TOOLS OF RESISTANCE OR REPRESSION?

Analyzing the use of the Internet by dissidents and dictators in authoritarian countries

Kieran Bergmann
Major Research Paper
GSPIA
4777076
Supervisor: David Zussman

There are now over two billion Internet users worldwide and it has become one of the most powerful instruments for increasing transparency in the conduct of the powerful and for allowing citizens to exercise their right to freedom of expression and opinion.[1] The potential of cyber space to eliminate traditional power structures is particularly important for populations living under repressive governments and authoritarian regimes. In these countries, dictators keep tight control over information, ideas and opinion and citizens often lack adequate spaces to criticize the government, express dissenting views, or worse, are punished for attempting to do so. The Internet, however, makes it much more difficult for governments to maintain control over its citizens, as its "inherent value and power comes from the fact that it is globally interoperable and decentralized, so that everybody can add to the network and create products, services, and platforms on top of it without having to obtain permission or license, or some kind of access code, from anybody in particular".[2] Many of the tools of the Internet, including blogs, social networking platforms, photo and video sharing tools and mobile technologies, can create an alternate arena for citizens to exercise their right to freedom of expression, disseminate information within and beyond their borders, and create networks of like-minded people. The political power of the Internet is not lost on dictators and authoritarian governments, however, and they have become very aware that it is threatening their ability to control their populations. These governments are therefore becoming ever more adept at using the Internet for their own nefarious purposes—to stifle free speech, repress dissent, and track, monitor and arrest threats to the persistence of their rule.

---

[1] Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," *Human Rights Council*, Seventeenth Session, no. Agenda Item 3 (16 May 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[2] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle Internet Freedom*, (New York: Basic Books, 2012), chap. 2.

The Internet has played an important role in opposition and protest movements movements in a number of authoritarian regimes in recent years. In the fall of 2007, for example, monks, students, political activists and regular people took to the streets in Burma to protest the rule of the military junta. Footage of the protests was captured on camera phones and posted to blogs or smuggled out of the country using Google Chat. During the uprising that erupted in the wake of fraudulent elections in Iran in June 2009, dramatic videos of the protests appeared on YouTube in almost real time, and Iranians tweeted reports and photos of the government's brutal crackdown.[3] Both of these would-be revolutions were violently suppressed by the governments, however, and the evidence to support the role that the Internet played in organizing and mobilizing support for the protests is anecdotal at best. In the winter of 2010 and 2011, however, the Internet was used in unprecedented ways to organize opposition movements in Tunisia and Egypt. Ultimately, these movements reached their goals and led to the ousting of long-standing dictators in both countries, largely because of their ability to harness the power of the Internet. The Arab Spring, as it has been called, then sparked movements in other countries in the Arab World, including Libya, Syria, Bahrain and Yemen, with varying degrees of success. The willingness and ability of the authoritarian governments in these countries to use the Internet to repress these movements, which seems to be increasing with each protest, has been a huge determinant of their success. The Arab Spring thus provides ideal case studies for this paper.

This paper will first analyze the ways in which the Internet and its most politically inclined tools can and have been utilized for the purposes of bolstering offline

[3] "Iran's Twitter revolution." *The Washington Times*, June 16, 2009. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.

opposition movements in authoritarian regimes. It will then proceed to demonstrate these uses by drawing on examples from the so-called Arab Spring, and particularly the revolutionary movements in Tunisia and Egypt, which were ultimately successful in employing these tools to help them reach their goals. Next, it will investigate the ways in which authoritarian governments use Internet technologies in order to censor, monitor and track opponents to their regimes, providing specific examples from Arab Spring countries. Ultimately, the paper will determine that the Internet can provide powerful tools for both opposition movements and authoritarian governments. As power continues to be contested in cyberspace, the international community must take steps to develop a free and open, yet secure Internet by developing a code of conduct for the use of the Internet by governments, strengthening the private sector's role in maintaining the freedom of the Internet by developing standards for international companies, and taking steps to reduce the digital divide. Doing so will help to shift the balance of power in favour of the citizens who would use the Internet legitimately, and out of the hands of those who would use it as a tool of repression or crime.

The Internet provides a powerful avenue for individuals to exercise many of their fundamental human rights, particularly freedom of expression and opinion, as outlined in Article 19 of the Universal Declaration of Human Rights. By protecting freedom of expression "through any medium regardless of frontier", the UDHR was actually quite farsighted in its prescriptions, and extended its protections to technologies that had not yet been invented when it was adopted in 1948.[4] Individuals should therefore be able to receive and convey information freely over the Internet, subject only to limitations that

[4] "The Universal Declaration of Human Rights," Accessed July 22, 2012. http://www.un.org/en/documents/udhr/.

would also be deemed legitimate by the international community offline—for example, the restriction of child pornography to protect the children's rights, hate speech to protect the rights of affected communities or incitement to commit genocide or ethnic cleansing.[5]

With the growth of social media and other associational tools that promote the creation of networks and online communities, the Internet is also being increasingly recognized as a way to promote freedom of association and assembly. It is also an enabler of many other rights, including economic, social and cultural rights, "such as the right to education, and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications".[6] This notion of "freedom of the Internet" also denotes the right to be free from something—government surveillance, censorship or arbitrary arrest based on online activities.

There is also a more contested notion of "freedom via the Internet", which asserts that the free flow of information and the increased collaboration between citizens that is associated with online freedom can translate into more freedom offline.[7] The Internet and associated communications technologies can therefore be powerful driving forces for democracy and human rights, and a potential tool to counter authoritarianism, if they are in the right hands. Of course, there is no direct causal relationship between Internet access or use and democratization or the fall of authoritarianism, and the relationship between these factors are complex. What remains important, however, is that dissidents and dictators around the world are acting as if this relationship exists and is important, and in response the ways in which opposition movements organize themselves, and the

[5] Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression".
[6] ibid.
[7] ibid.

ways in which governments respond to dissent, have fundamentally changed.[8] The notion of "freedom via the Internet" therefore has traction, and tools such as social networking platforms, blogs and mobile technologies will likely become more vital and prevalent tools in the belts of dissidents and dictators alike.

THE TOOLS

The surge in Internet use in the decade leading up to the Arab Spring—from 390 million in 2000 to over two billion in 2011—also brought with it an influx of new Information Communication Technologies (ICTs) and the creation of a second generation of web technologies, often referred to as Web 2.0.[9] These technologies are more collaborative and interactive, and facilitate the creation and dissemination of user-generated content. Users are able to easily and rapidly create and share content, and interact other people in their existing offline networks, or build new networks entirely, regardless of their actual physical location. As such, many of these tools have been adopted by civil society groups and opposition movements who use them to inform, mobilize and organize networks of like-minded people.

Blogs:

A blog is a website that acts as an online journal or opinion space where an author can share information and invite others to participate in an online dialogue. There are currently over 200 million blogs worldwide, with more than 900,000 new blog posts catalogued each day.[10] Blogs are inherently democratic and have led to the formation of an interconnected public space where every individual with access to a computer can

[8] Sheetal D. Agarwal, Philip N. Howard, and Muzammil M. Hussain, "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?," Issues in Technology Innovation, no. 13 (2011): 3.
[9] "Information and Communication Technology Statistics," Last modified July 16 2012, http://www.itu.int/ITU-D/ict/.
[10] "BlogPulse Stats," Accessed July 22, 2012, http://blogpulse.com/.

participate. This is fundamentally different from the top-down, hierarchical character of traditional media, such as newspapers and broadcast media, in which the public is told what the news is by an elite group of reporters.[11]

In the blogosphere, regular people, often referred to as citizen journalists or netizens, determine the news agenda by writing journals, producing videos and investigating and reporting on political, social and other issues. In countries where this type of content might be deemed sensitive or illicit, and strictly controlled by the government, blogs "have created new spaces, outside of society, where political discussion (is) relatively safe".[12] Here, citizen journalists can cover events and issues that the government-controlled, mainstream media cannot. As a tool of information publication and dissemination, blogs can also be used for coordination and organization purposes. The ease of use means "individuals who have no expertise in computer programming and HTML editing can very easily update their blogs, opening Web publication to a wide audience".[13] It is no surprise, then, that dissidents and activists have been particularly drawn to blogging. It is also of no surprise that bloggers are increasingly the targets of censorship, surveillance and arrest.

Social networking platforms:

The Internet is now home to a multitude of social media technologies, which allow normal citizens to create and share content, develop networks of like-minded

[11] Daniel Calingaert, "Authoritarianism vs. the Internet," Policy Review, no. 160 (2010): 66.

[12] Jillian York, "The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution," Language, Identity & Politics, 13, no. 1 (2012): 34, http://jilliancyork.com/wp-content/uploads/2012/02/33-42-FORUM-York.pdf.

