utopia.” In *The Aesthetic Turn in Political Thought*, edited by Nikolas Kompridis, 113–41. New York: Bloomsbury.
Harvey, Adam. 2015. “Adam Harvey NYC.” *Ahprojects.com*. Accessed July 13. http://ahprojects.com/.
Harvey, P D A. 2015. “Fra’ Mauro’s World Map: A History. by Piero Falchetta.” *Imago Mundi* 67 (1): 106–7. doi:10.1080/03085694.2015.974962.
Hattem, Julian. 2015. “DOJ Fears Tech ‘Zone of Lawlessness’.” *The Hill*, January.
Hawley, Chris. 2012. “NYPD Monitored Muslim Students All Over Northeast.” *The Huffington Post*. February 18. http://www.huffingtonpost.com/2012/02/18/nypd-monitored-muslim-stu_0_n_1286647.html.
Helfand, Glen. 2015. “Trevor Paglen Review: Turning the NSA’s Data Combing Into High-Concept Art.” *The Guardian*. March 13. http://www.theguardian.com/artanddesign/2015/mar/13/trevor-paglen-art-review-nsa-surveillance-systems.
Herrick, Linda. 2015. “Venice Biennale: Creepy Take on Power.” *New Zealand Herald*. May 6. http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11444394.
Hertz, Garnet, ed. 2018. *Disobedient Electronics*. The Studio for Critical Making.
Hogue, Simon. 2016. “Performing, Translating, Fashioning: Spectatorship in the Surveillant World.” *Surveillance & Society* 14 (2): 168–83.
Holden, Gerard. 2006. “Cinematic IR, the Sublime, and the Indistinctness of Art.” *Millennium-Journal of International Studies* 34 (3): 793–818.
Holden, Gerard. 2010. “World Politics, World Literature, World Cinema.” *Global Society* 24 (3): 381–400. doi:10.1080/13600826.2010.485558.

Holder, Eric H, Jr. 2009. *Exhibit a: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*. Washington, DC. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01df/66465da1.dir/doc.pdf.

Horkheimer, Max, and Theodor W Adorno. 1974. *La dialectique de la raison. Fragments philosophiques*. Paris : Gallimard.

Horowitz, Craig. 2003. "The NYPD's War on Terror." *New York Magazine*. February 3. http://nymag.com/nymetro/news/features/n_8286/index.html.

House, Brian, and Kyle McDonald. 2014. "Conversnitch." *Brian House*. Accessed July 8. http://brianhouse.net/works/conversnitch/.

Howe, Daniel C, Helen Nissenbaum, and Vincent Toubiana. 2015. "TrackMeNot." *TrackMeNot*. Accessed October 30. https://cs.nyu.edu/trackmenot/.

Hristova, Stefka. 2014. "Recognizing Friend and Foe: Biometrics, Veridiction, and the Iraq War." *Surveillance & Society* 12 (4): 516–27.

Hu, Tung-Hui. 2015. *A Prehistory of the Cloud*. Cambridge, MA: MIT Press.

Hughes, Rachel. 2007. "Through the Looking Blast: Geopolitics and Visual Culture." *Geography Compass* 1 (5): 976–94. doi:10.1111/j.1749-8198.2007.00052.x.

Huhtamo, Erkki, and Jussi Parikka. 2011a. "Introduction." In *Media Archeology*, edited by Erkki Huhtamo and Jussi Parikka, 1–21. An Archeology of Media Archeology. Berkeley: University of California Press.

Huhtamo, Erkki, and Jussi Parikka, eds. 2011b. *Media Archeology*. Berkeley: University of California Press.

Huxley, Margo. 2007. "Geographies of Governmentality." In *Space, Knowledge and Power: Foucault and Geography*, edited by J W Crampton and Stuart Elden, 185–204. Burlington: Ashgate.

Huysmans, Jef. 2002. "Defining Social Constructivism in Security Studies: the Normative Dilemma of Writing Security." *Alternatives*, no. 27: 41–62.

Huysmans, Jef. 2006. *The Politics of Insecurity*. New York: Routledge.

ICANN. 2011a. *Guide D'introduction aux noms de Domaine*. ICANN.

ICANN. 2011b. *Beginner's Guide to Internet Protocol (IP) Addresses*. Los Angeles: ICANN.

ICANN. 2015. *Fonctions IANA*. Los Angeles: ICANN.

ICANN. 2017a. "Amended and Restated Articles of Incorportation of Internet Corporation for Assigned Names and Numbers." *Icann.org*. https://www.icann.org/resources/pages/governance/articles-en.

ICANN. 2017b. "Resources for Country Code Managers." *Icann.org*. https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en.

Introna, Lucas D, and David Murakami Wood. 2004. "Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems." *Surveillance & Society* 2 (2/3): 177–98.

IXmaps. 2017a. "Faq." *Ixmaps.Ca*. https://www.ixmaps.ca/learn/faq.php#faq-issue-two.

IXmaps. 2017b. "Learn: Issues." *Ixmaps.Ca*. https://www.ixmaps.ca/learn/issues.php#issue-one.

IXmaps. 2016. "IXmaps." *Ixmaps.Ca*. Accessed August 23. https://www.ixmaps.ca/index.php.

Jabri, Vivienne. 2006. "Shock and Awe: Power and the Resistance of Art." *Millennium-Journal of International Studies* 34 (3): 819–39.

Jervis, Robert. 1976. *Perception and Misperception in International Politics*. Princeton: Princeton University Press.

Johnson, Gabe. 2017. “An Artist Stares Back at the Surveillance State.” *Wall Street Journal*. May 26. http://www.wsj.com/video/an-artist-stares-back-at-the-surveillance-state/F7C6D25A-1009-48B7-8F73-CF9EFBB164F3.html.
Jozuka, Emiko. 2015. “Find Out Your ‘Algorithmic Citizenship’ Based on the Websites You Visit.” *Motherboard*. May 29. https://motherboard.vice.com/en_us/article/find-out-your-algorithmic-citizenship-based-on-the-websites-you-visit-1.
Kaiser, Robert. 2015. “The Birth of Cyberwar.” *Political Geography* 46 (C): 11–20. doi:10.1016/j.polgeo.2014.10.001.
Kane, Natalie. 2016. “Private Data Is the Ultimate Luxury Good.” *Motherboard*. September 27. https://motherboard.vice.com/en_us/article/private-data-is-the-ultimate-luxury-good.
Kant, Immanuel, and Christopher Kul-Want. 2010. “Critique of Judgement: Immanuel Kant.” In *Philosophers on Art from Kant to the Postmodernists: a Critical Reader*, edited by Christopher Kul-Want, translated by Werner S Pluhar, 21–39. New York: Columbia University Press.
Katz, Cindi. 2006. “The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction.” In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 27–36. New York: Routledge.
Katz, Cindi. 2008. “Me and My Monkey: What’s Hiding in the Security State.” In *Indefensible Spaces: The Architecture of National Insecurity State*, edited by Michael Sorkin, 305–24. New York: Routledge.
Kear, Adrian. 2013. “Traces of Presence.” In *International Politics and Performance: Critical Aesthetics and Creative Practice*, edited by Jenny Edkins and Adrian Kear, 19–39. London; New York: Routledge.
Kennedy, Paul. 1987. *The Rise and Fall of the Great Powers*. New York: Random House.
Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.
Keohane, Robert O, ed. 1986. *Neorealism and Its Critics*. New York: Columbia University Press.
Kholeif, Omar. 2018. “Electronic Superhighway (2016-1966).” *Whitechapel Gallery*. http://www.whitechapelgallery.org/exhibitions/electronicsuperhighway/.
Kingsbury, Paul, and John Paul Jones. 2009. “Walter Benjamin’s Dionysian Adventures on Google Earth.” *Geoforum* 40 (4): 502–13. doi:10.1016/j.geoforum.2008.10.002.
Knight, Deborah. 2003. “Aesthetics and Cultural Studies.” In *The Oxford Handbook of Aesthetics*, edited by Jerrold Levinson, 783–95. Oxford: Oxford University Press.
Kompridis, Nikolas. 2014. “Introduction: Turning and Returning: The Aesthetic Turn in Political Thought.” In *The Aesthetic Turn in Political Thought*, edited by Nikolas Kompridis, xiv—xxxvii. New York: Bloomsbury.
Krasner, Stephen D. 2001. “Abiding Sovereignty.” *International Political Science Review* 22 (3): 229–51.
Krause, Keith, and Michael C Williams, eds. 1997. *Critical Security Studies: Concepts and Cases*. New York: Routledge.
Kravets, David. 2013. “NSA Leak Vindicates at&T Whistleblower.” *Wired*. June 27. https://www.wired.com/2013/06/nsa-whistleblower-klein/.
Kress, Gunther, and Thed Van Leeuwen. 2006. *Reading Images: the Grammar of Visual Design*. 2nd ed. New York: Routledge.
Kul-Want, Christopher. 2010. “Introduction: Art and Philosophy.” In *Philosophers on Art from Kant to the Postmodernists: a Critical Reader*, edited by Christopher Kul-Want, 1–19. New York: Columbia University Press.

