Major Research Paper

The Strategies of Cyberterrorism

Is Cyberterrorism an effective means to Achieving the Goals of Terrorists?

ADAM CHUIPKA

Graduate School of Public and International Affairs
University of Ottawa
Ottawa, Ontario
Supervised by Thomas Juneau

November 20, 2016

The convergence between the physical and digital world is growing exponentially as a result of ever increasing interconnectivity as well as reliability and dependence on technology. This has resulted in a growing fear that terrorists can exploit this interconnectivity and cause chaos via cyberspace by targeting critical infrastructures. Vulnerabilities in cyberspace are abundant and the consequences have the potential to be high, but terrorists may not have the capability or intent to adopt cyberterrorism in their strategies. In this major research paper, I contend that the strategies of cyberterrorism may be limited to attrition in pursuit of policy change goals. Therefore the threat from cyberterrorism is real but can be vastly overstated. I argue that the potential threat could be considerable, but the actual threat is significantly lower given that high-level cyber-attacks capable of being violent and causing terror require vast resources, intelligence, skill, and time – ultimately too much can go wrong in conducting a cyber-attack. Kinetic weapons for the time being are more suitable for the goals of terrorists. In presenting this argument, I first attempt to establish a common working definition of cyberterrorism, creating a criteria for what it is and what it is not; I review the literature to assess whether a cyber-attack can practicably meet this established criteria; and I draw on three case studies where parallels provide insight on the threat of cyberterrorism and judge the effectiveness of cyberterrorism as a strategy in pursuit of terrorist goals.

Keywords cyberterrorism, strategy, goals of terrorism, cybersecurity

Contents

INTRODUCTION

The convergence between the physical and digital world is growing exponentially as a result of ever increasing interconnectivity as well as reliability and dependence on technology.[1] The Internet transcends all borders and boundaries and can be accessed from anywhere, at any time, across the globe, provided a connection to the Internet is available. Deregulation and increased focus on profitability have forced companies and utilities to increasingly move their operations to the Internet to improve efficiency and reduce costs.[2] Critical infrastructures that we rely on are left vulnerable as a result of the increasing use of the Internet to manage industrial control systems (ICS) – such as supervisory control and data acquisition (SCADA) systems – that perform crucial operations.[3]

Too much connectivity reduces resilience in a complex world system leading to a reduced ability to adequately deal with crises. Smaller parts can affect larger wholes; technological power has changed the distribution of political power substantially allowing many actors to have large effects on global society. This increases the unknown unknowns of the world and thus potential unknown threats. Where globalization has allowed threats, such as terrorists, to be more fluid and difficult to track, as they are more embedded within civil society, cyberspace has likewise allowed for a new type of threat. The cyber threat from terrorism is such a manifestation of this phenomenon.

Terrorism expert Jessica Stern has stated that "Looking forward, cyberterrorism and cyberwar will likely pose a more serious threat to Americans' well-being than conventional terrorist violence".[4]

---

[1] Barry Collin, "Future of Cyberterrorism: The Physical and Virtual Worlds Converge," *Crime and Justice International* 13, no. 2 (1997): 7, http://www.cjimagazine.com/archives/cji4c18.html?id=415.

[2] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?," *Studies in Conflict & Terrorism* 28, no. 2 (2005): 139, http://dx.doi.org/10.1080/10576100590905110.

[3] "SCADA systems are used to monitor and remotely control critical industrial processes, such as gas pipelines electric power transmission, and potable water distribution/delivery." William T. Shaw, *Cybersecurity for SCADA Systems* (Tulsa: PennWell Corporation, 2006), 3; Weimann, "Cyberterrorism: The Sum of All Fears?," 144.

[4] Jessica Stern, "Obama and Terrorism: Like It or Not, the War Goes On," *Foreign Affairs* 94, no. 5 (2015): 67, https://www.foreignaffairs.com/articles/obama-and-terrorism.stern.

Accordingly, many governments around the world are making cybersecurity one of their biggest priorities.[5] Yet the concern surrounding threats in the shadows of cyberspace is not new. In 1997, Barry Collin forewarns of the cyber threat from terrorists in "Future of Cyberterrorism." Collin gives catastrophic examples of how this convergence between the physical and digital world leaves us vulnerable, such as: disrupting the banks, international financial transactions, and the stock exchanges; remotely accessing the processing control systems in cereal or baby formula manufacturers to change ingredients to be highly lethal; or even remotely taking over air traffic control systems and censors in the cockpit to cause crashes between commercial airlines.[6] By shifting many of these critical infrastructures and other industrial sectors operations to the Internet, they risk the possibility of infiltration. With complete control of these operations in the hands of those who wish to inflict harm, the damage could be catastrophic.

While the loss of human life caused by a cyber-attack has yet to be reported, this paper will demonstrate the potential is there. Cybercrime, cyber espionage, and acts of hacktivism are frequent and demonstrate the vulnerabilities in cyberspace which allow for these cyber-attacks to happen. Websites are hacked and defaced all the time.[7] Cybercrime has annually costed the global economy up to $575 billion.[8] Merrill Lynch Global Research of the Bank of America has indicated that we are potentially facing a worst case "Cybergeddon" scenario where cybercrime could extract as much $3 trillion of value created

[5] This year the U.S. and U.K. cybersecurity budgets were increased to $19 billion and $2.3 billion respectively.

[6] Collin, "Future of Cyberterrorism: The Physical and Virtual Worlds Converge," 16.

[7] For example, on the 10th of February 2010, the well-known hacktivist group *Anonymous* launched a cyber-attack on the Australian Parliament House website. This was provoked by, plans by the Rudd governments to introduce a forced filter on the Internet banning certain pornographic content. The cyber-attack consisted of bringing down the Australian Parliament House website, sending a barrage of the pornographic content in question to the email addresses of parliament members, as well as plastering this pornographic content on the Prime Minister's homepage. Keiran Hardy, "Operation Titstorm: Hacktivism or Cyberterrorism," *UNSW Law Journal* 33, no. 2 (2010): 474, http://www.austlii.edu.au/au/journals/UNSWLawJl/2010/21.pdf.

[8] Bank of America - Merrill Lynch Global Research, *You've Been Hacked! – Global Cybersecurity Primer*, 2015, 1, http://xxlsec.com/wp-content/uploads/2015/06/BankOfAmericaCyberReport.pdf.

by the Internet.[9] Moreover, governments are accusing others of cyber espionage and infiltrating their systems.[10] Given that Symantec has reported that "The capabilities required to inflict physical damage are similar to those needed for cyberespionage, and the target set is growing thanks to the proliferation of Internet-connected devices, including industrial control systems,"[11] this is particularly concerning. These frequent occurrences should be sufficient evidence that vulnerabilities in cyberspace is a critical issue that needs closer examination. In 2010, former Federal Bureau of Investigation Director, Robert Mueller stated in a speech that terrorists and other extremists "have shown a clear interest in pursuing hacking skills."[12] However, interest alone does not manifest a threat. To assess the risk of cyberterrorism, *threat*, *vulnerability*, and *consequence* must also be taken into consideration.[13]

While the growing literature on the subject is generally in agreement that the consequences have the potential to be high and the vulnerabilities in cyberspace are abundant, it remains divided on the overall threat of cyberterrorism. An evident gap in the literature is how cyberterrorism can be strategically used to achieve the goals of terrorists. *Capability* of terrorists to achieve a cyber-attack is often the focus when examining the overall threat of cyberterrorism. However, just as important when assessing the threat is the *intent* of a terrorist who must ultimately decide what may be the best course of action in

---

[9] Ibid.

[10] China for example, has been accused of cyber espionage on both private and government sectors (including the Pentagon) on multiple accounts, including the *Byzantine Hades*, *Aurora*, and *Titan Rain* espionage campaigns. Fahad Ullah Khan, "States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis," *Strategic Studies* 31, no. 3 (2011): 93.

[11] Symantec, *Internet Security Threat Report*, vol. 21, 2016, 45, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16707960&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2.

[12] Federal Bureau of Investigation (FBI), "The Cyber Threat: Using Intelligence to Predict and Prevent," last modified 2010, accessed November 2, 2016, https://archives.fbi.gov/archives/news/stories/2010/march/cyberintel030410.

[13] Henry H. Willis et al., *Estimating Terrorism Risk*, *Risk Management* (Santa Monica, CA: RAND Corporation - Center for Terrorism Risk Management Policy, 2005), 10, http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG388.pdf.

achieving their objectives and goals. Is cyberterrorism an effective means to achieving the goals of terrorists? In this paper I will argue that cyberterrorism has the potential to achieve the goals of terrorists, however, its use is limited when compared to kinetic weapons, thus rendering the conceived threat of cyberterrorism overstated.

This study will achieve this by: first, conceptualizing cyberterrorism; second, conducting a literature review on the subject to assess whether a cyber-attack can practicably meet the criteria created from conceptualizing cyberterrorism and review what the literature says on the threat, vulnerabilities, and consequences of cyberterrorism; third, examining three case studies of cyber-attacks to bring cyberterrorism into perspective; and finally, analyzing how cyberterrorism fits the strategies of terrorists in pursuit of their goals. Questions addressed in this analysis include: can cyber-attacks provide the same terror factor that kinetic weapons can? Who are the terrorists and do these terrorists have access to the funds, skill, and technology required to conduct a cyber-attack capable of causing violence, disruption, and terror? Are cyber weapons more effective than kinetic weapons? A final section will look at the bigger picture of cyberterrorism. A conclusion of the study will follow.

WHAT IS CYBERTERRORISM?

Before a discussion can be formulated on whether cyberterrorism is an effective means to achieve the goals of terrorists, cyberterrorism must be clearly defined. With an expanding range of scholarly work on cyberterrorism and cybersecurity in general, generating a meaningful debate on cyberterrorism requires a shared understanding of terms for discourse. Without shared meanings, it is impossible for different researchers to analyze the same propositions, so conceptualization is a necessary initial step of research. As cyberterrorism is evidently an aggregate of the terms 'cyberspace' and 'terrorism', it is important that these terms are thoroughly considered.