[13] Ronald Deibert, and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (Cambridge: The MIT Press, 2008), 136.

people and collaborate with other users.[14] The decentralized and participatory nature of these tools allows organizers of protest and opposition movements to move away from the more traditional hierarchical organization towards a more horizontal and networked organization that is more conducive to their goals. They are instantaneous, which allows news, images and information to reach a critical mass of people within minutes or hours. This is often referred to as "going viral". They are also visual, allowing the images and videos of the stifling of dissent or the abuse of government power to travel within and beyond borders, making the situation more real for individuals who may not be able to see it with their own eyes. Moreover, they facilitate collaboration and the building of networks and communities around a shared cause or vision.[15]

Facebook, a social networking service that allows users to create a profile, connect with 'friends', exchange messages, share links and photos, stream videos and provide updates, opened up to everyone over the age of thirteen with a valid email address in September 2006.[16] It is now available in more than seventy languages to over 901 million monthly active users, eighty percent of whom are located outside of the United States and Canada.[17] Originally envisioned for purely social and entertainment purposes, it has developed many political uses not initially anticipated by its creators. The addition of features such as 'Groups' and 'Events' has allowed it to be used as a

---

[14] Calingaert, "Authoritarianism vs. the Internet," 67.

[15] Brian Keeter, "The internet equalizer: Why isn't the Obama administration doing more to promote social media?," Foreign Policy, September 28, 2011, http://shadow.foreignpolicy.com/posts/2011/09/28/the_internet_equalizer_why_isn_t_the_obama_administration_doing_more_to_promote_soc.

[16] York, "The Arab Digital Vanguard," 35.

[17] Facebook, "Key Facts," Last modified March 31 2012, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

community-organizing platform to mobilize protest movements.[18] It can be used to share important information to a particular group of individuals during protests, such as the location of police, tips for protesters or where they can find health or legal services. It can also be used to disseminate reports of government and police abuses, such as the arrests of dissidents.

The microblogging social networking site Twitter also launched worldwide in 2006, and quickly became a primary source of news for many people.[19] Currently, more than 140 million active users regularly send and receive text-based posts, or "tweets" of up to 140 characters over the platform.[20] It has been an incredibly powerful tool for opposition movements who have used it to disseminate and receive news, galvanize support and mobilize the masses. The ability to "retweet" has amplified dissident voices the world over.

Twitter's political applications were also unanticipated, but its founders have embraced this responsibility. A statement on the website reads, "We believe that the open exchange of information can have a positive global impact. Everyday we are inspired by stories of people using Twitter to help make the world a better place in unexpected ways".[21] Originally envisioned as a vanity project where users would share the intricacies of their lives with friends and acquaintances, "five years after it's founding, Twitter has hit a critical mass of activists, casual observers on the ground, journalists in the office and

[18] York, "The Arab Digital Vanguard," 35.
[19] Ibid.
[20] Twitter, "About Us." Accessed July 22, 2012. https://twitter.com/about/.
[21] Ibid.

in the field, and analysts behind their desk".[22] To reflect this change, Twitter in 2009 changed its prompt from "what are you doing" to "what's happening".[23]

These days Twitter's uses have expanded to include organizing protests and disseminating news and information about opposition movements to local participants and observers around the world. The creation of 'hashtags' in August 2009, which allow users to aggregate information by adding a short word or phrase preceded by '#' in their tweets, really facilitated this organization application.[24] Groups of individuals now had a hub of information on a particular issue, and could provide all pertinent information in one place (such as the location of protests). Additionally, Twitter has been used as a real time breaking news forum, and as an emergency communication system.

Photo and Video sharing

Photo and video sharing sites have also been touted for their ability to act as a tool for protesters and opposition movements in authoritarian countries. YouTube, the most well known and widely used of these sites, allows users to upload, view and share video content, including movie and television clips, music videos and vlogs (video blogs). It was created in 2005, and currently seventy-two hours of video are uploaded every minute.[25] Activists and opposition movements post videos on YouTube that exhibit the abuse and repression that their fellow citizens suffer at the hands of government officials and police officers in the hopes that posting their videos will publicize and garner support for their cause, and deplete the support of the government. Often, these videos are picked up by major media outlets and broadcast around the world.

---

[22] Blake Hounshell, "The Revolution Will Be Tweeted," *Foreign Policy*, July/August 2011. http://www.foreignpolicy.com/articles/2011/06/20/the_revolution_will_be_tweeted?page=0,1.
[23] ibid.
[24] York, "The Arab Digital Vanguard," 35.
[25] YouTube, "Statistics," Accessed July 22, 2012. http://www.youtube.com/t/press_statistics/.

Mobile technology

Approximately eighty-six percent of people in the world have mobile subscriptions, many of whom access the Internet from their phones.[26] Smart phone applications allow people to instantly update their blogs, post to Facebook and Twitter, upload videos to YouTube and share photos with their networks. Using SMS (short message service) is incredibly cheap and easy, and has been embraced by people of all ages and in all parts of the world. In fact, in 2010 roughly 200,000 texts are sent every second.[27] The ease of use and accessibility of mobile phones has made it particularly useful in countries with higher poverty levels where people are unlikely to have a personal computer but most likely have a mobile phone, and which lack sufficient infrastructure and access to basic services, such as electricity.[28] They have become a key tool for organizing, particularly in these countries, as they provide users the ability to update their networks in real time. Protesters, for example, can instantaneously text updates, send photos or video and post updates to their blogs or social networking profiles from the middle of a demonstration. YouTube has a huge mobile platform, with three hours of video being uploaded from mobile devices every minute.[29] Fifty-five percent of Twitter users access the service on their mobile phones, and Facebook has over five hundred million mobile monthly active users.[30]

THE INTERNET AND THE ARAB SPRING

[26] International Telecommunications Union, "Information and Communication Technology Statistics"
[27] ibid.
[28] Digital Buzz Blog (blog), January 3, 2012, http://www.digitalbuzzblog.com/social-media-statistics-stats-2012-infographic/.
[29] YouTube, "Statistics".
[30] Facebook, "Key Facts".

The defining characteristics of the Internet, social media and mobile technologies—accessible, easily used, decentralized and relatively cheap—make them ideal tools for opposition movements, which are generally horizontal networks of like-minded people, uniting over a common cause. In authoritarian regimes in particular, these technologies have been used to push the limits on freedom of expression, association and information set by repressive governments. In many of these contexts the restrictive environment that journalists, dissidents and activists encounter offline have not yet been fully extended to cyberspace, either because governments do not fully realize the potential political power of these tools, or because they do not yet have the technical skills or resources to counter their opponents in cyberspace.

This was precisely the environment that Tunisians and Egyptians found themselves in when they took to the streets last winter. While the long-standing regimes in both countries kept close tabs and a tight leash on the traditional media, they largely underestimated the problems that the Internet could cause for the persistence of their rule. To be sure, they did make efforts to control the spread of information on the Internet, particularly when it came to censoring vocal activists and dissidents who had long been active offline as well as on. Yet the Internet provided a more open and free space to exercise their freedoms of expression, association and assembly. In 2009, Freedom House gave both Tunisia and Egypt a better rating for Internet freedom than they did for overall media freedom.[31] As the Arab Spring events unfolded, it became clear that the Tunisian and Egyptian governments did not fully grasp the ability of the Internet, and particularly the Web 2.0, to mobilize and organize mass amounts of citizens. The Internet allowed

[31] Freedom House, "Middle East and North Africa," Accessed July 22, 2012. http://www.freedomhouse.org/regions/middle-east-and-north-africa.

huge networks of citizens, sharing a common resentment and anger towards their governments, to develop right under their noses.

The Tunisian and Egyptian revolutions provide excellent examples of the ways in which the Internet and social media can be harnessed by opposition movements to challenge the status quo in authoritarian countries. The revolutionaries employed all of the political uses of the Internet outlined in the previous section, and developed new and innovative ways that had not previously been imagined. They created revolutionary content on their mobiles and digital media, and distributed this content to friends, families and various networks. Through social media and blogs this content reached the mainstream media and drove the international news agenda. Mobile phones ensured that information about the location of protests or other important information reached those without access to the Internet in these countries, as did some mainstream media such as Al-Jazeera.[32] Not surprisingly, the first reports of the Arab Spring touted the power of the Internet and social media in fueling the uprisings in Tunisia and Egypt. Headlines around the world read, "Revolution 2.0", Tunisia's Social Media Revolution", "In Egypt, pushing revolution by Internet".