Kwan, Alan. 2013. “Bad Trip: Navigate My Mind.” *Kwanalan.com*. Accessed November 14. http://www.kwanalan.com/#!blank/czod.
La Fondation Courage. 2018. “Free Snowden.” *Edwardsnowden.com*. Accessed February 9. https://edwardsnowden.com/fr/.
Landau, Susan. 2013. “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations.” *IEEE Security & Privacy* 11 (4): 54–63.
Latour, Bruno. 2003. “What if We *Talked* Politics a Little?” *Contemporary Political Theory* 2 (2): 143–64. doi:10.1057/palgrave.cpt.9300092.
Laudon, Kenneth C. 1986. *Dossier Society*. New York: Columbia University Press.
Lawrence, John Shelton, and John G McGarrahan. 2008. “Operation Restore Honor in *Black Hawk Down*.” In *Why We Fought: America’s War in Film and History*, edited by Peter C Rollins and John E O’Connor, 431–57. Lexington, KY: University Press of Kentucky.
Le Monde. 2016. “Accusé de Viol et de Harcèlement, Jacob Appelbaum démissionne du Projet TOR.” *Le Monde*. June 7. http://www.lemonde.fr/pixels/article/2016/06/06/jacob-appelbaum-demissionne-du-projet-tor_4939068_4408996.html.
Lechner, Marie. 2014. “Transmediale prend la NSA dans sa toile.” *Libération*. February 3. http://next.liberation.fr/arts/2014/02/03/transmediale-prend-la-nsa-dans-sa-toile_977518.
Lehtiniemi, Tuukka. 2017. “Personal Data Spaces: an Intervention in Surveillance Capitalism?” *Surveillance & Society* 15 (5): 626–39.
Leonard, Robert. 2017. “Secret Power.” *Simondennysecretpower.com*. Accessed May 3. http://simondennysecretpower.com/.
Leslie, Camilo Arturo. 2016. “Territoriality, Map-Mindedness, and the Politics of Place.” *Theory and Society* 45 (2). Springer Netherlands: 169–201. doi:10.1007/s11186-016-9268-9.
Levin, Thomas Y, Ursula Frohne, and Peter Weibel, eds. 2002. *Ctrl [Space]*. Cambridge, MA: MIT Press.
Levinson, Jerrold. 2003. “Philosophical Aesthetics: An Overview.” In *The Oxford Handbook of Aesthetics*, edited by Jerrold Levinson, 3–24. Oxford: Oxford University Press.
Lévy, Jacques, ed. 2008. *L’invention du Monde*. Paris : Presses de Science Po.
LFP. 2018. “Library Freedom Project — Making Real the Promise of Intellectual Freedom in Libraries.” *Library Freedom Project*. Accessed January 8. https://libraryfreedomproject.org/.
Light, Evan. 2016. “Snowden Archive-in-a-Box.” Accessed June 17. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/portablearchive.html.
Lind, Maria. 2016. “Center Stage: Trevor Paglen.” *Kaleidoscope*, no. 26 (January).
Lippert, Randy, and Kevin Walby, eds. 2013. *Policing Cities*. New York: Routledge.
Lozano-Hemmer, Rafael, and Krzysztof Wodiczko. 2017. “Zoom Pavilion.” *Lozano-Hemmer.com*. http://www.lozano-hemmer.com/zoom_pavilion.php.
Luksch, Manu. n.d. “The FACELESS Project,” 1–14. http://www.manuluksch.com.
Lund, Jonas. 2014. “Public Access Me.” *Jonas Lund*. Accessed June 13. http://jonaslund.biz/works/public-access-me/.
Lupton, Deborah. 2016. *The Quantified Self*. Cambridge & Malden, MA: Polity.
Lyon, David. 1994. *The Electronic Eye. The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Philadelphia: Open University Press.
Lyon, David. 2003. “Surveillance as Social Sorting: Computer Codes and Mobile Bodies.” In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, edited by David Lyon, 13–30. London; New York: Routledge.

Lyon, David. 2010. “Identification, Surveillance and Democracy.” In *Surveillance and Democracy*, edited by Kevin D Haggerty and Minas Samatas, 34–50. New York: Routledge-Cavendish.
Lyon, David. 2014. “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.” *Big Data & Society* 1 (2): 1–13. doi:10.1177/2053951714541861.
MacAskill, Ewen, and Gabriel Dance. 2013. “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained.” *The Guardian*. November 1. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.
MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 2013. “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications.” *The Guardian*. June 21. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
MACBA. 2018. “Condensation Cube.” *MACBA*. http://www.macba.cat/en/condensation-cube-1523.
MacDonald, Fraser, Rachel Hughes, and Klaus Dodds, eds. 2010. *Observant States: Geopolitics and Visual Culture*. London: I.B. Tauris.
Machiavelli, Niccolo. 1994. *Selected Political Writings*. Edited and translated by David Wootton. Indianapolis/Cambridge: Hackett Publishing Company.
Magid, Jill. 2014. “Evidence Locker.” *Evidence Locker*. Accessed July 8. http://www.evidencelocker.net/story.php.
Managhan, Tina. 2012. *Gender, Agency and War: the Maternalized Body in US Foreign Policy*. New York: Routledge.
Mandaville, Peter, and Andrew Williams, eds. 2003. *Meaning and International Relations*. London: Routledge.
Manhire, Toby. 2016. “Secret Power, Tech Culture, Critique and Complicity — a Conversation with Artist Simon Denny.” *The Spinoff*. September 20. https://thespinoff.co.nz/featured/20-09-2016/secret-power-interview-simon-denny/.
Mann, Steve, and Joseph Ferenbok. 2013. “New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World.” *Surveillance & Society* 11 (1/2): 18–34.
Marquez, Renata Moreira, and Wellington Cançado Cançado. 2010. “Myopia Index.” *Surveillance & Society* 7 (2): 126–43.
Marwick, Alice E. 2012. “The Public Domain: Social Surveillance in Everyday Life.” *Surveillance & Society* 9 (4): 378–93.
Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
Marx, Gary T. 2002. “What’s New About the ‘New Surveillance’? Classifying for Change and Continuity.” *Surveillance & Society* 1 (1): 9–29.
Marx, Gary T. 2006. “Soft Surveillance: the Growth of Mandatory Volunteerism in Collecting Personal Information—‘Hey Buddy Can You Spare a DNA?’.” In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 37–56. New York: Routledge.
Mathews, Jessica Tuchman. 1989. “Redefining Security.” *Foreign Affairs* 68 (2): 162–77. doi:10.2307/20043906.
MAZI. 2018. “Mazi Project | Developing a DIY Networking Toolkit for Location-Based Collective Awareness.” *Mazizone.Eu*. http://www.mazizone.eu/.