The "Cyber" in Cyberterrorism

The cyber in cyberterrorism refers to cyberspace. It is a prefix that has been commonly added to a number of subgroups regarding issues in the cybersecurity discourse, including but not limited to, cybercrime, cyberwar, cyberespionage, and of course cyberterrorism. Cyberspace, unlike terrorism, is a term that is generally agreed upon. It refers to the virtual world – including the Internet, and other computer-communications infrastructure – that is entirely composed of computers, algorithms, computer networks, and data.[14] A cyber-attack, as defined by Michael Kenney, is "a deliberate computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system, or damages or steals the information it contains."[15] While cyber-attacks in and of themselves take place in cyberspace, they may have effects in the physical world. For example, if a hacker gains unauthorized access to an ICS that

[14] Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 112, http://linkinghub.elsevier.com/retrieve/pii/S0030438714000787; Jonathan Matusitz and Elizabeth Minei, "Cyberterrorism: Its Effects on Health-Related Infrastructures," *Journal of Digital Forensic Practice* 2, no. 4 (2009): 162, http://www.tandfonline.com/doi/abs/10.1080/15567280802678657; Angela Gendron, "Cyber Threats and Multiplier Effects: Canada at Risk.," *Canadian Foreign Policy* 19, no. 2 (2013): 179, http://www.tandfonline.com/doi/abs/10.1080/11926422.2013.808578; P.W Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014), 13; Seymour E Goodman, Jessica C Kirk, and Megan H Kirk, "Cyberspace as a Medium for Terrorists," *Technological Forecasting and Social Change* 74, no. 2 (2007): 194, http://dx.doi.org/10.1016/j.techfore.2006.07.007.

[15] Kenney, "Cyber-Terrorism in a Post-Stuxnet World," 113.

controls electrical power, they could disable it. The ability to turn on and off certain functions may be already integrated into an ICS, but if they are not it is possible that malicious code be written to create that function that could achieve the same or similar results. The case studies presented in this paper will demonstrate three cyber-attacks, their effects and implications.

The "Terrorism" in Cyberterrorism

Unlike cyberspace, terrorism is a term that does not have an agreed upon definition. However, there are a number of similar aspects that are generally agreed upon. In Bruce Hoffman's *Inside Terrorism*, he provides an excellent definition and criteria of what constitutes terrorism:

> …the deliberate creation and exploitation of fear through violence or threat of violence in the pursuit of political change. All terrorist acts involve violence or the threat of violence. Terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or objects of the terrorist attack. It is meant to instill fear within, and thereby intimidate, a wider "target audience" that might include a rival ethnic or religious group, an entire country, a national government or political party, or public opinion in general. Terrorism is designed to create power where there is none or to consolidate power where there is very little. Through the publicity generated by their violence, terrorists seek to obtain the leverage, influence, and power they otherwise lack to effect political change on either a local or an international scale.[16]

Hence, Hoffman has distinguished terrorism from other types of crime and irregular warfare (see *Table 1*). In order to produce counter measures, having a criteria that differentiates terrorists from other threats is of particular importance in cyberspace where attribution can be especially difficult.

[16] Hoffman, *Inside Terrorism: Revised and Expanded Edition*, 40–41.

Table 1. Characteristics of Terrorism

1. Ineluctably political in aims and motives;
2. Violent – or, equally important, threatens violence;
3. Designed to have far-reaching psychological repercussions beyond the immediate victim or target;
4. Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and
5. Perpetrated by a subnational group or non-state entity.

Source: Bruce Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2006), 40.

A Criteria for Acts of Cyberterrorism

By adjusting Hoffman's definition of terrorism, a set of criteria for cyberterrorism can be constructed. First and foremost, albeit obvious, it must be executed via cyberspace; second, it must be ineluctably political or ideological in aims and motives; third, it must be violent or threaten violence; fourth, it must be designed to have far-reaching psychological repercussions beyond the immediate victim or target; fifth, it must be conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and finally, it must be perpetrated by a subnational group or non-state entity (see *Table 2*).

The criteria that requires the act of terrorism be violent or threaten violence is particularly important. The target of terrorists is generally people; damage to property is usually a byproduct of the act itself or part of the act to cause harm and terror to people. The World Health Organization defines violence as "is the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community that either results in or has a high likelihood of resulting

in injury, death, psychological harm, maldevelopment or deprivation."[17] By this definition, the cyber-attack would need to have an effect in the physical world. Furthermore, by this definition, disruption caused by a cyber-attack could be defined as violent if it results not just in injury or death, but also psychological harm, maldevelopment or deprivation. When considering the disruption of critical infrastructure, deprivation – or in extreme cases injury or death – could realistically be a consequence.

The criteria that requires the act of terrorism be "designed" to have far-reaching psychological repercussions beyond the immediate victim or target is also very important. While "designed" to cause terror, an act of cyberterrorism may fail to do so. Failure, however, does not explicitly restrict a cyber-attack from being labeled as a cyberterrorist attack. Though, as will be discussed in the final section, not labelling a cyber-attack as cyberterrorism may prove beneficial as a counter-cyberterrorism measure.

Table 2. Characteristics of Cyberterrorism

1. Executed via cyberspace;
2. Ineluctably political or ideological in aims and motives;
3. Violent or threatens violence;
4. Designed to have far-reaching psychological repercussions beyond the immediate victim or target;
5. Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and
6. Perpetrated by a subnational group or non-state entity.

Now that a criteria for cyberterrorism has been established, to prove that it is a distinct sub-issue of the greater cybersecurity discourse it can be tested against a number of other actors that pose a threat in cyberspace.

[17] World Health Organization, *Global Status Report on Violence Prevention 2014*, *World Health Organization*, 2014, 84, http://www.who.int/violence_injury_prevention/violence/status_report/2014/en/.

Other Cyber Threats that Are Not Cyberterrorism

Hacktivism

The term "hacktivism" is the amalgamation between hacking and political activism.[18]

Tim Jordan and Paul A. Taylor define *Hacktivism* as,

> …the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life. Social movements and popular protest are integral parts of twenty-first-century societies. Hacktivism is activism gone electronic.[19]

The main means to a hacktivists' ends include blockades and virtual sit-ins, web hacks and computer break-ins, automated email bombs, and computer worms and viruses.[20]

Cyberwarfare

Richard A. Clarke and Robert Knake are often quoted for their non-exhaustive definition of cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[21] Conveniently, this definition of cyberwarfare indicates that in order for an act to be characterized as cyberwarfare, it must involve actions of a nation-state. In addition, actions of non-state actors employed by a nation-state should also be considered cyberwarfare.

Cybercrime

The basic definition of cybercrime is the "use of computers or other electronic devices via information systems to facilitate illegal behaviours."[22] Examples of cybercrimes include: identity theft,

---

[18] "'Hacking' is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software." Weimann, "Cyberterrorism: The Sum of All Fears?," 135.

[19] Paul Taylor and Tim Jordan, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004), 1, papers3://publication/uuid/50380B27-672A-4D1A-89C0-6FC517868773.

[20] Weimann, "Cyberterrorism: The Sum of All Fears?," 135.

[21] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It*, *Terrorism and Political Violence*, vol. 23 (New York: HarperCollins Publishers, 2012), 6.

[22] Samuel C. McQuade, *Understanding and Managing Cybercrime* (Boston: Pearson Education, 2006), 2.

phishing scams, hacking – in which data or services are manipulated – and ecommerce fraud. However, cybercrime can also consist of activities such as cyber harassment, cyber stalking, preying on children through online activities, and even corporate espionage.[23]

Cyber Espionage

Cyber espionage is no different than conventional espionage; it is simply the means as to which information is collected.

> Cyber espionage involves obtaining secret or classified information without permission from individuals, companies or governments for economic, political or military advantage using illicit means through the Internet, networks and/or computers, and can involve cracking or malicious software such as Trojan horses and spyware.[24]

While cyber espionage does not directly pose as a physical threat, particular information collected through cyberspace runs the risk of being used for future operations that could prove to be violent.[25]

Chaotic Actors, Vigilantes, and Regulators

Besides the well understood agents that have operated in cyberspace, such as criminals, hacktivists, industrial spies, nation states, terrorists, and insiders, there are also new challenging threats, such as chaotic actors, vigilantes, and regulators.[26] These new actors could have the same effect as cyberterrorists, but distinguishing terrorists from these actors will drastically change counter measures.

For example, chaotic actors are not simply looking for anything logical, such as money. They don't necessarily have political aims or motives either. It can be difficult to deter, buy, negotiate, or reason with these actors.[27] Vigilantes on the other hand are only narrowly looking to right a wrong and do not

---

[23] Khan, "States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis," 92.

[24] Ibid., 93.

[25] Clay Wilson, "Cyber Threats to Critical Information Infrastructure," in *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2014), 129.

[26] Tyson Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things* (Cambridge: Morgan Kaufmann, 2016), 228.

[27] Ibid., 229.

necessarily think or care about the interdependencies that could be affected from their actions, whether they are technical, political, or personal.[28] Regulators may lack awareness of the interdependencies at play in cyberspace. Their actions, while well-considered, may have unintended consequences and cascading effects that could not have been predicted.[29]

As illustrated in *Table 3*, there are a number of crossovers between cyber actors that pose a cyber threat which demonstrates the confusion from the media and other actors that mislabel cyber-attacks. For example, distinguishing between hacktivism and other forms of cyber activity is especially important because acts of hacktivism have been labeled as acts of cyberterrorism on a number of accounts.[30] While there is a definitional difference between cyberterrorism in comparison to hacktivism, the intent of the latter is not to maim, kill, or terrify; though the means to achieving the desired results however, may be similar.[31] Therefore, hacktivism, as Gabriel Weimann warns, "hacktivism does highlight the threat of cyberterrorism, the potential that individuals with no moral restraint may use methods similar to those developed by hackers to wreak havoc." [32]

Likewise, while cyberterrorism and cyberwarfare are different, they have their similarities; attacking computers, networks, and the information stored therein and causing damage for political or ideological purposes. In the case of cyberterrorism its very nature has to be violent and has to be designed to cause terror. While cyberwarfare may result in violence and have psychological repercussions beyond the immediate victim or target, Michael Kenny argues that "such effects are incidental to the act, not indispensable, as they are in cyber-terrorism."[33] Therefore, cyber-attacks conducted by nation states

[28] Ibid.

[29] Ibid., 230.

[30] Kenney, "Cyber-Terrorism in a Post-Stuxnet World," 118.