A movement of this magnitude can not be solely attributable to one factor or tool, yet the Internet and its rapid, popular spread has allowed like-minded individuals in these two countries to network at a scale and scope not previously possible. The activists in Egypt and Tunisia had a long history of online collaboration that spanned a decade, and their expertise in digital activism gave them a distinct advantage over the governments they contended with. While the solidarity of networks has historically challenged

[32] Alula Berhe Kidani, Alula, "The Arab Spring and the Role of ICTs," *Sudan Vision Daily*, July 22, 2012. http://news.sudanvisiondaily.com/details.html?rsnpid=211636.

dictators around the world, Tunisia and Egypt provide the first example of an opposition movement bolstered by the Internet and social media, leading to "revolutionary changes to long-established political authority".[33]

The use of the Internet and social media to mobilize support, organize protests and disseminate information is, by itself, neither a necessary nor a sufficient cause of opposition movements, nor a determinant of their success. Indeed, as many countries around the world still have very limited access to these technologies, it is certainly possible that an opposition movement could occur without the use of the Internet at all (although it may not happen as fast as the Tunisian and Egyptian cases[34]). When social media does play a role, it always interacts with other factors, be they political, economic or cultural. It cannot be stressed enough how important the ways in which these variables interact within each unique context are. The levels of unemployment, poverty, government corruption, resentment towards the government, and timing that had already been devoted to cultivating networks—to name a few—are all critical factors that may determine whether a movement will develop in the first place, and how successful it will be. In Tunisia and Egypt, for example, high levels of poverty and unemployment, state repression, and state violation of many rights and freedoms, as well as the use of the Internet and social media, were all factors contributing the uprisings there.[35]

The Internet, and the opportunities it created, were, however, absolutely crucial in aiding and facilitating the building of activist networks. Without this new, novel tool of organization, governments would have been able to continue their control and dominance over civil society and bar all group association and cohesion. Social media empowered

[33] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 123.
[34] Howard, "A Tunisian on the role of social media in the revolution in Tunisia"
[35] Ghafour, "Enough! Why thousands of young Arabs have taken to the streets in protest"

individual, isolated dissenters by creating a platform to voice their grievances and reach out to other like-minded citizens, while also tapping into the unvoiced desire for change within the broad public. The Arab Spring unfolded because social media was a tool for citizens to challenge traditional power structures and unleash a democratic wave across the region.

Tunisia

On December 17 2010, images and video of a young Tunisian street vendor setting himself on fire began to spread across various digital channels. Mohamed Bouazizi's act of protest was prompted when police officers confiscated his vegetable cart, and was a reflection of the widespread frustration with the pervasive corruption, high unemployment and rising inflation rates in the country.[36] Prior to this catapulting event, the Tunisian opposition movement had been largely underground, but the images of this young man taking his own life went viral, spreading to thousands of people in a few short hours. In addition, in late November and early December, nine Wikileaks cables from the US Embassy in Tunis were released, which further confirmed what Tunisians already knew about their longstanding leader and his closest allies in government and the business community. They detailed the corruption, nepotism and financial mismanagement of the regime, likening the ruling family to the mafia.[37] Descriptions of the protests as the first-ever "Wikileaks revolution" are an exaggeration, but the leaked cables combined with Bouazizi's self-immolation certainly stoked the fires of discontent that had long existed in the country. A movement of Tunisians around the country, who

[36] Hamida Ghafour, "Enough! Why thousands of young Arabs have taken to the streets in protest," *The Globe and Mail*, May 6, 2011. http://m.theglobeandmail.com/news/world/enough-why-thousands-of-young-arabs-have-taken-to-the-streets-in-protest/article578874/?service=mobile.
[37] Elizabeth Dickinson, "The First WikiLeaks Revolution?," *Foreign Policy*, January 13, 2011. http://wikileaks.foreignpolicy.com/posts/2011/01/13/wikileaks_and_the_tunisia_protests.

shared Bouazizi's distrust and anger towards President Zine El Abidine Ben Ali's government, was energized and mobilized and eventually began calling for an end to the twenty-four year rule of Ben Ali's regime.

The roots of the revolution began long before that fateful December day. In 2010, when the country erupted in protest, 36.56 percent of Tunisians were using the Internet.[38] Nineteen years earlier, in 1991, Tunisia had become the first Arab country to connect to the Internet, and five years later the public was granted access, leading to a relatively quick rise of Internet penetration rates.[39] The government almost instantly began its attempts to control the Internet with the institution of L'Agence Tunisienne d'Internet, or ATI, cunning activists also quickly began to use the Internet to counter government propaganda and carve a political space for themselves. A vibrant blogosphere began to emerge in 2000, which provided many Tunisians with an arena to discuss many of the issues that mainstream journalists could not hope to touch because of the stifling controls the government placed on them. The Internet realm did not remain untouched, however, and on the fourth of June 2000, "Tunisia became the first country to arrest a blogger….Zouhair Yahyaoui, the creator of TUNeZINE, was arrested after initiating an online poll inviting readers to vote on whether Tunisia was 'a republic, a kingdom, a zoo, or a prison'".[40]

In 2004, a group blog called Nawaat was developed, which endeavored to inform Tunisians about abuses carried out by Ben Ali's regime, government censorship and their

[38] Google, "Internet users as percentage of population, Egypt" Last modified July 13 2012, http://www.google.ca/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:TUN&dl=en&hl=en&q=internet+users+as+percentage+of+population+tunisia

[39] York, "The Arab Digital Vanguard," 33.

[40] York, "The Arab Digital Vanguard," 37.

human rights.[41] As new social networking tools began to emerge in the digital realm, Nawaat's contributors and other activists co-opted them for their own purposes. Google Maps, for example, was used to create a "Tunisian Prison Map," which provided a visualization of the massive amounts of political prisoners in the country.[42] Yet, always the relentless foe, the government continued its impressive campaign of suppressing dissent over the Internet, and "by the late 2000s Tunisia had become among the worst in the world in respect to online censorship, surpassing other authoritarian states such as Syria".[43] Despite this, in 2005, Tunisia hosted the World Summit on the Information Society, which brought together policymakers, journalists, non-governmental organizations, academics and the private sectors to try to develop a shared vision for the future of Internet governance. Ironically, however, as the participants of the Summit ideals of a free and open Internet, Tunisians trying to access online information about human rights or view websites critical of the Summit view information critical of the Summit found that they were blocked.[44]

Despite the sophistication and pervasiveness of the Tunisian government's censorship and controls of the Internet, in December 2010, it became a primary tool to organize, mobilize and disseminate information about the protests against Ben Ali's regime. With two million active Facebook users in the country, approximately five hundred active Twitter accounts, and eighty-five percent of the population with mobile

[41] MacKinnon, *Consent of the Networked*, chap. 2.
[42] Ibid, chap. 2.
[43] York, "The Arab Digital Vanguard," 37.
[44] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 123.

phones, revolutionaries found in these tools a powerful ally.[45] Facebook acted as the primary organizing tool, where organizers would post pertinent information about the times, locations and activities of the protests. Twitter became the real-time venue to share stories and information from the field, with many people tweeting in the streets from their smart phones. Tweets extended beyond borders, helping the movement gain support regionally and internationally. Mobile phones were used to document the revolution, taking photos and videos that were almost instantly uploaded to YouTube, shared on Facebook and Twitter, or aggregated on Nawaat.org.[46] In the face of Ben Ali's escalation of censorship of the press and a smear campaign against international media outlets such as Al-Jazeera, these technologies became the source of news worldwide, and it was not uncommon for YouTube videos posted by protesters to turn up on the BBC or CNN.[47]

These uses, however, are fairly common and predictable applications of these tools. More likely it was the more innovative uses that helped shift the power out of the hands of the government and into the hands of the protesters. Tunisians used social media tools to "identify the positions of snipers, police and looters, and to alert one another to other violence".[48] Online communities that were formed also organized groups of citizens to clean the streets, protect shops and organize bread lines during the tumultuous time.[49] Another key use was to counter government propaganda and rumours that were being disseminated to keep people out of the streets. For example, news of a shooting in a

[45] Colin Delany, "How Social Media Accelerated Tunisia's Revolution: An Inside View." *The Huffington Post*, February 10, 2011. http://www.huffingtonpost.com/colin-delany/how-social-media-accelera_b_821497.html.
[46] MacKinnon, *Consent of the Networked*, chap. 2
[47] Bassam Bounenni, "The limits of silencing Tunisia," *Foreign Policy*, January 12, 2011, http://mideast.foreignpolicy.com/posts/2011/01/12/the_limits_of_silencing_tunisia.
[48] Alex Howard, "A Tunisian on the role of social media in the revolution in Tunisia," *Gov2.0* (blog), January 30, 2011, http://gov20.govfresh.com/a-tunisian-on-the-role-of-social-media-in-the-revolution-in-tunisia/.
[49] ibid.

neighbourhood was quickly dispelled as untrue over social media by dozens of people who were in the area at the time.[50] Finally, social media was used as a way to form common positions on government negotiations and offers. Any announcement or offer made by the Ben Ali government was analyzed and debated online by the protesters to ensure that any responses or discussions with the government were agreed upon.[51] Ultimately, the consensus was drawn that the only acceptable outcome was the stepping down of Ben Ali—a goal that was reached on January 14, 2011.