Mazzetti, Mark, and Justin Elliott. 2013. “Spies Infiltrate a Fantasy Realm of Online Games.” *The New York Times*. December 9. https://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html.
McCann, Colin. 2011. “Geolocating IP Addresses for the IXmaps Database.” *Ixmaps.ca*. June 9. https://www.ixmaps.ca/docs/report-2011-mccann-geolocating.pdf.
McClintock, Anne. 1995. *Imperial Leather: Race, Gender and Sexuality in the Colonial Contest*. New York: Routledge.
McCulloch, Jude, and Sharon Pickering. 2009. “Pre-Crime and Counter-Terrorism: Imagining Future Crime in the ‘War on Terror’.” *British Journal of Criminology* 49 (5): 628–45. doi:10.1093/bjc/azp023.
McCutcheon, Chuck. 2013. “Government Surveillance.” *CQ Researcher* 23 (30). CQ Researcher: 717–40.
McDonald, Kyle, and Lauren McCarthy. 2014. “Pplkpr.” *The Frank-Ratchye Studio for Creative Inquiry*. http://studioforcreativeinquiry.org/projects/pplkpr.
McGarry, Kevin. 2015. “New Zealand’s Contribution to the Venice Biennale: a Library and an Airport, Transposed.” *The New York Times*. May 1. http://tmagazine.blogs.nytimes.com/2015/05/01/new-zealand-venice-biennale-petzel-simon-denny/?_r=1.
McGrath, John. 2004. *Loving Big Brother: Performance, Privacy and Surveillance Space*. New York: Routledge.
McGrath, John, and Robert J Sweeny. 2010. “Editorial: Surveillance, Performance and New Media.” *Surveillance & Society* 7 (2): 90–93.
Mearsheimer, John J. 1990. “Back to the Future: Instability in Europe After the Cold War.” *International Security* 15 (1): 5–56.
Medovoi, L. 2007. “Global Society Must Be Defended: Biopolitics Without Boundaries.” *Social Text* 25 (2). Duke University Press: 53–79. doi:10.1215/01642472-2006-027.
Mendelsohn, Ben. 2011. *Bundled, Buried & Behind Closed Doors*. Edited by Ben Mendelsohn. New York.
Merson, Emily H. 2017. “International Art World and Transnational Artwork: Creative Presence in Rebecca Belmore’s Fountain at the Venice Biennale.” *Millennium-Journal of International Studies* 46 (September): 41–65.
Miller, Peter, and Nikolas Rose. 1990. “Governing Economic Life.” *Economy and Society* 19 (1): 1–31. doi:10.1080/03085149000000001.
Mirzoeff, Nicholas. 2011. “The Right to Look.” *Critical Inquiry* 37 (3): 473–96. doi:10.1086/659354.
Mittelman, James H, and Christine B N Chin. 2005. “Conceptualizing Resistance to Globalization.” In *The Global Resistance Reader*, edited by Louise Amoore, 17–27. New York: Routledge.
Monahan, Torin. 2006a. “Questioning Surveillance and Security.” In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 1–23. New York: Routledge.
Monahan, Torin. 2010. *Surveillance in the Time of Insecurity*. New Brunswick, NJ; London: Rutgers University Press.
Monahan, Torin. 2011. “Surveillance as Cultural Practice.” *The Sociological Quarterly* 52 (4). Wiley Online Library: 495–508.

Monahan, Torin. 2015. “The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance.” *Communication and Critical/Cultural Studies*, 1–22. doi:10.1080/14791420.2015.1006646.
Monahan, Torin. 2017. “Ways of Being Seen: Surveillance Art and the Interpellation of Viewing Subjects.” *Cultural Studies* 7 (September): 1–22. doi:10.1080/09502386.2017.1374424.
Monahan, Torin, and Jennifer T Mokos. 2013. “Crowdsourcing Urban Surveillance: the Development of Homeland Security Markets for Environmental Sensor Networks.” *Geoforum* 49 (C): 279–88. doi:10.1016/j.geoforum.2013.02.001.
Monahan, Torin, and Neil A Palmer. 2009. “The Emerging Politics of DHS Fusion Centers.” *Security Dialogue* 40 (6): 617–36. doi:10.1177/0967010609350314.
Monahan, Torin, David J Phillips, and David Murakami Wood. 2010. “Surveillance and Empowerment.” *Surveillance & Society* 8 (2): 106–12.
Monahan, Torin, ed. 2006b. *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.
Monfasani, John. 1982. “Review: Bessarion’s Library and the Biblioteca Marciana: Six Early Inventories by Lotte Labowsky.” *Renaissance Quarterly* 35 (2): 265–67.
Moore, Cerwyn. 2010. *Contemporary Violence: Post-Modern War in Kosovo and Chechnya*. Manchester: Manchester University Press.
Moore, Cerwyn, and Laura J Shepherd. 2010. “Aesthetics and International Relations: Towards a Global Politics.” *Global Society* 24 (3): 299–309. doi:10.1080/13600826.2010.485564.
Morgner, Christian. 2017. “Diversity and (in)Equality in the Global Art World: Global Development and Structure of Field-Configuring Events.” *New Global Studies* 11 (3): 522–32. doi:10.1515/ngs-2016-0015.
Morone, Jennifer Lyn. 2015. “JLM Inc.” *Jenniferlynmorone.com*. Accessed October 29. http://jenniferlynmorone.com/.
Mott, Nathaniel. 2016. “Take That, FBI: Apple Goes All in on Encryption.” *The Guardian*. June 15. http://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc.
Mouffe, Chantal. 2000. *The Democratic Paradox*. New York: Verso.
Mozilla, Tactical Technology Collective. 2017. “Data Detox Kit.” *Datadetox.Myshadow.org*. November. https://datadetox.myshadow.org/detox.
Muller, Benjamin J. 2014. “Is There a Cabin in the Woods? Reflections on Mass Surveillance and Human Rights.” *E-International Relations*. December 21. http://www.e-ir.info/2014/12/21/is-there-a-cabin-in-the-woods-reflections-on-mass-surveillance-and-human-rights/.
Mun, Sang. 2012. “Zxx.” *Z-X-X.org*. http://z-x-x.org/.
Murray, Ben. 2015. “Algorithmic Citizenship: Laura Poitras, James Bridle and the Digital Self.” *Institute of Contemporary Arts*. June 1. https://www.ica.art/blog/exploring-algorithmic-citizenship.
Mutlu, Can E, and Mark B Salter. 2013. “The Discursive Turn: Introduction.” In *Research Method in Critical Security Studies: An Introduction*, edited by Mark B Salter and Can E Mutlu, 113–19. New York: Routledge.
Müller-Maguhn, Andy, Laura Poitras, Marcel Rosenbach, Michael Sontheimer, and Christian Grothoff. 2014. “Treasure Map: the NSA Breach of Telekom and Other German Firms.” *Spiegel Online*. September 14. http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html.