[31] Weimann, "Cyberterrorism: The Sum of All Fears?," 135–136.

[32] Ibid., 137.

[33] Kenney, "Cyber-Terrorism in a Post-Stuxnet World," 122.

cannot be considered acts of cyberterrorism. These distinctions between different cyber threats are important as they allow for more calculated counter measures.

Table 3. Other Cyber Threats v. Cyberterrorism

Cyberterrorism Criteria	Hacktivism	Cyberwarfare	Cybercrime	Cyberespionage	Chaotic Actors	Vigilantes	Cyberterrorism
Executed via cyberspace	✓	✓	✓	✓	✓	✓	✓
Ineluctably political or ideological in aims and motives	✓	✓	X	–	–	✓	✓
Violent or threatens violence	X	–	X	X	–	–	✓
Designed to have far-reaching psychological repercussions beyond the immediate victim or target	X	–	X	X	–	X	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	–	X	–	–	X	—	✓
Perpetrated by a subnational group or non-state entity.	✓	X	–	–	✓	✓	✓

LITERATURE REVIEW

Now that cyberterrorism has a distinct definition that separates it from other threats in cyberspace, an assessment of whether a cyber-attack can practicably meet this criteria can be discussed. The following section is a review of the literature on cyberterrorism.

Cyberterrorism ≠ Terrorist use of Cyberspace

The first criteria that needs to be met on whether an action is deemed an act of cyberterrorism or not is whether the action is executed via cyberspace. This principle, while taken alone, has been used to broaden the definition of cyberterrorism to incorrectly include other activities in cyberspace, such as propaganda, communication, intelligence gathering, training, recruitment, and radicalization, to name a few. While there is no denying that terrorists are using modern technology to facilitate their operations, cyberterrorism in and of itself must involve a cyber-attack that fulfills the other characteristics of terrorism as previously mentioned. Most importantly, it needs to be violent or threaten violence and it needs to be designed to have far-reaching psychological repercussions beyond the immediate victim or target.[34]

That is not to say that the use of cyberspace by terrorists to facilitate operations is not important, as stated by Christopher Cox, "the use of cyber capabilities to support terrorist goals … must be considered when addressing the overall concern."[35] In fact, the use of cyberspace by terrorists has allowed for an

[34] Panayotis A. Yannakogeorgos, "Rethinking the Threat of Cyberterrorism," in *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2014), 53; Dorothy Denning, "Cyberterrorism: The Logic Bomb versus the Truck Bomb," *Global Dialogue* 2, no. 4 (2000): 2; Weimann, "Cyberterrorism: The Sum of All Fears?," 133; Michael Flemming, Peter; Stohl, "Myths and Realities of Cyber Terrorism," in *Countering Terrorism Through International Cooperation*, ed. Alex P. Schmid (Vienna: International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program, 2001), 38, http://www.comm.ucsb.edu/faculty/mstohl/Myths and Realities of Cyberterrorism.pdf.

[35] Christopher Cox, "Cyber Capabilities and Intent of Terrorist Forces," *Information Security Journal: A Global Perspective* 24, no. 1–3 (2015): 31, http://www.tandfonline.com/doi/full/10.1080/19393555.2014.998846.

escalating trend in radicalized individuals.[36] George Michael highlights this concern, stating "the increasing frequency of leaderless resistance among a disparate array of extremist and dissident movements suggests that the concept is gaining popularity as a tactical approach to terrorism and insurgency".[37]

On July 22, 2011, Anders Behring Breivik detonated a bomb in Oslo, killing 8 people, before driving to an Island where he fatally shot another 69 people at a summer camp for the Labour Youth political organization.[38] Breivik was motivated by the broader anti-Islamic social movement, as evident in his 1,518-page Manifesto, which he released via email just hours before the attacks.[39] On April 15, 2013, two explosive devices were set off by brothers Tamerlan and Dzhokhar Tsarnaev during the Boston Marathon near the finish line, killing 3 and injuring another 264 spectators.[40] FBI investigators indicated the assailants "were motivated by extremist Islamic beliefs but were not acting with known terrorist groups".[41] On June 12, 2016, Omar Mateen opened fire at a nightclub in Orlando, Florida, killing 49 people and injuring 53 more. According to federal law enforcement officials, "after his initial assault on the dance club, Mateen called 911 and pledged allegiance to the leader of the Islamic State".[42] Like the Tsarnaev

---

[36] Ines von Behr et al., *Radicalisation in the Digital Era* (Brussels, 2013), 31, http://www.rand.org/pubs/research_reports/RR453.html.

[37] George Michael, "Counterinsurgency and Lone Wolf Terrorism," *Terrorism and Political Violence* 26, no. 1 (2014): 46, http://www.tandfonline.com/doi/abs/10.1080/09546553.2014.849912.

[38] Lars Erik Berntzen and Sveinung Sandberg, "The Collective Nature of Lone Wolf Terrorism: Anders Behring Breivik and the Anti-Islamic Social Movement," *Terrorism and Political Violence* 26, no. 5 (2014): 759, http://www.tandfonline.com/doi/abs/10.1080/09546553.2013.767245.

[39] Ibid., 763.

[40] Government of Massachusetts, *After Action Report for the Response to the 2013 Boston Marathon Bombings* (Boston, 2014), 4–6, http://www.mass.gov/eopss/docs/mema/after-action-report-for-the-response-to-the-2013-boston-marathon-bombings.pdf.

[41] Michael Cooper, Michael Schmidt, and Eric Schmitt, "Boston Suspects Seen as Self-Taught, Fueled by Web," *New York Times*, April 23, 2013, http://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html?hp&pagewanted=all.

[42] Hayley Tsukayama, Mark Berman, and Jerry Markon, "Gunman Who Killed 49 in Orlando Nightclub Had Pledged Allegiance to ISIS," *The Washington Post*, June 13, 2016, https://www.washingtonpost.com/news/post-nation/wp/2016/06/12/orlando-nightclub-shooting-about-20-dead-in-domestic-terror-incident-at-gay-club/?hpid=hp_hp-top-table-high_orlando-banner%3Ahomepage%2Fstory&utm_term=.5576d5b796e7.

brothers, Mateen had no direct links to a terrorist organization but was inspired by extremist Islamic beliefs and the Islamic State.

It is important that a distinction is made between lone wolves and "solo-terrorists", both considered forms of "leaderless resistance".[43] A lone wolf, according to Weimann, can be defined as "an individual or a small group of individuals who use traditional terrorist tactics – including the targeting of civilians – to achieve explicitly political or ideological goals, but who acts without membership in, or cooperation with, an official or unofficial terrorist organization, cell, or group."[44] Thus, a solo-terrorist would operate in isolation with network ties to an extremist or terrorist organization.[45] The lone wolf is considered more dangerous from a counterterrorism perspective, as there are no previous ties with a terrorist organization to raise any red flags – meaning an attack can come out of nowhere.[46] However, the term "lone wolf" is contested; for some specialists, in practice lone wolves do not exist. The individuals mentioned above who conducted lone wolf terrorist attacks were in some form of contact, online or in person, with others – thus allowing for some form of detection to be possible.

This threat is exacerbated by cyberterrorism as radicalized individuals with the skills required to conduct cyber operations do not necessarily need to be resident in the state in which they are to conduct an act of terrorism. A further discussion will be had on this topic in the final section of this paper, however, as it stands, terrorists' use of cyberspace does not necessarily equate to cyberterrorism.

---

[43] Petter Nesser, "Research Note: Single Actor Terrorism: Scope , Characteristics and Explanations," *Perspectives on Terrorism* 6, no. 6 (2012): 23, http://www.terrorismanalysts.com/pt/articles/issues/PTv6i6.pdf.

[44] Gabriel Weimann, "Lone Wolves in Cyberspace," *Journal of Terrorism Research* 3, no. 2 (2012): 75.

[45] Center for Terroranalyse, *The Threat from Solo Terrorism and Lone Wolf Terrorism*, 2011, 1, https://www.pet.dk/~/media/Engelsk/the_threat_from_solo_terrorism_and_lone_wolf_terrorism_-_engelsk_version_pdf.ashx.

[46] Michael, "Counterinsurgency and Lone Wolf Terrorism," 49.

Aims and Motivations

The second criteria that needs to be met on whether an action is deemed as an act of cyberterrorism or not is dependent on if the action is ineluctably political or ideological in aims and motives. While many threat actors in cyberspace have political or ideological aims and motives, terrorists in particular would want those to be known and therefore be useful in attributing a cyber-attack as an act of cyberterrorism. However, there are many with the capabilities or relevant skill sets that are not inherently terrorists.

Interested in hackers' motives, University of South California professor, Douglas Thomas, spent several years interviewing and studying computer hackers, "they engage in behaviors that are typical of adolescent boys, challenging adult authority and flexing their muscles."[47] Most of these individuals are more likely to be hacktivists. Thomas continues, "with the vast majority of hackers, I would say 99 percent of them, the risk [of cyberterrorism] is negligible for the simple reason that those hackers do not have the skill or ability to organize or execute an attack that would be anything more than a minor inconvenience."[48] In his testimony on cyber terrorism and critical infrastructure protection to the United States Congress, Thomas goes on to say that even those hackers with the skill to possibly inflict serious damage, "strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of their list of priorities" and engaging in terrorism, for financial gain or otherwise, is not something that would suit their profile.[49]

---

[47] Douglas Thomas, "Cyber Terrorism and Critical Infrastructure Protection" (US Congress, House, 107th Cong. July 24, 2002), 2, http://www-bcf.usc.edu/~douglast/testimony.pdf.

[48] Ibid.

[49] Ibid., 2–3.

While terrorists have illustrated a desire to use cyberspace as a means of terrorism,[50] Maura Conway argues very few jihadists have computer backgrounds and assumes those that do, do not have the mastery of complex systems necessary to carry out a serious cyber-attack.[51] This is important as it means terrorists would be required to hire hackers with the skillset to achieve a terrorist's desired ends, which Conway argues is highly unlikely. To begin with, she argues it risks operational security; terrorist organizations would be at higher risk of infiltration.[52] Terrorists would also be unable to know for certain whether the hired assailant has the necessary skills to perform what is required for their operation.[53] Furthermore, hackers are likely to lack loyalty and would be easily persuaded by other parties for monetary gains.[54] However, Clay Wilson argues that alliances between hackers, criminals and terrorists might occur "because those nations that are targeted for illegal distribution of drugs are often the same nations that are targeted for attack by terrorists and extremists."[55]

Can a Cyber-Attack be Violent?