Egypt

This innovative use of the Internet extended beyond borders as news of the Tunisian revolution quickly spread over the Internet across the region. Egypt in particular, whose youth groups and activists had a long history of online collaboration with their Tunisian counterparts, began to take on a revolutionary fervor of its own. Bloggers began writing about their revolutionary goals and many normal Egyptians flocked to Twitter and Facebook to first witness history in Tunisia and then begin planning their own protests. The hashtag #Jan 25 was created to raise awareness of the protests that would occur on January 25, and then became a forum for the multitude of live tweets coming out of the protests around the country.[52] People around the world began following updates from Egypt in real-time over social media, and news organizations began to rely on these forums for their reports.

As in Tunisia, the roots of the movement that lead to the ousting of President Hosni Mubarak on February 11 2011, can be traced back to the rise of the Internet in the country. In 2010, 26.74 percent of Egyptians were using the Internet. Ten years earlier,

[50] ibid.
[51] ibid.
[52] York, "The Arab Digital Vanguard," 37.

when Egyptians began migrating online, that number was only 0.64 percent.[53] Yet, the potential of the Internet to provide a forum for discussion around issues not otherwise tolerated in the country was quickly realized by many, and a vibrant community of bloggers began to emerge in the country. By 2005, Egypt was at the helm of the Arab blogosphere with over 1,500 bloggers.[54] Many of these were activists in the traditional sense who found a new outlet for their political activities on the Internet. Political activists, for example, took to blogs to publicize the arrests of their colleagues and unveiled the brutal acts of torture that were common practices of Mubarak's police force.[55] With the creation of social media technologies, another channel was found, one that allowed for more dynamic collaboration. Facebook, in particular, has been a key tool for young Egyptians wishing to see change in the status quo. In a country with a population of 84.5 million, an estimated 3.4 million of them were on Facebook by mid-2010—more than any other country in the Arab world.[56]

On March 23, 2008, two young Egyptians, Ahmed Maher and Ahmed Salah, began a Facebook group to galvanize support for a worker's strike that was planned for April 6 to protest low wages and high food prices. The group—the April 6 Movement—attracted 3,000 members overnight, and by the end of the month had over 40,000 members.[57] Member of the Facebook group used the platform to organize the logistics of a nationwide general strike, report on the activities of the day and alert strikers of police

[53] Google, "Internet users as percentage of population," Last modified July 13 2012, http://www.google.ca/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:EGY&dl=en&hl=en&q=egypt internet users.

[54] York, "The Arab Digital Vanguard," 34.

[55] MacKinnon, *Consent of the Networked*, chap. 2.

[56] Ibid, chap. 10.

[57] David Wolman, "Cairo Activists Use Facebook to Rattle Regime," *Wired Magazine*, October 20, 2008. http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?currentPage=1.

activity.[58] After the strikes on April 6, the Facebook group and many of its members continued to be politically active, publicizing illegal government activities, including the use of torture as a method of interrogation, and police beatings. By March 2011 The April 6 Movement had over 100,000 members on Facebook.[59]

Another Facebook group emerged after a young Egyptian named Khaled Said was arrested and murdered by police, allegedly for posting a video on the Internet that showed police officers profiting from a drug bust. The group, "We are all Khaled Said", was started by an Egyptian Google marketing executive, Wael Ghonim, to educate the public about police brutality and democracy movements. The group often organized protests called "silent stands against torture" in locations around the country, and leading up to the revolution in the winter of 2011, hundreds of thousands of members had joined on Facebook.[60]

When these two groups heard of the uprisings in Tunisia being lead by activists with whom they had collaborated with in the past, they joined with the Youth Organization of the Muslim Brotherhood and supporters of Nobel Prize winner Mohamed ElBaradei, a leading figure of the opposition movement, to form Egypt's "Revolutionary Youth Coalition".[61] They tapped into their online and offline networks to organize a protest of their own on January 25, ironically a holiday marking 'Police Day'.[62] Egyptians who had been watching the events in Tunisia unfold and were angry not only about police violence and the brutality of the Mubarak regime, but also soaring food prices and

[58] ibid.
[59] ibid.
[60] MacKinnon, *Consent of the Networked*, chap. 10.
[61] Sarah A. Topol, "What Happened to My Revolution." *Foreign Policy*, January 24, 2012. http://www.foreignpolicy.com/articles/2012/01/24/what_happened_to_my_revolution?page=0,5.
[62] David D. Kirkpatrick, and David E. Sanger. "A Tunisian-Egyptian Link That Shook Arab History." *The New York Times*, February 13, 2011. http://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?pagewanted=all.

high rates of unemployment, took notice. 100,000 people signed up for the protest on Facebook, where the organizers had set the time and the place of smaller meetings that would march to Tahrir Square.[63] To ensure that a critical mass of people turned up to the protests, the organizers combined their online efforts with offline efforts. They plastered the streets with posters advertising the protests, and passed the information through text messages.

On that fateful day in January, tens of thousands of people marched to Tahrir Square, demanding that Mubarak step down. Mubarak, however, wasn't opposed to a fight, and certainly wasn't willing to bring his thirty year rule to a close in a single day. Police countered the sea of people with tear gas, rubber bullets and shields. This was when the relationships that had been built with Tunisian activists came in handy. Revolutionaries in the two countries communicated via social networking sites, and Tunisians shared the lessons they had recently learned. Messages such as, "Advice to the youth of Egypt: Put vinegar or onion under your scarf for tear gas", were commonly seen on Twitter and Facebook. Eighteen days, 1000 deaths and numerous protests later and Mubarak finally stepped down on February 11, 2011.[64]

The Domino Effect

Clearly, the Egyptian and Tunisian cases are excellent examples of how citizens can harness the potential of the Internet to shift power out of the hands of a repressive government and into the hands of the people. The reason they provide such excellent case studies, however, goes even deeper. As citizens in other countries in the region followed the protests over YouTube, Facebook, Twitter and blogs, they began to organize protest

[63] Ibid.
[64] ibid.

movements of their own and took the lessons they learned from the Tunisian and Egyptian examples to heart. Libya, Bahrain, Yemen and Syria all began to use online forums to discuss their own grievances with their authoritarian governments and the potential for change. This ability of the Internet to spread information regionally, providing a connection between "people who share a common language and relationships to their state, religion and social norms" is one of the most powerful ways in which the Internet can foster opposition or democracy movements.[65] The activists were not the only ones in the region to learn from the Tunisian and Egyptian experience, however. Authoritarian governments in the region began to truly understand the advantage the Internet could provide to its enemies, and began to act accordingly. In many ways they learned what not to do from Ben Ali and Mubarak, and they began to act with a much greater willingness and ability to use the Internet, social media and mobile technologies to repress the emerging opposition movements. Thus, while the revolutions in Egypt and Tunisia were able to harness these tools to successfully achieve their desired ends, the level of success has been varied in the countries that have risen up against their governments since.

THE DARK SIDE OF THE INTERNET

In the early hours of January 28 2011, in an unprecedented and seemingly desperate move, Mubarak's government cut off access to the Internet and mobile networks. Reports have estimated that this shutdown caused between an eighty-eight and ninety-three percent drop in data traffic in Egypt just hours prior to the scheduled "day of

[65] Evgeny Morozov and John Palfrey. "Economist Debates: Internet democracy." *The Economist*, February 23, 2011. http://www.economist.com/debate/days/view/662.

rage"—the largest planned protests of the revolution to date.[66] This significantly hindered the ability of protestors to communicate and organize.

This move on the part of the Egyptian government demonstrates that it is not only the opposition movements themselves that believe the Internet can help bring political and social change, so do the governments that they contend with. Governments with a vested interest in maintaining the status quo are becoming ever more adept at censoring, filtering and monitoring dissent, and tracking down those activists that use the Internet to create problems for their regime. Restrictions on the right of individuals to harness the power of the Internet ranges from the use of technical measures—which can prevent access to content, as in Egypt, monitor users, or manipulate content—to inadequate guarantees of the right to privacy and protection of personal data, or the arbitrary use of criminal law to punish legitimate exercises of freedom of expression. As the battle to gain strategic advantage and relative power in cyber space continues, many governments are demonstrating an ever-increasing desire, willingness and ability to utilize a broad range of tactics to gain the upper hand over their opponents.