Mythen, Gabe, and Sandra Walklate. 2008. “Terrorism, Risk and International Security: The Perils of Asking ‘What if?’.” *Security Dialogue* 39 (2–3): 221–42. doi:10.1177/0967010608088776.
Nakashima, Ellen. 2013. “Newly Declassified Documents on Phone Records Program Released.” *The Washington Post*. July 31. http://www.washingtonpost.com/world/national-security/governments-secret-order-to-verizon-to-be-unveiled-at-senate-hearing/2013/07/31/233fdd3a-f9cf-11e2-a369-d1954abcb7e3_story.html.
Nakashima, Ellen. 2014. “FBI Director: Tech Companies Should Be Required to Make Devices Wiretap-Friendly.” *The Washington Post*. October 16. http://www.washingtonpost.com/world/national-security/fbi-director-tech-companies-should-be-required-to-make-devices-wire-tap-friendly/2014/10/16/93244408-555c-11e4-892e-602188e70e9c_story.html.
Nakashima, Ellen, and Ashkan Soltani. 2014. “Privacy Watchdog’s Next Target: The Least-Known but Biggest Aspect of NSA Surveillance.” *The Washington Post*. July 23. https://www.washingtonpost.com/news/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/.
Nakashima, Ellen, and Joby Warrick. 2013. “For NSA Chief, Terrorist Threat Drives Passion to ‘Collect It All’.” *The Washington Post*. July 14. http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.
Naughton, John. 2016. “Death from Above, Dished Out by Algorithm.” *The Guardian*. February 21. http://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan.
Needleman, Rafe. 2009. “‘Sex-Positive URL Shortener’ Vbly Launches.” *Cnet*. August 9. https://www.cnet.com/news/sex-positive-url-shortener-vbly-launches/.
Nelson, Margaret K, and Anita Ilta Garey, eds. 2009. *Who’s Watching? Daily Practices of Surveillance Among Contemporary Families*. Nashville, TN: Vanderbilt University Press.
Neocleous, Mark. 2003. “Off the Map: on Violence and Cartography.” *European Journal of Social Theory* 6 (4): 409–25.
Neumann, Iver B. 1999. *Uses of the Other: the “East” in European Identity Formation*. Minneapolis: University of Minnesota Press.
Neumann, Iver B. 2002. “Returning Practice to the Linguistic Turn: The Case of Diplomacy.” *Millennium-Journal of International Studies* 31 (3): 627–51.
Nordstrom, Carolyn. 2007. *Global Outlaws: Crime Money and Power in the Contemporary World*. Berkeley, CA: University of California Press.
Norfolk, Simon. 2015. “Simon Norfolk.” *Simonnorfolk.com*. Accessed October 27. http://www.simonnorfolk.com/pop.html.
Norval, Aletta J. 2014. “‘Writing a Name in the Sky’: Rancière, Cavell, and the Possibility of Egalitarian Inscription.” In *The Aesthetic Turn in Political Thought*, edited by Nikolas Kompridis, 189–226. New York: Bloomsbury.
NSA. 2008. *ANT Catalog*.
NSA. 2010. *Bad Guys Are Everywhere, Good Guys Are Somewhere: NTOC Technology Development*.
NSA. 2012a. *Driver 1: Worldwide SIGINT/Defense Cryptologic Platform*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01d2/a9a5c2a3.dir/doc.pdf.
NSA. 2012b. *Tor Stinks*.

NSA. 2012c. *SIGINT Strategy 2012–2016*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0168/bba8e353.dir/doc.pdf.
NSA. 2012d. *TEMPORA--"the World's Largest XKEYSCORE"--Is Now Available to Qualified NSA Users*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc5f6.dir/doc.pdf.
NSA. 2016. "Frequently Asked Questions Oversight." *National Security Agency*. May 3. https://www.nsa.gov/about/faqs/oversight-faqs.shtml.
Nunes, Joao. 2012. "Reclaiming the Political: Emancipation and Critique in Security Studies." *Security Dialogue* 43 (4): 345–61. doi:10.1177/0967010612450747.
Nuti, Lucia. 2008. "Review: Terrarum Orbis: History of the Representation of Space in Text and Image, 5., by Piero Falchetta." *Isis* 99 (1): 169–70. doi:10.1086/589350.
O Tuathail, Gearoid. 1996. *Critical Geopolitics: The Politics of Writing Global Space*. London: Routledge.
Obermaier, Frederik, Henrik Moltke, Laura Poitras, and Jan Strozyk. 2014. "Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts." *Süddeutsche Zeitung*. November 25. http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsidiary-cable.
ODNI. 1981. "Executive Order 12333-United States Intelligence Activities." *Office of the Director of National Intelligence*. December 8. https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.
ODNI. 2017a. "Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents." *IC on the Record*. May 11. https://icontherecord.tumblr.com/tagged/section-702.
ODNI. 2017b. "Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016." *IC on the Record*. Accessed October 31. https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.
Office of General Counsel, Office of General. 2008. *FISA Amendments Act of 2008 Section 702: Summary Document*.
Oliver, Julian. 2015. "The Transparency Grenade." *Transparencygrenade.com*. Accessed July 13. http://transparencygrenade.com/.
Oliver, Julian, and Danja Vasiliev. 2014a. "PRISM: The Beacon Frame." *The Critical Engineering Working Group*. February 5. http://criticalengineering.org/projects/prism-the-beacon-frame/.
Oliver, Julian, and Danja Vasiliev. 2014b. "PRISM: The Beacon Frame." *Julian Oliver*. February 7. http://julianoliver.com/output/the-beacon-frame.
Oliver, Julian, Gordan Savicic, and Danja Vasiliev. 2014. "The Critical Engineering Manifesto." Translated by Benedicte Jacob. *The Critical Engineering Working Group*. http://criticalengineering.org/.
Olshin, Benjamin B. 2014. "Book Reviews: Piero Falchetta. Fra Mauro's World Map: a History." *Isis* 105 (4): 839.
Oremus, Will. 2014. "Facebook Atlas Ad Platform: Your Data Will Follow You Across Web, Apps, Devices." *Slate*. September 29. http://www.slate.com/blogs/future_tense/2014/09/29/facebook_atlas_ad_platform_your_data_will_follow_you_across_web_apps_devices.html.