The third criteria that needs to be met on whether an action is deemed an act of cyberterrorism or not is whether the action can be violent or threaten violence. Definitional disputes and problems of attribution aside, do today's terrorists have the capacity to launch a cyber-attack that is violent? Can a

[50] Roland Heickerö, "Cyber Terrorism: Electronic Jihad," *Strategic Analysis* 38, no. 4 (2014): 559, http://www.tandfonline.com/doi/abs/10.1080/09700161.2014.918435.

[51] Maura Conway, "Against Cyberterrorism," *Communications of the ACM* 54, no. 2 (2011): 27, http://dx.doi.org/10.1145/1897816.1897829.

[52] Maura Conway, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism," in *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2014), 112.

[53] Conway, "Against Cyberterrorism," 28.

[54] Maura Conway, "Hackers as Terrorists? Why It Doesn't Compute," *Computer Fraud & Security* 2003, no. 12 (2003): 10, http://dx.doi.org/10.1016/s1361-3723(03)00007-1.

[55] Wilson, "Cyber Threats to Critical Information Infrastructure," 129.

violent cyber-attack be threatening? Ultimately, wanting to do something and having the capabilities are two entirely different things.[56]

While Dorothy Denning brings to attention that "at Idaho National Labs, researchers demonstrated how a cyber-attack could cause a power generator to self-destruct,"[57] Erik Gartzke, Thomas Rid, Conway, Andrew Jones, and Weimann do not believe that terrorists currently possess the capabilities to perform a successful and significant cyber-attack that would cause physical harm to persons or property;[58] the capability to cause mass amounts of death is just not yet possible.[59] Real world terrorist attacks are hard enough to carry out and cyber-attacks do not provide the spectacle required to cause terror.[60] This suggests it is unlikely terrorists will favour using cyber-attacks over kinetic attacks.

Capabilities are just as much about the attackers as the defenders. Vulnerabilities are what permit hackers to infiltrate computers and networks in order to conduct a cyber-attack.[61] Weimann claims that ignorance is a major factor for those who are concerned about a cyber threat. Lawmakers and senior administration officials do not always understand the inner workings and functioning of the cyber world;

---

[56] Conway, "Against Cyberterrorism," 27.

[57] Dorothy Denning, "Stuxnet: What Has Changed?," *Future Internet* 4, no. 4 (2012): 674, http://www.mdpi.com/1999-5903/4/3/672/.

[58] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 68, http://dx.doi.org/10.1162/isec_a_00136; Conway, "Against Cyberterrorism," 28; Thomas Rid, "Think Again: Cyberwar," *Foreign Policy* 192 (2012): 2, http://foreignpolicy.com/2012/02/27/think-again-cyberwar/; Andrew Jones, "Cyber Terrorism: Fact or Fiction," *Computer Fraud & Security* 2005, no. 6 (2005): 5, http://dx.doi.org/10.1016/s1361-3723(05)70220-7; Weimann, "Cyberterrorism: The Sum of All Fears?," 139.

[59] Ibid., 143; Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 73; Rid, "Think Again: Cyberwar," 73.

[60] Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change* 46, no. 4–5 (2006): 236, http://dx.doi.org/10.1007/s10611-007-9061-9; Conway, "Against Cyberterrorism," 28.

[61] Audrey Guinchard, "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy," *Journal of Strategic Security* 4, no. 2 (2011): 83, http://dx.doi.org/10.5038/1944-0472.4.2.5.

a lack of understanding is a source of fear,[62] "the fear of random, violent victimization segues well with the distrust and outright fear of computer technology."[63]

Furthermore, Jones argues that disruption of critical infrastructures caused by a cyber-attack can only be deemed temporary, as damage in most cases can be repaired in a reasonable amount of time.[64] James Lewis sustains the same assertion in his report for the Center for Strategic and International Studies, "nations are more robust than the early analysts of cyberterrorism and cyberwarfare give them credit for. Infrastructure systems [are] more flexible and responsive in restoring service than the early analysts realized, in part because they have to deal with failure on a routine basis."[65] While this damage and or disruption to critical infrastructures may be costly, there are no long-term effects.[66] The *Cyber-Attack on the Ukrainian Power Grid* case study following this section illustrates this. Those skeptical of the cyber threat hold that both the capabilities and the vulnerabilities, that are often hyped, are just not there.

While many believe that cyberterrorism is nothing to be concerned about, there are some who believe that it *currently* is not a threat but *will be* in the future. Weimann echoes this position stating that "the threat of cyberterrorism may be exaggerated and manipulated, but it can be neither denied nor ignored."[67]

A fortress is only as strong as its weakest link. Reliability, not security, was priority when the Internet was first conceived.[68] Andrew Krepinevich states "critical infrastructure functionality is growing progressively more vulnerable to cyber-attacks, given its increasing reliance on information systems in

---

[62] Weimann, "Cyberterrorism: The Sum of All Fears?," 132.

[63] Ibid., 131.

[64] Jones, "Cyber Terrorism: Fact or Fiction," 6.

[65] James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, D.C., 2002), 10, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

[66] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 58.

[67] Weimann, "Cyberterrorism: The Sum of All Fears?," 146.

[68] Charles A Shoniregun, *Synchronizing Internet Protocol Security* (New York: Springer, 2007), 7.

general and access to the Internet in particular."[69] These systems are often complex and therefore "are bound to contained weaknesses that might be exploited," Weinmann continues, "even systems that seem 'hardened' to outside manipulation might be accessed by insiders, acting alone or in concert with terrorists, to cause considerable harm."[70] The *Maroochy Shire Cyber-Attack* case study following this section will examine this in greater detail.

A National Security Agency (NSA) exercise that took place in 1997 code-named "Eligible Receiver," revealed the vulnerabilities in computers and networks across the U.S. and need for greater cybersecurity.[71] Upon the NSA's briefing on ground rules to a team of thirty-five computer hackers, the exercise commenced. Given the label "Red Team" and posing as hackers hired by the North Korea's intelligence service, they scattered throughout the US looking to infiltrate military networks. Their primary objective: hack into and disrupt U.S. national security systems of the U.S. Pacific Command in Hawaii. Two principle rules were given to follow: only download freely available hacking utilities and software tools, and breaking U.S. law was prohibited. The Red Team was restricted from using the Pentagon's arsenal of secret offensive information warfare tools.

The Red Team was able to penetrate the Pentagon's networks with ease; they accomplished this unidentified and untraced. The Committee to Review Department of Defense (DOD) C4I Plans and Programs, the Commission on Physical Sciences, Mathematics, and Applications, and the National Research Council found "the vulnerabilities exploited were common ones, including bad or easily guessed passwords, operating system deficiencies, and improper system configuration control, sensitive site-related information posted on open Web pages, inadequate user awareness of operational security, and

[69] Andrew F. Krepinevich, *Cyberwarfare: A "Nuclear Option"?* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2012), 2.

[70] Weimann, "Cyberterrorism: The Sum of All Fears?," 144.

[71] Fundamental Challenges Committee et al., *Realizing the Potential of C4I: Fundamental Challenges*, 1999.

poor operator training."[72] Even with impenetrable defenses it only takes one person to let the enemy in, intentional or not; according to the Red Team, "sometimes it was just easier to call somebody on the telephone, pretend to be a technician or high-ranking official, and ask for the password."[73]

The team of hackers were able to gain access to unauthorized data, alter data clandestinely, achieve identity fraud, and execute Denial-of-Service (Dos) attacks, penetrating numerous Pentagon computer systems.[74] Essentially the Red Team demonstrated the asymmetric imbalance between cyber-offense and defense. Lewis, Kenneth Geers, and Krepinevich argue that cyberspace favours the attacker.[75] Defensive systems always need be on guard, whereas the attacker has the discretion to choose when to strike.[76] Even being able to keep out the low-level threats, there will always be a "small percentage of 'professionals' with largely unlimited resources that, given time, will be able to penetrate any defense."[77] Nation states are an example of such actors that have both the resources and time available conduct such activities in cyberspace.

Rid disputes the fact and argues the contrary. First, he argues that developing a cyber weapon capable of significant damage is costly in terms of time, skills, and carefully conducted target intelligence vital to operational success.[78] Secondly, offensive cyber weapons developed need to be specific to each and every operation as the potential for universal cyber weapons is less than previously thought. Finally,

---

[72] Ibid., 132.

[73] Weimann, "Cyberterrorism: The Sum of All Fears?," 138.

[74] Committee et al., *Realizing the Potential of C4I: Fundamental Challenges*, 135.

[75] James A. Lewis, *Cyberwarfare and Its Impact on International Security* (New York: United Nations Publications, 2010), 20, https://www.un.org/disarmament/publications/occasionalpapers/no-19/; Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 125, http://dx.doi.org/10.1080/15567281.2010.536735; Krepinevich, *Cyberwarfare: A "Nuclear Option"?*, 40.

[76] Committee et al., *Realizing the Potential of C4I: Fundamental Challenges*, 139.

[77] Ibid., 160.

[78] Rid, "Think Again: Cyberwar," 20.

a cyber weapon more than likely cannot be reused. After an attack, defensive measures can be put into place to prevent cyber-attacks from being repeated on the same computer and or network.[79]

In addition, coercive action by a terrorist is limited.[80] By threatening to use a cyber weapon, warning is given to targets risking compromising the mission's operational success. Even proving capabilities to a target before unleashing a major cyber-attack exposes weaknesses and security vulnerabilities that can be swiftly fixed[81] or temporarily put offline, and places security officials on high alert to be prepared and ready to fix the problem.

However, while these cyber-attacks may be temporary, they do open a window of opportunity and can therefore be useful. While it is argued that they may not be able to currently inflict death or physical damage on a large scale alone, they may be able to be used in conjunction with kinetic weapons. Otherwise, the cyber-attack is just a nuisance more than anything, as the effects are temporary and do not achieve any political or ideological goals.