Information denial

A complete shutdown of Internet and mobile networks, as occurred in Egypt, is the most brazen and overt approach to information denial that a government can execute. Given the increasing reliance that opposition groups place on the Internet during political protests, it also has the potential to be a very effective one. Moreover, as the majority of authoritarian governments in the world maintain strict control over the communication

[66] Matt Richtel, "Egypt Cuts Off Most Internet and Cell Service." *The New York Times*, January 28, 2011. http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=1.

networks in their countries, it is a very feasible strategy.[67] Although the Egyptian example was "unprecedented in its scope and scale", it is not the first time that a government has employed such a tactic, nor is it likely to be the last.[68] This tactic is often referred to as just-in-time blocking as it occurs only during key moments, such as elections, protests or important anniversaries, when the content that citizens are seeking out may have the greatest political impact and is therefore deemed by governments to be too sensitive for their citizens to view.[69]

Approximately one month after Egypt went offline, the Libyan government intermittently shutdown the Internet on February 18 and 19, and again on March 3 2011, amidst growing political tension in the country.[70] Syria followed suit on June 3 2011, disconnecting two-thirds of Syrian networks from the Internet—the remaining one-third included all government sites—in response to an escalation in revolts and the uproar over the torture and murder of a thirteen-year-old boy.[71] In the latter case, the foreign media had been banned from the country, and the information, photos and videos that revolutionaries posted on YouTube, Facebook and Twitter had become a key source of news inside and outside of the country.[72] The takedown therefore seriously hampered the opposition movement's ability to utilize the Internet and social media to their advantage.

Any significant shutdown of the Internet can have can have damaging economic, diplomatic, political and social consequences and the government must decide whether the benefits of cutting off their enemies primary communication channels will outweigh

[67] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 123.
[68] ibid.
[69] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 144.
[70] The Citizen Lab, "Syrian Internet Shutdown and the Ongoing Militarization and Contestation of Cyberspace." *The Citizen Lab* (blog), June 3, 2011. https://citizenlab.org/2011/06/syrian-internet-shutdown-and-the-ongoing-militarization-and-contestation-of-cyberspace/ (accessed July 22, 2012).
[71] Ibid.
[72] Ibid.

the potential repercussions—the so-called dictator's dilemma.[73] According to the OECD, the Egyptian shutdown cost the economy at least ninety million US dollars.[74] It was also considerably less effective than the government likely hoped it would be. A few "tech-savvy students and civil society leaders had organized satellite phones and dialup connections to Israel and Europe" and they were therefore able to maintain their external communications.[75] In addition, finding themselves cut off from news of the protests and the fates of friends and families, many normal Egyptians simply took to the to the streets to supplement the information that they would have otherwise found online.[76]

Many other governments therefore tend to choose less all-encompassing strategies. Internet filtering and blocking is often employed by governments to restrict freedom of "undesirable" expression and deny access to online information deemed to be too sensitive to view.[77] The content targeted—most often political, cultural, religious or sexually explicit—and scope of filtering ranges from country to country and may be permanent or temporary.[78] The tactics used also vary in their sophistication, effectiveness, cost and stealth. Common methods of filtering include blocking specific IP addresses, websites, or entire domain names, or blocking access to content based on keywords. Keyword filtering can also be used to censor mobile phones, ensuring that text messages with sensitive content are never delivered.[79]

---

[73] Agarwal, Howard, and Hussain, "The Dictators' Digital Dilemma," 1.
[74] OECD, "The economic impact of shutting down Internet and mobile phone services in Egypt," February 4 2011. http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html.
[75] Agarwal, Howard, and Hussain, "The Dictators' Digital Dilemma," 2.
[76] ibid, 3
[77] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 124.
[78] ibid.
[79] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, (New York: PublicAffairs, 2011), 174

More covert tactics are being used increasingly frequently, as they provide the government with plausible deniability. Distributed Denial of Service (DDoS) attacks, for example, overwhelm a targeted site with information requests so that it is no longer able to respond to regular traffic or communicate with its intended users.[80] Such attacks may be particularly appealing to governments who wish to retain their reputations in the international community, as they are difficult to trace and allow the attacker to remain anonymous.[81]

The Syrian government has provided, at the very least, tacit support to a pro-regime group that has become very skilled in the art of DDoS attacks. The Syrian Electronic Army (SEA) has targeted media websites, including Al-Jazeera, BBC News, Orient TV and al-Arabia TV, with a denial of service software known as Bunder Fucker 1.0. It is employed by many people simultaneously as part of a manual DDoS attack.[82] The SEA claims to have chosen these particular targets because off their "biased reporting" on the uprising and hostility towards the Syrian regime. Ironically, however, "pro-revolution hackers have re-purposed the same software" in order to attack pro-regime or government targets.[83]

The OpenNet Initiative, which investigates, exposes and analyzes Internet filtering and surveillance practices around the world, has witnessed a significant increase in the number of countries that actively control online content. There are now more than forty countries around the world that engage in technical filtering of the Internet whereas in 2003, when they began investigating Internet censorship, only a handful of countries

[80] ibid, 107
[81] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 145.
[82] OpenNet Initiative, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets." Accessed July 22, 2012. http://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets.
[83] ibid.

were witnessed.[84] As dictators around the world receive news of the success of opposition movements like those in Egypt and Tunisia, and the methods of information denial become more sophisticated, this number will likely continue to grow.

Information monitoring

The increasing use of the Internet and mobile phones by dissidents and opposition movements has certainly had an amplifying effect on dissent around the world, but the enormous amount of information shared over these networks can be just as valuable to the governments they contend with. "Finding ways to understand and gather information—especially about threats to the regime—is one invariable feature of authoritarian survival".[85] This is one of the reasons why complete shutdowns of communication infrastructures are so rare—allowing a flow of information between citizens provides governments with opportunities to know their enemies through their surveillance and monitoring efforts. Not to mention that surveillance has become more practical in the cyber age—it is cheaper, easier to conceal and can provide infinitely more information than its analog predecessors.[86]

As Syrian President Bashar al-Assad began to hear calls for the end of his eleven-year rule in the wake of Tunisia and Egypt's successful revolutions and the spread of political unrest across the region, the dictator chose a much different path than his counterparts in similar positions. Instead of moving to repress the voices that were emerging online, social media in the country was unblocked on February 9, 2011 for the

[84] ibid.
[85] Morozov, *The Net Delusion*, 107
[86] ibid, 150

first time since 2007.[87] Government hackers then began infiltrating Syrian Facebook users' accounts to gain access to and control over their profiles, allowing them to view their contact lists, networks and event information.[88] As Facebook has a "real name" policy, which is meant to prohibit users from registering with pseudonyms, the information gathered from this attack may have provided the Syrian government with invaluable information about their rivals.

In the era of social media, hacking accounts has become an excellent way for governments to keep one step ahead of their enemies—providing them with location sites of protests and the real names of protesters and their co-conspirators. Governments can also track the habits of their citizens over social media to predict when unrest or a protest may occur, and act preemptively by arresting known dissidents or sending police to popular protest locations (like Tahrir square). If they find citizens to be retweeting a particular activist more than usual, for example, or using the word "democracy" more frequently in their online correspondence, comments and tweets, then they know that it is time to act.[89] Often times they may find that they do not even need to go through the trouble of hacking their accounts—so much of this information is public.

Other popular methods of Internet surveillance include deep packet inspection (DPI) and targeted malware attacks. DPI examines packets of data, searching for viruses, spam or other intrusions in a network. It can also, however, be used to collect statistical

[87] Jillian York, Jillian. "Unblocking Syria's social media." *Al Jazeera*, February 12, 2011. http://www.aljazeera.com/indepth/opinion/2011/02/2011212122746819907.html.
[88] OpenNet Initiative, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets."
[89] Morozov, *The Net Delusion*, 87

information, making it an excellent method of intercepting emails, monitoring content and generally keep an eye on dissidents.[90]

In a targeted malware (malicious software) attack, the target receives an email prompting them to click on a link or open an attachment, which subsequently exploits vulnerabilities on their computer allowing the malware to install. Once the computer is compromised, the assailant essentially has complete control, and can extract documents, email and other data, log keystrokes, take screen shots, and even capture audio and record a web cam's view—all without the victim even knowing their computer has been compromised.[91] The most important step of the attack, however, is the first—the carrier email must be uniquely targeted to each victim to ensure that they open the attachment or click on the link. Attackers have therefore become increasingly sophisticated in their social engineering of these attacks, manipulating the targets network by sending an email from what appears to be a legitimate or trusted source, ensuring the text of the message is targeted to the work or interests of the victim, or even sending invitations to real events.[92] The amount of detail that can be obtained from an attack combined with its relative ease of use and availability (the technology is widely offered online), makes a targeted malware attack an incredibly attractive tactic of cyber espionage for any government desiring to monitor or obtain information from its political enemies. Perhaps even more appealing, attribution is incredibly difficult, as the attacker can utilize a proxy server or compromised computer to hide their true location.[93]

---

[90] Calingaert, "Authoritarianism vs. the Internet,"63.
[91] "Shadows in the Cloud: Investigating Cyber Espionage 2.0," *Information Warfare Monitor* (April 6 2010), http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0.
[92] ibid.
[93] ibid.