Organisation internationale de normalisation. 2017. “Codes des Noms de Pays — ISO 3166.” *Iso.org*. Accessed July 5. https://www.iso.org/fr/iso-3166-country-codes.html.
Packard, Cassie. 2015. “The Sublimity of the Surveillance State.” *Hyperallergic*. October 21. http://hyperallergic.com/246790/the-sublimity-of-the-surveillance-state/.
Packer, Jeremy. 2006. “Becoming Bombs: Mobilizing Mobility in the War of Terror.” *Cultural Studies* 20 (4–5): 378–99. doi:10.1080/09502380600711105.
Paglen, Trevor. 2008. *I Could Tell You but Then You Would Have to Be Destroyed by Me*. New York: Melville House.
Paglen, Trevor. 2014a. “Autonomy Cube.” *Paglen*. http://www.paglen.com/?l=work&s=cube.
Paglen, Trevor. 2014b. “National Security Agency Surveillance Base, Cornwall, UK, 2014.” *Artnet*. http://www.artnet.com/artists/trevor-paglen/national-security-agency-surveillance-base-bude-54CEzoqk3eo-V8Kj52Fhhg2.
Paglen, Trevor. 2015. “NSA Surveillance Base, Egelsbach, Germany, 2015.” *Artsy.Net*. https://www.artsy.net/artwork/trevor-paglen-nsa-surveillance-base-egelsbach-germany.
Paglen, Trevor. 2016. “NSA-Tapped Fiber Optic Cable Landing Site, Keawaula, Hawaii, United States, 2016.” *Art Basel*. https://www.artbasel.com/catalog/artwork/44868/Trevor-Paglen-NSA-Tapped-Fiber-Optic-Cable-Landing-Site-Keawaula-Hawaii-United-States.
Paglen, Trevor. 2018. “Biography.” *Paglen.com*.
Paglen, Trevor. 2017a. “Code Names of the Surveillance State.” Accessed June 30. http://www.paglen.com/?l=work&s=code_names_of_the_.
Paglen, Trevor. 2017b. “Symbology.” Accessed September 13. http://www.paglen.com/?l=work&s=symbology&i=0.
Paglen, Trevor, and Jacob Appelbaum. 2016. “Trevor Paglen & Jacob Appelbaum.” *Bomb*. March 16. https://bombmagazine.org/articles/trevor-paglen-jacob-appelbaum/.
Pallister-Wilkins, Polly. 2016. “How Walls Do Work: Security Barriers as Devices of Interruption and Data Capture.” *Security Dialogue* 47 (2): 151–64. doi:10.1177/0967010615615729.
Pangburn, D J. 2014. “This Parody of NSA’s PRISM Was So Good Police Almost Shut It Down.” *Motherboard*. February 4. http://motherboard.vice.com/blog/this-parody-of-nsas-prism-was-so-good-police-almost-shut-it-down.
Parikka, Jussi. 2012. *What Is Media Archaeology?* Cambridge; Malden, MA: Polity Press.
PCLOB. 2014. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Edited by David Medine, Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald. Washington, DC. https://www.pclob.gov/library/702-Report.pdf.
Pearlman, Ellen. 2014. “Transmediale Festival Shuts Down NSA Imitators.” *Hyperallergic*. February 19. http://hyperallergic.com/109546/transmediale-festival-shuts-down-nsa-imitators/.
Peng! 2016. “Intelexit.” Accessed April 11. http://pen.gg/.
Peoples, Columba, and Nick Vaughan-Williams. 2010. *Critical Security Studies*. London; New York: Routledge.
Perkins, Chris, and Martin Dodge. 2009. “Satellite Imagery and the Spectacle of Secret Spaces.” *Geoforum* 40 (4): 546–60. doi:10.1016/j.geoforum.2009.04.012.
Perlroth, Nicole, Jeff Larson, and Scott Shane. 2013. “N.S.a. Able to Foil Basic Safeguards of Privacy on Web.” *The New York Times*. September 5. https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

Peterson, Tim. 2014. “Google Tests Way to Track Consumers from Mobile Browsers to the Apps They Use.” *Ad Age*. August 7. http://adage.com/article/digital/google-tie-mobile-web-app-trackers-ad-targeting/294502/.
PirateBox. 2017. “Start [PIRATEBOX].” *Piratebox.Cc*. July 7. https://piratebox.cc/start.
Platon. 1967. *Protagoras — Euthydème — Gorgias —Ménexène —Ménon —Cratyle*. Translated by Émile Chambry. Paris : GF-Flammarion.
Poitras, Laura. 2015. “‘The Art of Dissent’.” *The New York Times*. June 9. http://www.nytimes.com/2015/06/09/opinion/the-art-of-dissent.html?_r=0.
Poitras, Laura, and Kate Crawford. 2015. “Divorce Your Metadata: A Conversation Between Laura Poitras and Kate Crawford.” *Rhizome*. June 9. http://rhizome.org/editorial/2015/jun/9/divorce-your-metadata/?ref=nwslettr.
Poitras, Laura, ed. 2014. *Citizenfour*.
Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, Holger Stark, and Jonathan Stock. 2013. “Cover Story: How the NSA Targets Germany and Europe.” *Spiegel Online*. July 1. http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.
Pouliot, Vincent. 2007. “‘Sobjectivism’: Toward a Constructivist Methodology.” *International Studies Quarterly* 51 (2): 359–84.
Privacy France. 2018. “Big Brother Awards France— Qui surveillera Les Surveillants ?” *Big Brother Awards France*. http://bigbrotherawards.eu.org/.
Programme des Nations Unies pour le développement. 1994. “Rapport mondial sur Le Développement humain 1994.” Paris : Economica.
Pusca, Anca. 2008. “The Aesthetics of Change: Exploring Post-Communist Spaces.” *Global Society* 22 (3): 369–86. doi:10.1080/13600820802090512.
Rafman, Jon. 2015. “Jon Rafman.” *Jonrafman.com*. Accessed October 28. http://jonrafman.com/.
Raley, Rita. 2009. *Tactical Media*. Minneapolis: University of Minnesota Press.
Raley, Rita. 2013. “Dataveillance and Counterveillance.” In *“Raw Data” Is an Oxymoron*, edited by Lisa Gitelman, 121–45. Cambridge.
Rancière, Jacques. 1999. *Dis-Agreement. Politics and Philosophy*. Translated by Julie Rose. Minneapolis: University of Minnesota Press.
Rancière, Jacques. 2000. *Le Partage du Sensible. Esthétique et Politique*. Paris : La fabrique.
Rancière, Jacques. 2008. *Le Spectateur émancipé*. Paris : La fabrique.
Rancière, Jacques. 2010. “The Janus-Face of Politicized Art.” In *Philosophers on Art from Kant to the Postmodernists. A Critical Reader*, edited by Christopher Kul-Want, translated by Gabriel Rockhill, 293–302. New York: Columbia University Press.
Rancière, Jacques. 2014. “The Aesthetic Dimension: Aesthetics, Politics, Knowledge.” In *The Aesthetic Turn in Political Thought*, edited by Nikolas Kompridis, 263–80. New York: Bloomsbury.
Rasmussen, Mikkel Vedby. 2002. “‘A Parallel Globalization of Terror’: 9–11, Security and Globalization.” *Cooperation and Conflict* 37 (3): 323–49. doi:10.1177/0010836702037003676.
Reed, Michael G, Paul F Syverson, and David M Goldschlag. 1998. “Anonymous Connections and Onion Routing.” *IEEE Journal on Selected Areas in Communications* 16 (4): 482–94.
Regan, Priscilla M, and Valerie Steeves. 2010. “Kids R Us: Online Social Networking and the Potential for Empowerment.” *Surveillance & Society* 8 (2): 151–65.
Reid, Julian. 2006. *The Biopolitics of the War on Terror*. Manchester & New York: Manchester University Press.