The "Terror" in Cyberterrorism

The fourth criteria that needs to be met on whether an action is deemed an act of cyberterrorism or not is whether the action was designed to have far-reaching psychological repercussions beyond the immediate victim or target. As mentioned earlier, while an act may be "designed" to cause terror, it may fail to do so. However, failure does not explicitly restrict a cyber-attack from being labeled cyberterrorist attack. Lack of empirical evidence of an act cyberterrorism having occurred aside, can a cyber-attack have far-reaching psychological repercussions beyond the immediate victim or target?

---

[79] Ibid., 20; Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 60.

[80] Rid, "Think Again: Cyberwar," 20; Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 59.

[81] Ibid., 60.

Gartzke gives the example of an act of cyberterrorism, such as forcing power grids to shut down or being locked out of your bank account online. People will often not immediately presume there has been an "attack". People are used to experiencing power outages every now and then or having technical glitches with computers. Reactions evoked may be anger, frustration, or even resignation, but most certainly not terror.[82] The damage done does not cause terror, but an essential ingredient for a cyber-attack to be an act of cyberterrorism. Jones agrees with Gartzke regarding cyber-attacks impact on producing mass terror, "the majority of people are not currently so dependent on [technology] that their malfunction or absence would have the capability to cause terror."[83]

Furthermore, attribution to a cyber-attack by a terrorist is conceivably the most important factor in putting the word "terror" in cyberterrorism.[84] Gartzke argues this particular factor makes cyberterrorism particularly "ill-suited" for the task of inducing terror. For those whose computers and networks are being infiltrated and seek justice, they will be left perplexed to the identity of the assailant. However, terrorists are politically or ideologically motivated and would most definitely seek credit for an attack. Terrorists however face a major problem for conducting attacks in cyberspace. Proving a cyber-attack was their operation proves difficult. Without attribution, any cyber-attack that disrupts major infrastructures will most likely be initially assumed to be technical problems. This can also work to the advantage of the attacked state. Even with proof, a government can claim to the public that the events that caused a particular critical infrastructure to malfunction was a minor technical mishap, alleviating any possible concerns and undermining any terrorist claims to infamy. Similarly, the inability to prove whom the assailant of an attack is leaves any terrorist organization open to falsely claim a malfunction of critical

[82] Ibid., 69.

[83] Jones, "Cyber Terrorism: Fact or Fiction," 4.

[84] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 69.

infrastructure or an actual cyber-attack as their operation.[85] However, this does not necessarily cause terror.

Michael Stohl furthers this argument bringing attention the Northeast blackout of 2003 citing Lewis, "cyber terror was at first suspected in the 2003 Northeast blackout. The cause turned out to be incompetence and falling trees. The widespread blackout did not degrade U. S. military capabilities, did not damage the economy, and caused neither casualties nor terror."[86] Even when people *believed* that such an event was the work of terrorists, widespread terror was not a reaction. The ability for a terrorist to prove a cyber-attack was a product of their actions may still have little effect. This also illustrates that cyber-attacks would only be effective, if at all, in developed countries. The level of dependence on technology in underdeveloped countries would prove ineffective in the case of a cyber-attack.[87] This also limits the purpose of a cyber-attack when it comes to the types of strategies a terrorist uses in pursuit of particular goals. This will be discussed in greater detail in the final section of this paper.

While there are those that argue terror is just not possible through a cyber-attack, there are those who would disagree. For example, Ayn Embar-Seddon argues that "the level of fear that would result from the threat of shutting down a large portion of the power grid would very likely be as great as, if not greater than, the level of fear that would result from the threat of downing an airliner."[88] All other critical infrastructures depend on electricity; there is no substitute. Geers argues that governments should

---

[85] Conway, "Against Cyberterrorism," 28.

[86] James A. Lewis, "The War on Hype: The Deadly Terror Lurking Around the Corner May Not Be Such a Big, Ominous Threat after All," *San Francisco Chronicle*, February 19, 2006, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/02/19/INGDDH8E2V1.DTL; Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," 234.

[87] Jones, "Cyber Terrorism: Fact or Fiction," 5; Hardy, "Operation Titstorm: Hacktivism or Cyberterrorism," 501; Weimann, "Cyberterrorism: The Sum of All Fears?," 131.

[88] Ayn Embar-Seddon, "Cyberterrorism: Are We Under Siege?," *American Behavioral Scientist* 45, no. 6 (2002): 1038, http://dx.doi.org/10.1177/0002764202045006007.

therefore begin by evaluating the security of their "life-line industries."[89] Jonathan Matusitz argues that attacking a power grid, for example, can bring about a "cascading failure," a ripple effect where the failure of one important node in a network can overload the next and overwhelm the network causing mass failure.[90] These interconnected parts of some critical infrastructures are dependent on preceding parts, which without, successive parts cannot operate. Not only can a single cyber-attacker launch numerous viruses from the same location, they can also launch these viruses simultaneously to multiple targets as if they were more than one person.[91] Matusitz therefore believes this gives cyberterrorists a distinct advantage over the use of physical attacks, "because a single conventional terrorist incident cannot, in and of itself, jeopardize our national critical infrastructures."[92] Matusitz provides an example, stating although the Twin Towers on 9/11 caused mass terror across the U.S., major infrastructures continued to function, including airports and businesses.[93]

Knowing Who Conducted the Cyber-Attack

Finally, for an act to be considered an act of cyberterrorism it has to conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and perpetrated by a subnational group or non-state entity. However, as stated previously, attribution in cyberspace can prove extremely difficult.

---

[89] Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," 127.

[90] Jonathan Matusitz, "Cyberterrorism: Postmodern State of Chaos," *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 119, http://dx.doi.org/10.1080/15567281.2010.536733.

[91] Ibid., 117.

[92] Ibid.

[93] Ibid.

To begin with, very little digital evidence is left behind from a cyber-attack to trace back to the attacker. As David Chaikin describes, "Digital evidence is different from evidence created, stored, transferred and reproduced from a non-digital format. Digital evidence has been described as ephemeral in nature, not reproducible, easily manipulated and inherently suspicious."[94] Digital evidence is limited in nature and temporary. The defenders of a cyber-attack have to act fast or their chances of tracing the attack back to the assailant's origin dwindles.[95]

If a trace is not established during or shortly after a cyber-attack, it is unlikely that an origin can be traced. This is further complicated by the fact that it is not always clear whether certain activity is "hostile". At first, certain activities could be seen as routine or simply a minor malfunction. As will be seen with the case studies below, this delay in reaction to infiltration may be crucial to tracing the origins of the attack. Digital evidence in cyberspace is highly problematic in nature and is an important issue in regards to cybersecurity and the attribution dilemma. Without evidence of who the attacker is, justice, retaliation, or a counter-strike cannot be delivered.

Even if those being attacked are quick enough to respond and establish a trace, attribution to the assailant is difficult.[96] Attackers also have the added benefit of being able to mislead those seeking their identity by using others' networks and computers.[97] While motive may be a good indicator as to whom the attacker may be, it is insufficient evidence to prove attribution. Further investigation is required before an identity can be revealed since digital evidence is easily manipulated. Had the defender been

[94] David Chaikin, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence," *Crime, Law and Social Change* 46, no. 4–5 (2006): 241.

[95] Krepinevich, *Cyberwarfare: A "Nuclear Option"?*, 47.

[96] Ibid.; Lewis, *Cyberwarfare and Its Impact on International Security*, 9; Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," 126; Goodman, Kirk, and Kirk, "Cyberspace as a Medium for Terrorists," 196.

[97] Krepinevich, *Cyberwarfare: A "Nuclear Option"?*, 4.

able to trace the attack to the "origin", the defenders could end up believing the source discovered is somebody they are not; a diversionary tactic used to create a red herring. The attacker can mislead the defenders from discovering their identity by using proxies, sending their traffic through other people's computers and networks across the globe.[98] Another way is the use of a botnet,[99] in this case, the wrong actors, state or non-state can be accused and be victims of unwarranted counter-strikes, cyber or digital. Even with the assailant "caught", they cannot automatically be assumed to be sponsored by a particular state or terrorist group based on location, nationality, or language.[100]

Without clear knowledge of who the assailant of a cyber-attack is, how can it be distinguished whether the attack was conducted by a nation state, a chaotic actor or vigilante, a terrorist, or even a regulator whose actions may have accidently caused cascading failures that could not have been predicted? A cyber-attack that is violent can be any number of actors in cyberspace. The debates in this area of research are partly a result of terminological disputes and partly a result of confusion of who the assailants are.

[98] Ibid., 48.

[99]

[100] Singer and Friedman, *Cybersecurity and Cyberwar*, 74; Jones, "Cyber Terrorism: Fact or Fiction," 5.

CASE STUDIES

The following section will examine three case studies: the *Maroochy Shire Cyber-Attack*, the *Stuxnet Virus*, and the *Cyber-Attack on the Ukrainian Power Grid*. As will be illustrated, none of these cases are acts of cyberterrorism as defined in this study. However, these three cases do offer parallels that can be drawn upon to provide insight on the threat of cyberterrorism and judge the effectiveness of cyberterrorism in terms of achieving a terrorists goals. The Maroochy Shire cyber-attack was chosen as a case study because it illustrates the dangers of insiders; the importance of security protocols and controls in place; the vulnerabilities present in computer systems and industrial control systems; and the capabilities of a cyber-attack to cause physical damage. The Stuxnet virus was included as a case study because it illustrates that high-level cyber-attacks require vast resources, intelligence, skill, and time; as well as the capability of cyber-attacks to achieve physical damage. The cyber-attack on the Ukrainian power grid was selected because it was the first cyber-attack on a nation-state's electric grid – demonstrating the vulnerabilities to critical infrastructures; the capabilities of a cyber-attack to disrupt services; that more developed countries may be more vulnerable to cyber-attacks; that such an attack requires vast resources, reconnaissance, skill, and time; the importance of security protocols and controls in place; and that other cyber operations could increase the effects of terrorist attacks.

These cases are presently the most detailed cases open to the public and therefore provide a rich amount of information for analysis. They are representative of cyber-attacks that have demonstrated the capability of cyber-attacks resulting in actions in the physical world, and are therefore highly important when assessing the overall threat of cyberterrorism. Each case will be divided up into a brief overview of the cyber-attack, a quick assessment of whether the act could be considered cyberterrorism, followed by a section illustrating the implications of the cyber-attack as they relate to cyberterrorism.