Utilizing mobile devices for political activity also leaves the user vulnerable to surveillance. Whenever a mobile phone is on it connects to "base stations" in the surrounding area. If the phone connects to three base stations, the location of the user can be triangulated, and the more stations in the area, the more accurate the positioning becomes.[94] As well, each phone and SIM card has an identifying number that can be traced to the owner if they did not take mitigating steps when they acquired it. This can help governments identify the location of protests if they see a number of known dissidents are in the same location or if a large mass of people are heading towards the same public area during times of unrest, an election or an anniversary.[95]

Information projection and manipulation

The tried and true method of propaganda has also found a new home on the Internet, and can be used to compliment the strategies of censorship and surveillance, or even as an alternative. According to Evgeny Morozov, "the most effective system of Internet control is not the one that has the most draconian system of censorship, but the one that has no need for censorship whatsoever".[96] Efforts to censor and monitor online content tend to be fairly transparent and easily exposed, and often add credibility to the individual or group that is the object of a government's efforts. Effective propaganda, however, can counter criticism and influence online discussions, and can be easily spread without attributing blame to the government by using pro-regime supporters (like the SEA) or covert government-sponsored or run websites.[97]

[94] Morozov, *The Net Delusion*, 175
[95] ibid, 176
[96] ibid.
[97] ibid.

In Bahrain, where protests against the government erupted shortly after Tunisians and Egyptians took to the streets, the government decided to embrace social media to counter the growing number of opposition voices online. The country has an extremely high Internet penetration, at eighty-eight percent, making the online battleground particularly important.[98] The Interior Ministry and the foreign minister, Khalid Alkhalifa, both have very active Twitter accounts (with 82,870 and 90,622 followers respectively at the time of writing), which they use to publicize government messages and encourage support of the government.[99]

In Bahrain, social networking sites such as Twitter and Facebook have seen a surge in the number of pro-regime users in the country since the beginning of the unrest, provided another avenue of propaganda for the government.[100] These users post misinformation and violent video footage, which they then try to attribute to protesters. The "Bahraini Twitter Trolls", for example, post "corrective statements" to counter any and all anti-government commentary on the social networking site.[101] The information that they post is often controversial or simply factually incorrect, but all in support of the regime. In times of political unrest, this type of misinformation preys on people's need for information, fears and vulnerability.[102]

The SEA is also in the business of pro-regime propaganda. On August 26 2011, the group uploaded YouTube videos of the "Friday of Patience and Persistence Protests". The videos portrayed protestors killing Syrian security forces, or at least that is what they

[98] York, "The Arab Digital Vanguard," 39.
[99] J. David Goodman, "'Twitter Trolls' Haunt Discussions of Bahrain Online," *The Lede*, October 11, 2011. http://thelede.blogs.nytimes.com/2011/10/11/twitter-trolls-haunt-discussions-of-bahrain-online/.
[100] Ibid.
[101] ibid.
[102] Morozov, *The Net Delusion*, 145.

were meant to do. The videos were actually uploaded on the Thursday—one day before the protests apparently took place.[103] In another attempt to manipulate the storyline of the Syrian uprising, the SEA inserted news stories into the websites of media outlets. An article about a military coup in Qatar, for example, was successfully placed on the websites of Al-Arabiya and the pan-Arab TV station in April 2012.[104] The goal of such a strategy was likely to draw international attention away from the escalating crisis in Syria.

Website defacement, however, is where the SEA's expertise really lies. This method of information manipulation and projection changes the appearance of a website or webpage, and the SEA has used it to target individuals and groups, inside and outside of the country, that have expressed their opposition to the government. The Facebook pages of opposition groups have, for example, been defaced with pro-regime text and SEA logos. Not long after the Libyan Transitional National Council recognized the Syrian National Council as the legitimate government, the "New Libya" website was defaced with text denouncing the Libyan rebels because they "sold their dignity, honor, and country to NATO".[105] The SEA has also defaced various American universities and fan websites of Johnny Depp, Ben Affleck and Brad Pitt to try to counter the negative international attention that the Syrian government has been receiving.[106]

As previously mentioned, the SEA cannot be directly linked to the Syrian regime, but the government has publicly expressed its gratitude to the organization for its efforts. As well, many of the SEA's targets have been hit shortly after being arrested, accused of

[103] OpenNet Initiative, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets."
[104] ibid.
[105] ibid.
[106] ibid.

defamation or otherwise denounced by the regime. Shortly after a media blackout on the Syrian uprisings was imposed, for example, the SEA defaced news sites that expressed dissenting views.[107] The website of a political cartoonist critical of the regime, who had previously been abducted by and beaten by security forces, was defaced by the army, as was the website of a singer who had been denounced by for supporting the uprisings.[108] At the very least, the Syrian government has a powerful ally in the SEA; at the most, a group of tech-savvy government supporters on its payroll.

Legal, regulatory and extra-legal measures

Despite all of the advances in technological repression, the use of legal, regulatory and extra-legal measures still tends to be the method most commonly employed by authoritarian regimes. This tactic is easily used by all dictators, regardless of the communications infrastructure or availability of tech-savvy government supporters in the country—all they really need are some security forces, judges in their back pockets and a jail. With it comes the added bonus of intimidating citizens into submission, encouraging self-censorship and getting dissidents who may be spreading discontent to the masses out of the picture.

In some countries, an existing legal framework allows governments to arrest, prosecute and inflict harsh sentences on bloggers, opposition group leaders using social media to organize or other opponents to their regime. These usually come in the form of defamation or libel laws, intended to protect people from malicious or slanderous

[107] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers." *The Huffington Post*, September 27, 2011. http://www.huffingtonpost.com/2011/09/27/syrian-electronic-army_n_983750.html.
[108] Committee to Protect Journalists, "Syrian forces harass Sky News; hackers attack Ferzat," May 1 2012. http://cpj.org/2012/05/syrian-forces-harass-sky-news-hackers-attack-ferza.php.

statements against them, but often used to protect governments from criticism.[109] More commonly, however, individuals using the Internet to exercise their freedom of expression are arbitrarily arrested and prosecuted without legal recourse and sentenced to long or even indefinite prison terms.[110] As the judiciaries in many of these countries are not independent, it is not difficult to get a judge's complicity, and entire proceedings may go on behind closed doors.[111] The people are at the full discretion of the state.

This tactic has been used in all of the Arab Spring countries. In Egypt, Wael Ghonim, the Google executive who took a leading role in the organization of the revolution, was arrested on January 28 and detained, blindfolded and interrogated for eleven days.[112] Bahraini authorities arrested dozens of bloggers and netizens in 2011, some for posting pictures and videos of protests on Facebook, others for the defamatory content of their blogs. On April 2 2011, for example, a blogger named Zakariya Rashid Hassan al-Ashiri was arrested and charged for promoting secularism and inciting hatred against the government. He died in prison shortly after. Photos that emerged of al-Ashiri in prison showed signs of torture.[113] Syrian security forces have arrested tens of thousands of people—some of whom have reportedly been tortured to reveal their social media passwords.[114]

Corporate complicity

[109] Calingaert, "Authoritarianism vs. the Internet,"69.
[110] Deibert and Rohozinski, "Good for Liberty, Bad for Security?," 138.
[111] ibid.
[112] Kirkpatrick and Sanger. "A Tunisian-Egyptian Link That Shook Arab History."
[113] Committee to Protect Journalists, "Zakariya Rashid Hassan al-Ashiri," April 9 2011. http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.
[114] Data Protection Centre, "Syrians targeted in cyber attacks and tortured for Facebook passwords ." Accessed July 22, 2012. http://www.dataprotectioncenter.com/social-media/facebook/syrians-targeted-in-cyber-attaks-and-tortured-for-facebook-passwords/.