Reuters. 2013. “NSA Controls Global Internet Traffic via Private Fiber-Optic Cables.” *Reuters*. July 8. https://www.rt.com/usa/nsa-fiber-optic-cable-790/.
Reynolds, Bryan, and Joseph Fitzpatrick. 1999. “The Transversality of Michel de Certeau: Foucault’s Panoptic Discourse and the Cartographic Impulse.” *Diacritics* 29 (3). The Johns Hopkins University Press: 63–80.
Rhizome. 2016. “Net Art Anthology.” *Antology.Rhizome*. October 27. http://anthology.rhizome.org/.
Richard, Claire. 2015. “Découvrez Votre Citoyenneté algorithmique.” *Le Nouvel Observateur*. June 2. http://tempsreel.nouvelobs.com/rue89/rue89-rue89-culture/20150602.RUE9292/decouvrez-votre-citoyennete-algorithmique.html.
Riches, Harriet. 2016. “Electronic Superhighway (2016-1966).” *Afterimage* 43 (6): 17–19.
Rickford, Russell. 2016. “Black Lives Matter.” *New Labor Forum* 25 (1): 34–42. doi:10.1177/1095796015620171.
Ridgway, Renée. 2017. “Against a Personalisation of the Self.” *Ephemera* 17 (2): 377–97.
Risen, James, and Laura Poitras. 2013. “N.S.a. Report Outlined Goals for More Power.” *The New York Times*. November 22. https://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html.
Roberts, Dan, Ben Jacobs, and Spencer Ackerman. 2015. “NSA Reform: Bush-Era Powers Expire as US Prepares to Roll Back Surveillance.” *The Guardian*. June 1. http://www.theguardian.com/us-news/2015/may/31/nsa-reform-senate-deal-as-patriot-act.
Rokeby, David. 2010. “Works: Sorting Daemon (2003).” *Davidrokeby.com*. November 25. http://www.davidrokeby.com/sorting.html.
Ronnenberg, Philipp. 2017. “Ronnenberg Creative Technology.” *Ronnenberg.Io*. http://ronnenberg.io/.
Rose, Nikolas, Pat O’Malley, and Mariana Valverde. 2006. “Governmentality.” *Annual Review of Law and Social Science* 2 (1): 83–104. doi:10.1146/annurev.lawsocsci.2.081805.105900.
Rosenau, James N. 1992. “Governance, Order, and Change in World Politics.” In *Governance Without Government: Order and Change in World Politics*, edited by James N Rosenau and Ernst-Otto Czempiel. Cambridge: Cambridge University Press.
Roth, Evan. 2015. “Evan Roth.” *Evan-Roth.com*. Accessed October 29. http://www.evan-roth.com/shows/.
Rouvroy, Antoinette, and Thomas Berns. 2010. “Le Nouveau Pouvoir statistique.” *Multitudes*, no. 1 : 88–103.
Rowley, Christina. 2010. “Popular Culture and the Politics of the Visual.” In *Gender Matters in Global Politics: A Feminist Introduction to International Relations*, edited by Laura J Shepherd, 309–25. New York; London: Routledge.
Rutkin, Aviva. 2015. “Cyber Citizen Tool Shows Which Countries’ Laws Cover Our Surfing.” *New Scientist*. June 11. https://www.newscientist.com/article/dn27705-cyber-citizen-tool-shows-which-countries-laws-cover-our-surfing/#.VXnzV9m9LCQ.
Salter, Mark B. 2004. “Passports, Mobility, and Security: How Smart Can the Border Be?” *International Studies Perspectives* 5 (1): 71–91.
Salter, Mark B. 2006. “The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics.” *Alternatives: Global, Local, Political* 31 (2): 167–89.
Salter, Mark B. 2008a. “Risk and Imagination in the War on Terror.” In *Risk and the War on Terror*, edited by Louise Amoore and Marieke de Goede, 233–46. London; New York: Routledge.

Salter, Mark B, ed. 2008b. *Politics at the Airport*. Minneapolis: University of Minnesota Press.
Salter, Mark B, ed. 2015. *Making Things International, 1: Circuits and Motion*. Minneapolis: University of Minnesota Press.
Salter, Mark B, ed. 2016. *Making Things International, 2: Catalysts and Reactions*. Minneapolis: University of Minnesota Press.
Scahill, Jeremy, and Glenn Greenwald. 2014. "The NSA's Secret Role in the U.S. Assassination Program." *The Intercept*. February 10. https://theintercept.com/2014/02/10/the-nsas-secret-role/.
Scahill, Jeremy, and Ryan Devereaux. 2014. "Watch Commander: Barack Obama's Secret Terrorist-Tracking System, by the Numbers." *The Intercept*. August 5. https://theintercept.com/2014/08/05/watch-commander/.
Schmitt, Carl. 1988. *Théologie politique*. Translated by Jean-Louis Schlegel. Paris : Éditions Gallimard.
Schrager, Leah, and Jennifer Chan. 2015a. "About." *Body Anxiety*. January 24. http://bodyanxiety.com/about/.
Schrager, Leah, and Jennifer Chan. 2015b. "Body Anxiety." *Body Anxiety*. January 25. http://bodyanxiety.com/gallery/landing/.
Schwartz, Rafi. 2015. "What Your 'Algorithmic Citizenship' Says About Your Web Habits." *Good*. June 2. https://www.good.is/articles/whats-your-global-internet-algorithmic-citizenship.
Scott, Allen. 2004. "Hollywood and the World: The Geography of Motion-Picture Distribution and Marketing." *Review of International Political Economy* 11 (1): 33–61. doi:10.1080/0969229042000179758.
Scott, James C. 2012. *Two Cheers for Anarchism*. Princeton & Oxford: Princeton University Press.
SecureDrop. 2018. "The Official SecureDrop Directory." *SecureDrop*. January 2. https://securedrop.org/directory.
Sending, Ole Jacob, and Iver B Neumann. 2006. "Governance to Governmentality: Analyzing NGOs, States, and Power." *International Studies Quarterly* 50 (3): 651–72.
Senellart, Michel. 2004. "Situation des Cours." In *Sécurité, Territoire, Population. Cours Au Collège de France (1977-1978)*, 379–411. Paris: Seuil/Gallimard.
Sessions, Jeff. 2017. *Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*. https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf.
Sécurité publique Canada. 2010. *Guide pour La Préparation D'un Plan stratégique de Gestion Des Urgences 2010–2011*. Ottawa : Sa Majesté la Reine du Chef du Canada.
Sécurité publique Canada. 2012. *Bâtir Un Canada sécuritaire et résilient*. Ottawa : Sa Majesté la Reine du Chef du Canada.
Shapiro, Michael J. 2013. *Studies in Trans-Disciplinary Method: After the Aesthetic Turn*. London; New York: Routledge.
Shapiro, Michael J. 2018. *The Political Sublime*. Durham, NC: Duke University Press.
Shaw, Ian Graham Ronald. 2010. "Playing War." *Social & Cultural Geography* 11 (8): 789–803. doi:10.1080/14649365.2010.521855.
Sheller, Mimi, and John Urry. 2006. "The New Mobilities Paradigm." *Environment and Planning A* 38 (February): 207–26.