Case I: Maroochy Shire Cyber-Attack

The Cyber-Attack

In 2000, disgruntled Australian man, Vitek Boden was turned down for a job at the Maroochy Shire Council. In retaliation to rejection of employment, the man infiltrated and remotely accessed the Maroochy Shire Council's computer system and proceeded to unleash 800,000 litres of raw sewage into rivers and parks along the Sunshine coast, causing extensive contamination.[101] He achieved this, between February 9 and April 23, 2000, by driving around the area in his car with a laptop computer and stolen radio equipment that had the capability to communicate with the Maroochy Water Services Sewage SCADA systems.[102] The radio commands were able to electronically change data causing alarms to be disabled, pumps to malfunction, and a disruption in communication between the central computer and various pumping systems.[103]

Noticing that there had been malfunctions in the system, the Maroochy Shire Council appointed Mr. Yager, a Hunter Watertech employee, to investigate. Checking the pumping stations, it was found that there was no physical damage or tampering. Mr. Yager achieved a temporary success when he was able to program the system to exclude the malicious code from altering the system. This did not last long, and for a short period of time Mr. Yager's access to the network was blocked. Mr. Yager, eventually concluded that human interference must be the cause of the disruption in the network. Eventually suspicions that Boden may be the culprit arose and he was put under surveillance. Boden was caught and arrested by chance when a Police officer pulled him over for a traffic violation; it was later discovered that the man

---

[101] Angela Clem, Sagar Galwankar, and George Buck, "Health Implications of Cyber-Terrorism," *Prehospital and Disaster Medicine* 18, no. 3 (2003): 274, http://www.journals.cambridge.org/abstract_S1049023X00001163; Matusitz, "Cyberterrorism: Postmodern State of Chaos."

[102] Marshall Abrams and Joe Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*, 2008, 4, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

[103] Ibid., 5.

had worked for Hunter Watertech, the company that designed and installed the sewage treatment plant's SCADA system.[104]

Assessment

Boden has been titled a cyberterrorist.[105] His actions however, do not meet this criteria. While the attack was perpetrated by a non-state entity, conducted via cyberspace, and caused damage to property, ultimately, the cyber-attack was a result of a disgruntled individual whose aims and motives were revenge, rather than political or ideological, and whose attack was not designed to have far-reaching psychological repercussions beyond the immediate victim or target. Boden would arguably be considered a chaotic actor (see *Table 4*).

Table 4. Categorization of the Maroochy Shire Case Study

Cyberterrorism Criteria	Maroochy Shire Case Study	Chaotic Actors	Cyberterrorism
Executed via cyberspace	✓	✓	✓
Ineluctably political or ideological in aims and motives	X	X	✓
Violent or threatens violence	✓	–	✓
Designed to have far-reaching psychological repercussions beyond the immediate victim or target	X	–	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	X	X	✓
Perpetrated by a subnational group or non-state entity.	✓	✓	✓

[104] Ibid., 1.

[105] Matusitz and Minei, "Cyberterrorism: Its Effects on Health-Related Infrastructures," 164.

Implications

The Maroochy Shire case demonstrates a number of important considerations in regards to cyberterrorism. To begin with, Boden was an insider. Having an insider with the motive and capabilities to cause damage is the ultimate vulnerability. While Boden was not an employee of the organization he attacked itself, he was an employee of the contractor, Hunter Watertech. As Abrams and Weiss note, "the attack by an insider who is not an employee demonstrates several critical physical, administrative, and supply chain vulnerabilities of industrial control systems."[106] Hunter Watertech designed and installed the sewage treatment plant's SCADA system for the Maroochy Shire Council.[107] With access to all of the right tools and equipment from Hunter Watertech, Boden ultimately had immediate and direct access to the SCADA systems for the water treatment plant.[108] With the motive and know-how, the Maroochy Water Services essentially became a playground for Boden's wrath. This case not only demonstrates the threat of insiders, but the threat of radicalized insiders.

Furthermore, Boden was able to mask his actions in cyberspace. In order to even determine that the malfunctions were not defects or glitches in the software, thorough digital forensics was necessary.[109] Civil engineer Robert Stringfellow was in charge of the water supply and sewage systems at the time of infiltration.[110] As reported by Jill Slay and Michael Miller,

> Stringfellow commented that at first it was easier to blame installation errors for the problems. However, upon reinstalling all the software and checking the system, he noticed that pump

---

[106] Abrams and Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*, 16.

[107] Ibid., 8.

[108] Denning, "Stuxnet: What Has Changed?," 674.

[109] Abrams and Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*, 8.

[110] Jill Slay and Michael Miller, "Lessons Learned from the Marchoory Water Breach," in *Critical Infrastructure Protection*, ed. Eric Goetz and Sujeet Shenoi (Boston: Springer, 2008), 78, http://www.springer.com/us/book/9780387754611.

> station settings kept changing beyond the ability of the system to do this automatically. He, therefore, concluded that an external malicious entity was responsible.[111]

Defending against insider cyber-attacks is challenging. In many cases, it is unlikely that the first reaction to malfunctioning of SCADA systems is the cause of a cyber-attack. It is after-all commonplace to experience glitches in the system and malfunctions with computers and networks. This is valuable time that can be used to trace the assailant. More often than not, radio communications used in SCADA systems lack proper configuration and are commonly insecure.[112] Observations by Stringfellow as reported by Slay and Miller state "it is often that case that security controls are not implemented or not used properly."[113] Something as simple as following protocol can make the difference.

Moreover, the Maroochy Shire case illustrates that physical harm from a cyber-attack is very possible. Australian Environmental Protection Agency representative Janelle Bryant expressed, "marine life died, the creek water turned black and the stench was unbearable for residents."[114] While human lives were not the victims of this incident, the Maroochy Shire case still demonstrates the destructive capability of a cyber-attack. Had a terrorist with the same direct and immediate access to a critical infrastructure's SCADA systems with the intention on causing mass damage to persons are property, the result could be devastating.

Ultimately, the Maroochy Shire case demonstrates the dangers of insiders to security, the importance of security protocols and controls in place, the vulnerabilities present in computer systems and industrial control systems, and the capabilities of a cyber-attack to cause physical damage.

---

[111] Ibid., 79.

[112] Abrams and Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*, 8.

[113] Slay and Miller, "Lessons Learned from the Marchoory Water Breach," 79.

[114] Tony Smith, "Hacker Jailed for Revenge Sewage Attacks," *WWW The Register*, October 31, 2001, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

Case II: The Stuxnet Virus

The Cyber-Attack

In 2010, just three years after President Bush reportedly requested and received $400 million from Congress to fund major escalations in covert operations aimed at undermining Iran's nuclear ambitions, it would be discovered that the Iranian nuclear facility at Natanz was victim of a cyber-attack; a cyber worm[115] that became to be known as Stuxnet.[116] It was the first of its kind. Agreeing with many experts, Ivanka Barzashka claims it is "the world's first-known cyber-weapon to target critical industrial control systems."[117] While Stuxnet began reaching headlines in the spring and summer of 2010, Stuxnet spread over the course of several months worldwide since 2009; evidence suggests that an earlier version was unleashed in 2007.[118]

While Stuxnet was reported to infect over 100,000 computers worldwide, 50 to 60 percent were concentrated within Iran.[119] Initially, this gave some insight into Stuxnet's purpose and likely targets. However, the absence of digital evidence had kept the assailants shrouded and has at least given any accused plausible deniability. While no one has officially declared ownership of the worm, speculation

---

[115] A *worm* is "a type of malware that spreads automatically over a network, installing and replicating itself. The network traffic from rapid replication and spread can cripple networks even when the malware does not have a malicious payload," Singer and Friedman, *Cybersecurity and Cyberwar*, 299.

[116] Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, Kobo Ed. (New York: Crown Publishers, 2014), chap. 16; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 23.

[117] Ivanka Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," *The RUSI Journal* 158, no. 2 (2013): 48, http://www.tandfonline.com/doi/abs/10.1080/03071847.2013.787735.

[118] Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, chap. 15; Thomas M. Chen and Saeed Abu-Nimeh, "Lessons from Stuxnet," *Computer* 44, no. 4 (2011): 91; Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," 50.

[119] Other countries included China, Indonesia, Australia, India, South Korea, Malaysia, Azerbaijan, the United Kingdom, Finland, Germany, and the United States found traces of Stuxnet as well, Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 23; Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," 50; Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, chap. 15.

initially spread that the United States and Israel were accountable.[120] Since then, the Stuxnet virus has been confirmed by leaked documents to be a joint operation between these states, with the U.S. leading the operation.[121]

Unlike most malware, Stuxnet had very specific conditions that had to be met before unleashing its contents. Stuxnet was state-of-the-art; its complex structure revealed that a vast amount of resources and time, as well as in-depth intelligence was required for its creation and deployment. Ultimately, the purpose of the Stuxnet virus has been widely accepted to be the delaying of Iran's nuclear program at Natanz by destroying vital centrifuges and therefore disrupting their uranium enrichment process that is fundamental to the creation of nuclear weapons.[122]

Looking at the code, one can see the precision that was required, not only for the virus to get to where it needed to go, but also for the virus to accomplish what it was trying to achieve. To begin with, Stuxnet was written in multiple computer languages and carried exploits for four "zero-day" unpatched vulnerabilities.[123] A Zero-Day is "an attack that exploits a previously unknown vulnerability; taken from the notion that the attacks takes places on the zeroth day of the awareness."[124] These vulnerabilities are not easily acquired and it was rare to have more than one for a single virus.[125] Stuxnet had a very specific purpose and was crafted with the means to assure its purpose was fulfilled.

---

[120] Denning, "Stuxnet: What Has Changed?," 673; Singer and Friedman, *Cybersecurity and Cyberwar*, 117; Chen and Abu-Nimeh, "Lessons from Stuxnet," 93; Irving Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity," *Georgetown Journal of International Affairs – Special Issue: International Engagement on Cyber* 1 (2011): 121; Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 63.

[121] Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, chap. 14.

[122] Ibid., chap. 18.

[123] Chen and Abu-Nimeh, "Lessons from Stuxnet," 91.

[124] Singer and Friedman, *Cybersecurity and Cyberwar*, 299.

[125] Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, chap. 6.