Many authoritarian governments have had some assistance in their efforts to deny, monitor and manipulate information in cyberspace. Companies—including, Internet service providers, blog-hosting companies, social networking platforms, technology firms, mobile phone operators and cybercafés—have been complicit in efforts to suppress political opposition in the digital realm.[115]

In March 2011, the OpenNet Initiative reported that North American companies had provided censorship software to governments in Bahrain, the UAE, Qatar, Oman, Saudi Arabia, Kuwait, Yemen, Sudan and Tunisia—not the most human rights abiding states by any standard. These technologies were used by these governments to censor social and political content, "effectively blocking a total of over twenty million Internet users from accessing such websites."[116] A Canadian company called Netseepwer Inc., based in Guelph, Ontario, for example, has provided content-filtering software to some of the most repressive regimes in the Arab world—clients include national Internet service providers in Qatar, Yemen and the UAE. The technology allows these governments to block political, social and religious content based on a list of categories.[117]

Similarly, in the fall of 2011 a California-based technology manufacturer called Blue Coat Systems was found to be supplying the Syrian regime with network security and optimization tools. According to The Citizen Lab, which has done extensive research on the use of commercial filtering technologies in authoritarian countries, "these tools include ProxySG devices that work with WebFilter, a product that categorizes billions of

[115] Calingaert, "Authoritarianism vs. the Internet,"68.

[116] Rebecca MacKinnon, *Consent of the Networked*, chap. 8.

[117] Amy Dempsey and Nicki Thomas, "Guelph-based software censors the Internet in the Middle East," *The Toronto Star*, June 13, 2011. http://www.thestar.com/news/article/1007399--canadian-made-censorship?bn=1.

web pages to permit filtering of unwanted content".[118] Given the government's brutal crackdown on the uprisings in the country, and their apparent skill in the use of technology to counter their political enemies, this is a very troubling finding.

Western corporations are also receiving an increasing number of requests from authoritarian governments to remove or block access to content that they deem to be inappropriate, or to provide information about users. In most cases, these practices lack transparency, and users who have their content removed or personal information handed over are not consulted or informed of the reasons for the decision.[119] One exception is American-based Google, which has developed the Google Transparency report to detail the removal and user data requests that it receives on a bi-annual basis. In the last report, however, covering the period from July to December of 2011, an increasing number of government requests were not accompanied by a court order, and instead fell into Google's category of "other" requests from the "executive, police, etc".[120] This demonstrates that governments are increasingly bypassing formal and lawful processes in their attempts to get the compliance of private sector companies in their Internet censorship activities.

In response to criticism of their business practices, companies often insist that as profit-maximizing organizations, it is not their responsibility to be concerned about human rights.[121] At the same time, the Western governments that should be regulating these companies stay largely on the sidelines. Unless steps are taken by the international

[118] The Citizen Lab, "Behind Blue Coat: Investigations of commercial filtering in Syria and Burma." Last modified November 9 2011. http://citizenlab.org/2011/11/behind-blue-coat/.
[119] MacKinnon, *Consent of the Networked*, chap. 8.
[120] Google, "Google Transparency Report." Last modified 2012. https://www.google.com/transparencyreport/.
[121] MacKinnon, *Consent of the Networked*, chap. 8.

community and Western governments to hold companies to account, it is unlikely that the growing trend of corporate complicity in the human rights abuses of authoritarian governments is likely to slow down anytime soon.

The future of online repression

As Internet penetration rates continue to increase around the world, and technology continues to become more and more sophisticated, the potential for online censorship, surveillance and propaganda also grows. Just as Facebook and Google are able to target advertisements at users based on their online activities, so too are governments beginning to learn how to trace online networks and accurately target censorship. Take, for example, the recommendation and "like" technology utilized by social media applications—those with anti-government sentiments share links with other citizens, providing authoritarian governments with the opportunity to trace these networks, and block the type of content that those within them share with one another.[122] Facebook's face recognition technology, which allows users to identify a single photo of a friend and then identifies that individual in other photos across the site, could be used by governments to identify people caught in a photo or on tape at a protest.[123] As the Internet becomes even more social and different websites and social networks become more connected, the opportunities abound for governments to utilize the Internet to their advantage.

Whatever a government's chosen tactic, the effects can be far-reaching and devastating for citizens. Website downtime is an obvious consequence, which can have serious implications for citizens trying to access information in times of crisis. The

[122] Morozov, *The Net Delusion*, 160.
[123] ibid, 154

chilling effect on free speech is also pervasive. When individuals know that they may be monitored by the government, or arrested for their online activities, they may air on the side of self-censorship and limit their online political activity. The tactics themselves may be useful for authoritarian governments, but the secondary effects of creating a culture of fear and uncertainty are where the power really lies.

It is important to note that just as the use of the Internet is only one of a multitude of factors that contribute to the emergence of opposition or democracy movements, the co-optation of the Internet and other information communication technologies by authoritarian governments is also only one factor contributing to the persistence of authoritarianism in many countries and regions around the world. Other factors include "energy endowment, little or no previous experience with democratic forms of rule, covert support from immoral Western democracies, bad neighbours".[124] For these opposing groups, the use of technology has been a tool, and tools do not topple governments nor do they keep governments in power, people do.

THE WAY FORWARD:

In order to place the power of the Internet in the hands of those who would use it legitimately and out of the hands of those who would use it as a tool of repression or crime. Currently, "the corporations and governments that build, operate and govern cyberspace are not being held sufficiently accountable for their power over the lives and identities of people who use digital networks".[125] In order to rectify this, the international community must take steps to promote a free and open, yet secure Internet where

[124] ibid.
[125] MacKinnon, *Consent of the Networked*, chap. 1.

universal human rights are respected and Internet users are protected from censorship and repression, as well as illegal content or content that incites violence or hate.

One step is to develop a set of non-binding principles, akin to a code of conduct, that builds common and transparent principles for domestic Internet use and clearly defines what constitutes a legitimate restriction of Internet freedom—for example, child pornography, inciting violence or a national security threat in cyberspace—and make it clear that targeting political speech will not be accepted as a reason for declaring a cyber emergency. Efforts should particularly be made to reach out to countries that have been the most active in controlling their populations in cyberspace, including China, Iran and Syria. It should not, however, be just about pointing fingers, but also attempting to get more people and states committed to principles of Internet freedom.

Steps should also be taken to increase and strengthen the private sector's role in protecting freedom of the Internet. International companies must be prevented from assisting or being complicit in human rights violations of states. To date, there have been a number of civil society initiatives attempting to make companies accountable and take Internet freedom principles into account in their business operations. These have, however, generally been disconnected and would benefit from more leadership from individual states, the United Nations and various other international arenas. In July 2011 the UN Human Rights Council unanimously endorsed a set of "guiding principles for human rights and business" which provides an excellent opportunity for countries, like Canada and the United States, to implement these principles domestically and be at the cutting edge of determining what this means for companies working internationally.[126]

126 John Ruggie, "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," *Human Rights Council*, Seventeenth Session, Agenda Item 3

Specifically, companies operating in authoritarian countries should undertake a human rights impact assessment of their decisions before and after entering a foreign market. Company policies should be created which require them to refrain from disclosing the personal and private information of activists, dissidents and opposition groups when such requests can be reasonably believed to be for the purposes of stifling legitimate freedom of expression or for identifying opposition in order to detain or torture them. As well, these policies should prohibit companies from providing repressive governments with any technologies that could assist in their efforts to censor legitimate content or identify dissenters based on their online presence. Along with these efforts there should be a reporting mechanism in which they are required to publicly report any government inquiries for information about users and requests to remove content from their services.

The international community should also ramp up its efforts to assist developing countries to bridge the "digital divide" and gain greater access to information communication technologies (such as modems, computers and software) and mobile technologies. This effort should include an education component, which would support digital literacy initiatives.

Perhaps most importantly, Western governments that claim moral authority over these authoritarian governments, and call on them to respect freedom of expression, association and privacy, must get their own houses in order. Countries like the United States and Canada set dangerous precedents when they announce bills that would allow them to obtain the private information of citizens or request companies to remove legitimate online content for view without going through the proper legal channels. They

(21 March 2011), http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf.

cannot expect that the Syrias and Chinas in the world will respect their citizen's rights to Internet freedom if they do not themselves.

CONCLUSION

The Internet has provided an excellent tool for citizens living under repressive regimes who wish to challenge the status quo in their countries. As opposed to the traditional sources of information in these countries, such as the mainstream media, it has remained largely untouched by many governments, and provides citizens with a way to exercise their freedom of expression, assembly and association. It also provides a way for these individuals to form networks of like-minded people, mobilize support for their cause and provide the outside world with a glimpse of the abuses they face at the hands of their governments. In the Arab Spring revolutions in Tunisia and Egypt in particular, the Internet, blogs, social networking platforms, photo and video sharing tools and mobile technologies were utilized by opposition movements in their efforts to see the end of the repressive rule of Presidents Ben Ali and Mubarak. Ultimately, they were able to harness the power of these tools to reach their goals. While the use of the Internet was not the only factor contributing to the existence of these movements or their success, it certainly increased their speed, scope and scale. The protesters were empowered by these tools, and it is unlikely that their movements would have been as effective without their use.