Shim, David. 2014. “Remote Sensing Place: Satellite Images as Visual Spatial Imaginaries.” *Geoforum* 51 (C): 152–60. doi:10.1016/j.geoforum.2013.11.002.
Shusterman, Richard. 2003. “Aesthetics and Postmodernism.” In *The Oxford Handbook of Aesthetics*, edited by Jerrold Levinson, 771–82. Oxford: Oxford University Press.
Smith, Steve. 2004. “Singing Our World into Existence: International Relations Theory and September 11.” *International Studies Quarterly* 48 (3). Wiley Online Library: 499–515.
Snowden, Edward, Laura Poitras, and Glenn Greenwald. 2013. “NSA Whistleblower Edward Snowden: ’I Don’t Want to Live in a Society That Does These Sort of Things’.” *The Guardian*. June 9. http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.
Soltani, Ashkan, Andrea Peterson, and Barton Gellman. 2013. “NSA Uses Google Cookies to Pinpoint Targets for Hacking.” *The Washington Post*. December 10. http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/.
Soulellis, Paul. 2016. “The Download: Technologies of Care.” *Rhizome*. October 4. http://rhizome.org/editorial/2016/oct/04/the-download-technologies-of-care/.
Spahr, Robert. 2010. “Recent Thoughts on Panoptic Cruft (Fragments).” *Surveillance & Society*, no. 7: 2.
Spiegel. 2014. “New NSA Revelations: Inside Snowden’s Germany File.” *Spiegel Online*. June 18. http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html.
Springer, Simon. 2010. “Public Space as Emancipation: Meditations on Anarchism, Radical Democracy, Neoliberalism and Violence.” *Antipode* 43 (2): 525–62. doi:10.1111/j.1467-8330.2010.00827.x.
Squires, Paul. 2014. “PRISM Is Disabled at Transmediale.” *Imperica*. February 3. http://www.imperica.com/en/news/prism-is-disabled-at-transmediale.
Stoddart, Eric. 2014. “(In)Visibility Before Privacy: A Theological Ethics of Surveillance as Social Sorting.” *Studies in Christian Ethics* 27 (1): 33–49. doi:10.1177/0953946813509335.
Stonebridge, Lyndsey. 2015. “How Books Help Us to Be Better Political Citizens.” *New Statesman*. August 25. https://www.newstatesman.com/culture/2015/08/how-books-help-us-be-better-political-citizens.
Sylvester, Christine. 2009. *Art/Museums: International Relations Where We Least Expect It*. Boulder: Paradigm Publishers.
Sylvester, Christine. 2013. “Power, Security and Antiquities.” In *International Politics and Performance: Critical Aesthetics and Creative Practice*, edited by Jenny Edkins and Adrian Kear, 203–20. London; New York: Routledge.
Tactical Technology Collective. 2018. “Alternative App Centre.” *Me and My Shadow*. Accessed January 31. https://myshadow.org/resources.
Tactical Technology Collective, Front Line Defenders. 2017. “Security in a Box—Digital Security Tools and Tactics.” *Security in a Box*. Accessed June 7. https://securityinabox.org.
Taylor, Diana. 2013. “Animating Politics.” In *International Politics and Performance: Critical Aesthetics and Creative Practice*, edited by Jenny Edkins and Adrian Kear, 84–95. New York: Routledge.
Te Papa. 2016a. “Watch: Simon Denny on the Most Important Visual Documents of Our Age.” *Museum of New Zealand/Te Papa Tongarewa*. September 16. https://www.tepapa.govt.nz/visit/whats-on/exhibitions/nga-toi-arts-te-papa/simon-denny-secret-power/watch-simon-denny-on-most.

Te Papa. 2016b. “Watch: Simon Denny Talks Terminator and the Irony of Artificial Intelligence.” *Museum of New Zealand/Te Papa Tongarewa*. September 16. https://www.tepapa.govt.nz/visit/whats-on/exhibitions/nga-toi-arts-te-papa/simon-denny-secret-power/terminator-artificial-intelligence.
Te Papa. 2016c. “Watch: Simon Denny’s Guide to Secret Power at Te Papa.” *Museum of New Zealand/Te Papa Tongarewa*. September 16. https://www.tepapa.govt.nz/visit/whats-on/exhibitions/nga-toi-arts-te-papa/simon-denny-secret-power/watch-simon-dennys-guide.
Teasly, Martell Lee, Jerome H Schiele, Charles Adams, and Nathern S Okilwa. 2018. “Trayvon Martin: Racial Profiling, Black Male Stigma, and Social Work Practice.” *Social Work* 63 (1): 37–45.
TeleGeography. 2017a. “Global Internet Map Map 2017.” Edited by Markus Krisetya, Larry Lairson, Alan Mauldin, and Tim Stronge. *TeleGeography*. http://global-internet-map-2017.telegeography.com/.
TeleGeography. 2017b. “Submarine Cable Map.” *TeleGeography*. http://www.submarinecablemap.com/.
TeleGeography. 2017c. “Submarine Cable Map 2015.” *TeleGeography*. Accessed July 21. http://submarine-cable-map-2015.telegeography.com/.
Thackara, Tess. 2015. “The New Zealand Pavilion Uncovers the Art of the NSA.” *Artsy*. May 8. https://www.artsy.net/article/artsy-editorial-the-new-zealand-pavilion-uncovers-the-art-of.
The Creators Project. 2016. *Trevor Paglen’s Deep Web Dive | Behind the Scenes*.
The Glass Room. 2017. “About The Glass Room.” *The Glass Room*. https://theglassroom.org/about/.
The Guardian. 2013a. “Glenn Greenwald’s Partner Detained at Heathrow Airport for Nine Hours.” *The Guardian*. August 19. http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow.
The Guardian. 2013b. “NSA Prism Program Slides.” *The Guardian*. November 1. http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.
The New Transparency. 2013. “What Is IXmaps?” *Vimeo*. May 27. https://vimeo.com/67102223.
Timberg, Craig, and Ellen Nakashima. 2013. “Agreements with Private Companies Protect U.S. Access to Cables’ Data for Surveillance.” *The Washington Post*. July 6. https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.
Tor. 2018a. “Users — Tor Metrics.” *Tor Project*. February 1. https://metrics.torproject.org/userstats-relay-country.html.
Tor. 2018b. “The Tor Project Is Always Looking for More Great People to Join Our Team!” *Tor Project*. Accessed January 8. https://www.torproject.org/about/jobs.html.en.
Tor. 2018c. “Tor Project: FAQ.” *Tor Project*. Accessed January 31. https://www.torproject.org/docs/faq.html.en#AmITotallyAnonymous.
Tor. 2018d. “Tor: Overview.” *Tor Project*. Accessed January 2. https://www.torproject.org/about/overview.html.en.
Tor. 2018e. “Who Uses Tor?” *Tor Project*. Accessed January 8. https://www.torproject.org/about/torusers.html.en.
transmediale. 2014a. “Afterglow.” *Transmediale*. https://transmediale.de/content/afterglow.
transmediale. 2014b. “Transmediale 2014 Afterglow.” *Transmediale*. http://www.transmediale.de/archive/history/festival/2014.