Kim Zetter provides a good description of cyber weapons: "Like conventional weapons, most digital weapons have two parts—the missile, or delivery system, responsible for spreading the malicious payload and installing it onto machines, and the payload itself, which performs the actual attack, such as stealing data or doing other things to infected machines."[126] What made Stuxnet state-of-the-art and very unique was its ability to target and infiltrate industrial control systems (ICS). Upon penetration of the cybersecurity defenses, Stuxnet then manipulated code within the programmable logic controller (PLC). This ultimately allowed Stuxnet to surgically infiltrate and control the centrifuges at Natanz and to maliciously and quietly cause them to spin out of control until they were damaged.[127] Stuxnet was able to deceive workers by digitally providing the correct variables as if normal operation was in action. By the time those in charge of overseeing the centrifuges operations were aware that there was something wrong, the damage was already done.[128]

Assessment

The Stuxnet was considered an act of cyberterrorism by the Iranian government.[129] However, the attack cannot be considered as such. While the attack was conducted via cyberspace, caused damage to property, may have been designed to have far-reaching psychological repercussions beyond the immediate attack on Iran, and was ineluctably political in aims and motives, ultimately Stuxnet can be categorized as an act of cyberwarfare as it was conducted by the United States and Israel *(see Table 5).*

[126] Ibid., chap. 4.

[127] Denning, "Stuxnet: What Has Changed?," 673.

[128] Chen and Abu-Nimeh, "Lessons from Stuxnet," 93.

[129] Conway, "Against Cyberterrorism," 26.

Table 5. Categorization of the Stuxnet Virus Case Study

Cyberterrorism Criteria	Stuxnet Virus Case Study	Cyberwarfare	Cyberterrorism
Executed via cyberspace	✓	✓	✓
Ineluctably political or ideological in aims and motives	✓	✓	✓
Violent or threatens violence	✓	–	✓
Designed to have far-reaching psychological repercussions beyond the immediate victim or target	✓	–	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	X	X	✓
Perpetrated by a subnational group or non-state entity.	X	X	✓

Implications

Information in the public domain is limited on the subject and facts regarding Stuxnet's destructibility at Natanz cannot be verified. Furthermore, information can be bias as a result of potential Iranian government misinformation campaign.[130] Upon assessing Stuxnet's impact on the Iranian enrichment program, Barzashka concludes that the virus was not as successful or effective as originally accepted and even goes so far to say that Iranian enrichment had improved since they the attack.[131] His analysis is based off of technical information published and provided by the Symantec Corporation, Kaspersjy Labs, and ESET.[132] Be that as it may, while Barzashka provides a fresh perspective and analysis

[130] Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," 50.

[131] Ibid., 54.

[132] *For a detailed report on the Stuxnet Virus see,* Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier* (Cupertino, 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Kaspersky Lab, "Kaspersky Lab Provides Its Insights on Stuxnet Worm," *Virus News*, September 24, 2010, http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm; Aleksandr Matrosov et al., "Stuxnet Under the Microscope," *Eset* (2010): 1–85, http://ece.wpi.edu/~dchasaki/papers/Stuxnet_Under_the_Microscope.pdf.

of the effect of the Stuxnet virus, it does not detract from the significance that Stuxnet has brought to the cyber world.

Using Stuxnet as a case study has a number of implications as it relates to cyberterrorism. To begin with, Stuxnet is a case where physical damage was done to ICS. Stuxnet, being a relatively recent event, had illustrated that critical infrastructures are no longer safe from being infiltrated. This is important, because critical infrastructures are more than likely the biggest targets of terrorists as they offer the most potential violence and terror when disrupted or destroyed.

The nuclear facility at Natanz was allegedly "air-gapped." This means that the system was not directly connected to the Internet, a method used to prevent malware and cyber-attacks from infiltrating systems.[133] Singer and Friedman address the air-gapped issue stating, "at some point, old data needs to come out, and new instructions need to go in. Systems need to be patched, updated, and maintained",[134] that is new data or software needs an access point, which is a vulnerability. In 2002, Green argued that "nuclear weapons and other sensitive military systems enjoy the most basic form of Internet security: they're 'air-gapped,' meaning that they're not physically connected to the Internet and are therefore inaccessible to outside hackers."[135] Yet, Stuxnet was able to spread to the Natanz nuclear facility regardless of this security measure in place via USB and software that was inserted by clandestine means.[136]

More advanced cyber weapons have since been engineered. For example, other cyber-weapons similar to Stuxnet have since been freed into cyberspace to achieve their designer's aims, such as *Flame* and *Duqu*. While both Flame and Duqu utilize Stuxnet's code, they were created for different purposes.

---

[133] Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity," 124.

[134] Singer and Friedman, *Cybersecurity and Cyberwar*, 63.

[135] Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly*, 2002, para. 9, http://werzit.com/intel/regions/cyber/articles/archives/Myth of Cyberterrorism.pdf.

[136] Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*, chap. 4.

Flame was created to secretly map and monitor Iranian networks where as Duqu secretly collects data. Both resemble Stuxnet using similar means to achieve different ends.[137] These sort of cyber weapons could be used for cyber espionage operations by terrorists to collect information that can be used in future cyberterrorism or terrorist operations that use kinetic weapons.

Cyber espionage has an additional advantage over human intelligence, as information can be collected without leaving the territory of the sponsoring state.[138] Vice-versa, cyber espionage can be conducted inside another state to avoid the true identity of the assailant. Anonymity, as a result of the often lack of digital evidence, results in the inability of infiltrated states to lay attribution. This contributes to a safer and more cost effective method of intelligence collection for terrorists making this form of cyber activity both desirable and popular. However, if the desired ends were destruction rather than reconnaissance, the code is similar enough to allow changes to be made to achieve the desired effect. Most malware is not developed from scratch, but altered and expanded on to in order to generate a renewed variant.[139] Stuxnet has thus provided hackers, and potentially terrorists, with a new means and use for cyber activity.

Stuxnet had a clear purpose, and a very specific target; that's how it was programmed. While the thousands of computers that were infected were not damaged, they served the purpose of transporting the worm to where it needed to go, air-gapped system or not. Given the potential that a Stuxnet-like virus was to include multiple targets, with multiple parameters, with multiple variables, and several different commands to be used when certain circumstances are met, the potential could be catastrophic.

However, this is where Stuxnet has proved its value as a case study as it relates to cyberterrorism. Stuxnet was not easily created: it required vast resources, intelligence, skill, and time. Where a nation

[137] Denning, "Stuxnet: What Has Changed?," 674.

[138] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 70.

[139] Denning, "Stuxnet: What Has Changed?," 675.

state can be patient, terrorists do not have the luxury to waste time and money on an operation that may fail. All it takes is one parameter to be changed, and the code written for such a cyber weapon could inexplicitly fail. With all that could go wrong during such an operation, it would make more sense to use kinetic weapons, a more proven and effective mean, to achieve their goals.

Case III: Cyber Attack on the Ukrainian Power Grid

The Cyber-Attack

On December 23, 2015, power outages were reported across a number of different areas in Ukraine. However, this was no ordinary power outage that often come from severe weather, the computer and SCADA systems of three Ukrainian regional electricity distribution companies were infiltrated remotely by external attackers. Several substations were pulled offline in a coordinated and synchronized attack that resulted in the loss of power to approximately 225,000 people for three hours.[140]

While malware was discovered in the computer and SCADA systems, they were not the primary cause of the disruption. Instead, the power outages were caused by the direct use of the software and control systems that the companies used. Malwares KillDisk and BlackEnergy3, as well as other tools and technology used, only enabled the cyber-attack or delayed efforts to restore power.[141]

SANS ICS and Electricity Information Sharing and Analysis Center (E-ISAC)'s analysis of the cyber-attack on the Ukrainian power grid indicated that "These incidents should be rated on a macro scale as low in terms of power system impacts as the outage affected a very small number of overall power consumers in Ukraine and the duration was limited", though they also point out "it is likely that the impacted companies rate these incidents as high or critical to the reliability of their systems and business

[140] ICS-CERT, "Cyber-Attack Against Ukrainian Critical Infrastructure (IR-ALERT-H-16-056-01)," *Industrial Control Systems Cyber Emergency Response Team*, last modified 2016, accessed November 10, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[141] E-ISAC and SANS, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, D.C., 2016), 3, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

operations."[142] Therefore, while the power outage may have been a minor inconvenience to most consumers, it would have had a higher impact on businesses.

Ukrainian government officials asserted that the Russian security services were responsible for the cyber-attack on their power grid. However, they have declined to provide proof to back up these claims.[143]

Assessment

The cyber-attack on the Ukrainian power grid illustrates the complexity for categorizing cyber-attacks. We know the attack was conducted via cyberspace and that it caused disruption of the power grid that effected thousands of people. However there are still a lot of unknowns.

Robert M. Lee, former cyber warfare operations officer for the U.S. Air Force and co-founder of Dragos Security, assisted in the investigation of the incident. Lee has stated that the cyber-attack was designed to send a message, and thus we can assume it was designed to have far-reaching psychological repercussions beyond the immediate victim or target.[144] We can also therefore make the assumption that the attack was likely political in aims. While Ukraine was quick to point fingers at Russia for the cyber-attack, no proof has been provided and therefore attribution cannot be established so quickly. Given this unknown element, the attack could very well be categorized as one conducted by chaotic actors. Technically, the possibility remains that the attack was conducted by terrorists, though the lack of announcement by a terrorist group makes this highly unlikely. Taking into consideration that the attackers had the "capability to perform long-term reconnaissance operations required to learn the environment

[142] Ibid., vi.

[143] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* (Boone, IA, March 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[144] Ibid.

and execute a highly synchronized, multistage, multisite attack",[145] and that the political tensions between the two nation-states, it is more likely that Russia was behind the attacks. If we were to make this assumption, then the cyber-attack could be categorized as cyber-warfare (see *Table 6*).