As news of the Tunisian and Egyptian revolutions spread across the region, citizens and governments took notice. Increasingly, governments in the Arab World and beyond are recognizing the ways in which their citizens can use the Internet to challenge

them politically. As such, these regimes are operating with an ever-greater willingness and ability to use the Internet against their citizens. Once confined to the offline world, censorship, surveillance and propaganda are becoming increasingly common in the online world as well. In addition, governments are using existing laws and regulatory frameworks, creating new laws and using extra-legal measures to punish their political opponents for online dissent. To do so, they have often enlisted the help of sympathetic citizens and profit-driven corporations.

Left unchecked, the Internet is likely to be used more frequently and more effectively by repressive governments. The international community must therefore take steps to ensure that the Internet remains free and open, yet secure, and that freedom of expression and association online is subject only to the limitations deemed acceptable offline as well. Corporations around the world must be required to take a greater stake in protecting the rights of citizens who pay a high price for their complicity in the abuses of authoritarian governments. The framework for ensuring that the power of the Internet remains in the right hands already exists in international human rights standards, it just needs to be properly applied to the ever-evolving realm of the Internet. Doing so will allow new movements to flourish, allow citizens to exercise fundamental human rights and place a check on governments and dictators who would use it as yet another tool of repression against their citizens.

BIBLIOGRAPHY

Agarwal, Sheetal D., Philip N. Howard, and Muzammil M. Hussain. "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?." *Issues in Technology Innovation*. no. 13 (2011): 1-11.

Berhe Kidani, Alula. "The Arab Spring and the Role of ICTs." *Sudan Vision Daily*, July 22, 2012. http://news.sudanvisiondaily.com/details.html?rsnpid=211636.

BlogPulse, "BlogPulse Stats." Accessed July 22, 2012. http://blogpulse.com/.

Bounenni, Bassam. "The limits of silencing Tunisia." *Foreign Policy*, January 12, 2011. http://mideast.foreignpolicy.com/posts/2011/01/12/the_limits_of_silencing_tunisia.

Calingaert, Daniel. "Authoritarianism vs. the Internet." *Policy Review*. no. 160 (2010): 63-75.

Committee to Protect Journalists, "Syrian forces harass Sky News; hackers attack Ferzat," May 1 2012. http://cpj.org/2012/05/syrian-forces-harass-sky-news-hackers-attack-ferza.php.

Committee to Protect Journalists, "Zakariya Rashid Hassan al-Ashiri," April 9 2011. http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.

Data Protection Centre, "Syrians targeted in cyber attacks and tortured for Facebook passwords ." Accessed July 22, 2012. http://www.dataprotectioncenter.com/social-media/facebook/syrians-targeted-in-cyber-attaks-and-tortured-for-facebook-passwords/.

Deibert, Ronald, and Rafal Rohozinski. *Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet*. *Access Denied: The Practice and Policy of Global Internet Filtering*. Edited by Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain. Cambridge: The MIT Press, 2008.

Delany, Colin. "How Social Media Accelerated Tunisia's Revolution: An Inside View." *The Huffington Post*, February 10, 2011. http://www.huffingtonpost.com/colin-delany/how-social-media-accelera_b_821497.html.

Dempsey, Amy and Thomas, Nicki. "Guelph-based software censors the Internet in the Middle East." *The Toronto Star*, June 13, 2011. http://www.thestar.com/news/article/1007399--canadian-made-censorship?bn=1.

Dickinson, Elizabeth. "The First WikiLeaks Revolution?." *Foreign Policy*, January 13, 2011. http://wikileaks.foreignpolicy.com/posts/2011/01/13/wikileaks_and_the_tunisia_protests.

Digital Buzz Blog (blog), January 3, 2012. http://www.digitalbuzzblog.com/social-media-statistics-stats-2012-infographic/.

Facebook, "Key Facts." Last modified March 31 2012. http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

Freedom House, "Middle East and North Africa." Accessed July 22, 2012. http://www.freedomhouse.org/regions/middle-east-and-north-africa.

Ghafour, Hamida. "Enough! Why thousands of young Arabs have taken to the streets in protest." *The Globe and Mail*, May 6, 2011. http://m.theglobeandmail.com/news/world/enough-why-thousands-of-young-arabs-have-taken-to-the-streets-in-protest/article578874/?service=mobile.

Goodman, J. David. "'Twitter Trolls' Haunt Discussions of Bahrain Online." *The Lede*, October 11, 2011. http://thelede.blogs.nytimes.com/2011/10/11/twitter-trolls-haunt-discussions-of-bahrain-online/.

Google, "Google Transparency Report." Last modified 2012. https://www.google.com/transparencyreport/.

Google, "Internet users as percentage of population, Egypt." Last modified July 13 2012. http://www.google.ca/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:EGY&dl=en&hl=en&q=egypt internet users.

Google, "Internet users as percentage of population, Tunisia." Last modified July 13 2012. http://www.google.ca/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:TUN&dl=en&hl=en&q=internet+users+as+percentage+of+population+tunisia

Hounshell, Blake. "The Revolution Will Be Tweeted." *Foreign Policy*, July/August 2011. http://www.foreignpolicy.com/articles/2011/06/20/the_revolution_will_be_tweeted?page=0,1.

Howard, Alex. "A Tunisian on the role of social media in the revolution in Tunisia." *Gov2.0* (blog), January 30, 2011. http://gov20.govfresh.com/a-tunisian-on-the-role-of-social-media-in-the-revolution-in-tunisia/.

International Telecommunications Union, "Information and Communication Technology Statistics." Last modified July 16 2012. http://www.itu.int/ITU-D/ict/.

"Iran's Twitter revolution." *The Washington Times*, June 16, 2009. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.

Karam, Zeina. "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers." *The Huffington Post*, September 27, 2011. http://www.huffingtonpost.com/2011/09/27/syrian-electronic-army_n_983750.html.

Keeter, Brian. "The internet equalizer: Why isn't the Obama administration doing more to promote social media?." *Foreign Policy*, September 28, 2011. http://shadow.foreignpolicy.com/posts/2011/09/28/the_internet_equalizer_why_isn_t_the_obama_administration_doing_more_to_promote_soc.

Kirkpatrick, David D. and Sanger, David E. "A Tunisian-Egyptian Link That Shook Arab History." *The New York Times*, February 13, 2011. http://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?pagewanted=all.

La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *Human Rights Council*. Seventeenth Session. no. Agenda Item 3 (16 May 2011). http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle Internet Freedom*. New York: Basic Books, 2012.

Morozov, Evgeny, and Palfrey, John. "Economist Debates: Internet democracy." *The Economist*, February 23, 2011. http://www.economist.com/debate/days/view/662.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs, 2011.

OECD. "The economic impact of shutting down Internet and mobile phone services in Egypt," February 4 2011. http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html .

OpenNet Initiative, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets."

Richtel, Matt. "Egypt Cuts Off Most Internet and Cell Service." *The New York Times*, January 28, 2011. http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=1.

Ruggie, John. " Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework." *Human Rights Council*. Seventeenth Session. Agenda Item 3 (21 March 2011). http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf.

"Shadows in the Cloud: Investigating Cyber Espionage 2.0." *Information Warfare Monitor*. (April 6 2010). http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0.

Topol, Sarah A. "What Happened to My Revolution." *Foreign Policy*, January 24, 2012. http://www.foreignpolicy.com/articles/2012/01/24/what_happened_to_my_revolution?page=0,5.

The Citizen Lab, "Behind Blue Coat: Investigations of commercial filtering in Syria and Burma." Last modified November 9 2011. http://citizenlab.org/2011/11/behind-blue-coat/.

Twitter, "About Us." Accessed July 22, 2012. https://twitter.com/about/.

United Nations, "The Universal Declaration of Human Rights." Accessed July 22, 2012. http://www.un.org/en/documents/udhr/.

Wolman, David. "Cairo Activists Use Facebook to Rattle Regime." *Wired Magazine*, October 20, 2008. http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?currentPage=1.

York, Jillian. "The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution." *Language, Identity & Politics*. 13. no. 1 (2012): 33-42. http://jilliancyork.com/wp-content/uploads/2012/02/33-42-FORUM-York.pdf.

York, Jillian. "Unblocking Syria's social media." *Al Jazeera*, February 12, 2011. http://www.aljazeera.com/indepth/opinion/2011/02/2011212122746819907.html.

YouTube, "Statistics." Accessed July 22, 2012. http://www.youtube.com/t/press_statistics/.