transmediale. 2014c. “Transmediale Statement Regarding the Partial Disablement of the Work ‘PRISM: The Beacon Frame’ by Julian Oliver and Danja Vasiliev.” *Transmediale*. https://transmediale.de/content/transmediale-statement-regarding-the-partial-disablement-of-the-work-prism-the-beacon-frame.
transmediale. 2015. “Festival Theme.” *Transmediale*. https://transmediale.de/content/festival-theme.
transmediale. 2017. “An Ongoing Adventure in Art, Culture and Technology.” *Transmediale*. Accessed June 8. https://transmediale.de/content/an-ongoing-adventure-in-art-culture-and-technology.
Ullman, Richard H. 1983. “Redefining Security.” *International Security* 8 (1): 129–53. doi:10.2307/2538489.
United Nations General Assembly. 2016. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. New York: United Nations.
Valverde, Mariana, and Michael Mopas. 2004. “Insecurity and the Dream of Targeted Governance.” In *Global Governmentality*, edited by Wendy Larner and William Walters, 233–50. London & New York: Routledge.
van den Dorpel, Harm. 2016. “Deli Near Info.” *Harm van den Dorpel*. Accessed April 11. http://harmvandendorpel.com/deli-near-info.
Van Tomme, Niels. 2009. “Seeing Things: Trevor Paglen Talks About the Art of Documenting That Which Does Not Want to Be Documented.” Edited by John Feffer. *Foreign Policy in Focus*. April 16. http://fpif.org/seeing_things/.
Vandermotten, Christian, and Julien Vandeburie. 2005. *Territorialités et Politique*. Bruxelles : Éditions de l’Université de Bruxelles.
Vogel, Klaus A. 2011. “Fra Mauro and the Modern Globe.” *Globe Studies*, no. 57/58: 81–92.
Wachter, Christoph, and Mathias Jud. 2018. “Qaul.Net — قول.” *Qaul.Net*. http://qaul.net/index.html.
Waever, Ole. 1995. “Securitization and Desecuritization.” In *On Security*, edited by Ronnie Lipschutz, 46–86. New York: Columbia University Press.
Wagenknecht, Addie. 2015. “Addie Wagenknecht.” *Placesiveneverbeen.com*. Accessed October 29. http://placesiveneverbeen.com/.
Wagenknecht, Addie, ed. 2014. *Deep Lab*. New York: Frank-Ratchye STUDIO for Creative Inquiry; CyLab Usable Privacy and Security Laboratory.
Walker, R B J. 1993. *Inside/Outside: International Relations as Political Theory*. Cambridge: Cambridge University Press.
Walker, R B J. 2006. “Lines of Insecurity: International, Imperial, Exceptional.” *Security Dialogue* 37 (1): 65–82. doi:10.1177/0967010606064137.
Walt, Stephen M. 1991. “The Renaissance of Security Studies.” *International Studies Quarterly* 35 (2): 211–39.
Walters, William. 2012. *Governmentality: Critical Encounters*. New York: Routledge.
Walters, William, and Anne-Marie D’Aoust. 2015. “Bringing Publics into Critical Security Studies: Notes for a Research Strategy.” *Millennium-Journal of International Studies* 44 (1): 45–68. doi:10.1177/0305829815594439.
Waltz, Kenneth N. 1979. *Theory of International Politics*. New York: McGraw-Hill.
Waltz, Kenneth N. 1999. “Globalization and Governance.” *PS: Political Science and Politics* 32 (4): 693–700.
Warner, Michael. 2002. *Publics and Counterpublics*. New York: Zone Books.

Weaver, Matthew. 2009. “G20 Protesters Blasted by Sonic Cannon.” *The Guardian*. October 19. http://www.theguardian.com/world/blog/2009/sep/25/sonic-cannon-g20-pittsburgh.
Weber, Cynthia. 2006. *Imagining America at War: Morality, Politics and Film*. London: Routledge.
Weber, Cynthia, and Mark J Lacy. 2011. “Securing by Design.” *Review of International Studies* 37 (03): 1021–43. doi:10.1017/S0260210510001750.
Weber, Jutta. 2016. “Keep Adding. On Kill Lists, Drone Warfare and the Politics of Databases.” *Environment and Planning D: Society and Space* 34 (1): 107–25. doi:10.1177/0263775815623537.
Weiss, Thomas G. 2004. “The Sunset of Humanitarian Intervention? The Responsibility to Protect in a Unipolar Era.” *Space and Culture* 35 (2): 135–53. doi:10.1177/0967010604044973.
Weldes, Jutta. 1999. *Going Cultural: Star Trek, State Action, and Popular Culture*. Vol. 28. Millennium-Journal of International Studies.
Weldes, Jutta. 2003. “Popular Culture, Science Fiction, and World Politics: Exploring Intertextual Relations.” In *To Seek Out New Worlds: Science Fiction and World Politics*, edited by Jutta Weldes, 230. New York: Palgrave MacMillan.
Weldes, Jutta, and Christina Rowley. 2015. “So, How *Does* Popular Culture Relate to World Politics?” In *Popular Culture and World Politics: Theories, Methods, Pedagogies*, edited by Federica Caso and Caitlin Hamilton, 11–34. Bristol: E-International Relations Publishing.
Wendt, Alexander. 1992. “Anarchy Is What States Make of It: The Social Construction of Power Politics.” *International Organization* 46 (02): 391–425.
Wilk, Elvia. 2015. “Transmediale 2015: Why We Need Spaces for Art and Tech Beyond Corporate Influence.” *Rhizome*. February 18. http://rhizome.org/editorial/2015/feb/18/transmediale-2015-capture-all/?ref=nwslettr.
Williams, M J. 2008. “(In)Security Studies, Reflexive Modernization and the Risk Society.” *Cooperation and Conflict* 43 (1): 57–79. doi:10.1177/0010836707086737.
Williams, Michael C. 2003. “Words, Images, Enemies: Securitization and International Politics.” *International Studies Quarterly* 47 (4): 511–31.
Williams, Michael C. 2007. *Culture and Security: Symbolic Power and the Politics of International Security*. New York; London: Routledge.
Williams, Michael C, and Keith Krause. 1997. “Preface: Toward Critical Security Studies.” In *Critical Security Studies: Concepts and Cases*, edited by Keith Krause and Michael C Williams, vii—xxiv. New York: Routledge.
Winner, Langdon. 2006. “Technology Studies for Terrorists: a Short Course.” In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 275–91. New York: Routledge.
Writers Against Mass Surveillance. 2013. “A Stand for Democracy in the Digital Age.” *Change.org*. December 10. https://www.change.org/p/a-stand-for-democracy-in-the-digital-age-3.
Yadron, Danny, Spencer Ackerman, and Sam Thielman. 2016. “Inside the FBI’s Encryption Battle with Apple.” *The Guardian*. February 18. http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.
Yang, Robert. 2015. “Cobra Club as Ouroboros.” *Radiator*. May 28. http://www.blog.radiator.debacle.us/2015/05/cobra-club-as-ouroboros.html.

Yu, Peter K. 2003. “The Neverending ccTLD Story.” *SSRN Electronic Journal*. Cardoso Law School Public Law Research Paper. doi:10.2139/ssrn.388980.
Zer-Aviv, Mushon. 2015. “Mushon.com | Dissing Information.” *Mushon.com*. Accessed October 29. http://mushon.com/.
Zhong, Peng. 2017. “Opt Out of Global Data Surveillance Programs Like PRISM, XKeyscore, and Tempora.” *Prism Break*. May 3. https://prism-break.org/en/.
Zimmer, Tobias, and David Ebner. 2017. “Database.” *Database-Installation.com*. Accessed December 11. http://www.database-installation.com/.
Zuboff, Shoshana. 2015. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30 (1): 75–89. doi:10.1057/jit.2015.5.
Zureik, Elia, and Mark B Salter, eds. 2005. *Global Surveillance and Policing*. Portland, OR: Willan Publishing.
Zwitter, Andrej. 2014. “Big Data Ethics.” *Big Data & Society* 1 (2): 1–6. doi:10.1177/2053951714559253.
2012a. “Breaking with Consensus Reality, From the Politics of Consent to the Seduction of Revolution.” *CrimethInc.* http://crimethinc.com/texts/recentfeatures/breakwith.php.
2012b. “NSA Possible Domestic Interception/Collection Points Map.” *Public Intelligence*. April 25. https://publicintelligence.net/nsa-domestic-collection-points/.
2015. “Newly Disclosed N.S.a. Files Detail Partnerships with at&T and Verizon.” *The New York Times*. August 15. https://www.nytimes.com/interactive/2015/08/15/us/documents.html.
2016a. “From Democracy to Freedom.” *CrimethInc.* March 16. https://crimethinc.com/2016/04/29/feature-from-democracy-to-freedom.
2016b. “Occupy : Democracy Versus Autonomy.” *CrimethInc.* April 14. https://crimethinc.com/2016/04/14/occupy-democracy-versus-autonomy.
2017a. “Google Earth.” *Google Earth*. https://www.google.com/intl/fr/earth/.
2017b. “Homo Digitalis.” *Arte*. https://www.arte.tv/en/videos/RC-015228/homo-digitalis/.
2018. “About CrimethInc..” *CrimethInc.* https://crimethinc.com/about.