Table 6. Categorization of Ukrainian Power Grid Case Study

Cyberterrorism Criteria	Ukraine Power Grid Case Study	Cyberwarfare	Chaotic Actors	Cyberterrorism
Executed via cyberspace	✓	✓	✓	✓
Ineluctably political or ideological in aims and motives	✓	✓	–	✓
Violent or threatens violence	✓	–	–	✓
Designed to have far-reaching psychological repercussions beyond the immediate victim or target	✓	–	–	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	–	X	X	✓
Perpetrated by a subnational group or non-state entity.	–	X	✓	✓

Implications

The cyber-attack on the Ukrainian power grid as a case demonstrates a number of important considerations in regards to cyberterrorism. To begin with, the most important implication of this case study is that this cyber-attack was the first recorded cyber-attack to have caused disruption to a nation's critical infrastructure, and therefore the first civilian target.[146] In this particular case, power was the target. Without power, nothing else functions and this could have a cascading effect on other critical

[145] E-ISAC and SANS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2.

[146] Ibid., 20.

infrastructure. This makes the power grid a very likely target of terrorists looking to cause the most destruction, disruption, and chaos.

Second, the joint SANS ICS and E-ISAC report has stated that this cyber-attack was not "inherently specific to Ukraine Infrastructure", and that "the impact of a similar attack may be different in other nations, but the attack methodology, tactics, techniques, and procedures observed are employable in infrastructure around the world."[147] However, one noticeable difference between Ukraine and many other developed countries around the world is that Ukraine still had the capability to return to manual control. CEO of the Canadian Electricity Association, Francis Bradley has stated that the United States and Canada for example have slowly removed the capability to return to analog controls, meaning in a similar situation, it may prove extremely difficult to bring the power back online.[148] In countries where operations have increasingly moved online and backup analog systems have been removed to increase efficiency and decrease costs, cyber-attacks may prove more effective in more developed countries.

Third, like the Stuxnet virus, this cyber-attack illustrates the amount of resources, reconnaissance, skill, and time required for a successful operation. Over a six month period, the assailants conducted reconnaissance where they harvested credentials and information necessary to gain access to the ICS network.[149] This cyber-attack took a great deal of planning for the synchronized, multisite, multistage attack to be carried out just right. As mentioned before, terrorists do not have the luxury to waste time and money on an operation that may ultimately fail.

It is worth noting that this case offers examples of how terrorists could use cyberspace to multiply the effects of their terrorist attacks, regardless of the attack itself not being an act of cyberterrorism. In

---

[147] Ibid.

[148] Canadian Association for Security and Intelligence Studies, "Private Sector and Critical Infrastructure," in *The Cyber Challenge* (Ottawa: CASIS, 2016), http://www.casis-acers.ca/wp-content/uploads/2016/11/Final-Summary-Highlights-from-the-CASIS-2016-Annual-Symposium.pdf.

[149] E-ISAC and SANS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 12.

this case, thousands of calls were generated by the attackers to the energy company's call center in order to deny access to customers reporting outages.[150] If this sort of operation can take place, in theory it would also be possible to flood the lines of emergency services – thus delaying response time of the attack. This is one are that further research is required and beyond the scope of this paper.

Ultimately, the cyber-attack on the Ukrainian power grid demonstrates that critical infrastructure is vulnerable to cyber-attacks; the capabilities of a cyber-attack to disrupt the power grid; that developed countries may be more vulnerable to cyber-attacks; that such an attack requires vast resources, reconnaissance, skill, and time; the importance of security protocols and controls in place; and that other cyber operations could increase the effects of terrorist attacks.

[150] Ibid., 2.

AN ANALYSIS OF CYBERTERRORISM AS A STRATEGY

Cyber-attacks have the potential to destroy infrastructure machinery, infiltrate into the controls of a facility handling hazardous materials, a nuclear power plant or a dam, or cause the breakdown of power grids. Not only are cyber-attacks on critical infrastructure becoming more common, their ability to inflict more destructive physical damage is evolving. Both the Stuxnet and Maroochy Shire case studies have demonstrated that physical damage to persons or property is a real risk. The cyber-attack on the Ukrainian power grid illustrated that critical infrastructure is also vulnerable to disruption through cyber-attacks. Had malicious code been used instead of just disabling the power, as demonstrated by Idaho National Labs, power generators could have been made to self-destruct causing more permanent damage and a longer power outage. The destructibility and effects of a cyber-attack is no longer the subject of science fiction – and terrorists know this as well. Of course, a terrorist could accomplish this by the use of kinetic weapons. Therefore, cyberterrorism would have to prove to be an effective means in pursuing terrorists' goals to be considered a threat.

While the possibility of a cyber-attack to be violent has been demonstrated, there are other factors that should be taken into consideration when assessing the likely use of cyber weapons by terrorists over kinetic weapons. First, what are the common goals and principal strategies of these terrorist groups? Is cyberterrorism an effective means to achieving these goals? Second, can cyber-attacks provide the same terror factor that kinetic weapons can? Third, do these terrorists have access to the funds, skill, and technology required to conduct a cyber-attack capable of causing violence? Is there an attraction of cyber weapons over kinetic weapons? A final section will look at the bigger picture of cyberterrorism.

The Goals and Strategies of Terrorism

As Andrew H. Kydd and Barbara F. Walter claim, "Terrorism works not simply because it instills fear in target populations, but because it causes governments and individuals to respond in ways that aid the terrorists' cause."[151] When assessing the likelihood of cyberterrorism, it is therefore important to examine terrorist goals and how cyberterrorism can fit in their strategies in pursuit of these goals. Kydd and Walter provide an excellent overview of known terrorist organizations as designated by the U.S. State Department, and their primary goals. These ultimate goals, while varied over time, had five which endured in importance: regime change, territorial change, policy change, social control, and status quo maintenance.[152] Along with these goals, Kydd and Walter identified five principal strategies that terrorist organizations employed in pursuit of their goals, namely attrition, intimidation, provocation, spoiling, and outbidding.[153] By cross-examining Kydd and Walter's research with the characteristics and assumptions that have been presented in this paper about cyberterrorism, it is revealed that cyberterrorism can only serve a very specific purpose.

Terrorist Goals

Academics, journalists, and policymakers occasionally forget that terrorists are more often than not concentrating their efforts in their own region. For example, while one of Al-Qaeda's main goals is to expel the U.S. from the Muslim world, they also seek to overthrow apostate regimes, replacing them with Islamic governments, and creating a society of true Muslims.[154] Many terrorist organizations – if not most

[151] Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (2006): 50.

[152] Ibid., 52.

[153] Ibid., 51.

[154] Daniel Byman, *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know*, *Intelligence and National Security*, Kobo Ed. (New York: Oxford University Press, 2016), chap. 3.

– have more locally focused goals in mind.[155] The Islamic State, for example, is more concerned with building a state, purifying it, and expanding.[156] While terrorist attacks on the West by the Islamic State occur, it is not what drives them.

This is what Kydd and Walter's research has shown. The goals of regime change and territorial change, are the most popular two goals of the surveyed terrorist groups. The least two popular goals surveyed, social control and maintaining status quo, are also more locally concentrated. A majority of these terrorist organizations live in less developed countries where they are in pursuit of these goals. However, as argued earlier and demonstrated in the Ukrainian power grid case, cyber-attacks would be more effective, if not only effective, in more developed countries, or developing in the case of Ukraine – specifically those that have moved their operations to computer systems and networks. Many of these less developed countries would have purely analog control systems in place, or at least a lesser dependence on them, making cyberterrorism less effective, if not completely useless. There are however exceptions to this case. Even in the case where critical infrastructure in these countries is dependent on ICS and experiences a cyber-attack, these countries are even more likely to ignore it as a commonplace. Given that these four goals generally focus on the population or regional population of a terrorists group, the use of kinetic weapons are more likely to be used given their record of being more reliable, easier to get access to, and easier to deploy in such an environment.

Ruling out the above 4 popular goals of terrorists, this leaves policy change as the likely only option for cyberterrorism. Policy change is a category of lesser demands. While these goals can be focused on a terrorist group's own population, like the four other goals mentioned above, they can also be directed

[155] Ibid., chap. 8.
[156] Ibid.

towards their enemies, near and far. Al-Qaida for example, demands the U.S. drop support for Israel and corrupt Arab regimes such as Saudi Arabia.[157]

Therefore, terrorist organizations existing at this time – more specifically, jihadist terrorists – are more likely to only use cyberterrorism in pursuit of policy change goals of more developed countries that are more highly connected in cyberspace. Furthermore, they are likely to continue using kinetic weapons for their more locally focused goals.

Terrorist Strategies

With policy change remaining the only likely goal that current terrorist organizations are likely to pursue using cyberterrorism, the strategies that terrorists could adopt that make use of cyber weapons becomes limited. Kydd and Walter identified five principal strategies that terrorist organizations employed in pursuit of their goals, namely intimidation, provocation, spoiling, outbidding, and attrition.

Intimidation

> Terrorists using intimidation try to convince the population that the terrorists are strong enough to punish disobedience and that the government is too weak.[158]

To begin with, Kydd and Walter argue that weak states and rough terrain facilitate a strategy of intimidation. Furthermore, an intimidation strategy is focused mainly on regime change or social change.[159] However, developed states that are vulnerable to cyberterrorism are not usually weak states. Though it is worth arguing that cyberspace is a "rough terrain" and allows terrorist groups to operate clandestinely. While it could be argued that a strategy of intimidation may be capable achieving a goal of policy change, as will be discussed further following this section, the ability of cyber weapons to have the same terrorizing impact that kinetic weapons have is a highly debated issue.

---

[157] Kydd and Walter, "The Strategies of Terrorism," 53.

[158] Ibid., 51.

[159] Ibid., 67.

Provocation

> A provocation strategy is an attempt to induce the enemy to respond to terrorism with indiscriminate violence, which radicalizes the population and moves them to support the terrorists.[160]

Second, Kydd and Walter argue that a strategy of provocation is mainly used in pursuit of regime change and territorial change. For this strategy to work, a population must support this goal as well. Given the limits of cyberterrorism in some of the more local goals of terrorists, it is unlikely to prove a useful strategy. A terrorist group would be incapable of provoking a strong state's population to the point where its own citizenry turn against it, especially from a cyber-attack that may not prove to have a far-reaching psychological effect or have a long lasting impact.

Spoiling

> Spoilers attack in an effort to persuade the enemy that moderates on the terrorists' side are weak and untrustworthy, thus undermining attempts to reach a peace settlement.[161]

Third, similar to the above strategies, a spoiling strategy is more locally oriented, thus rendering cyber-attacks as particularly inefficient given there may not be many targets available that could effectively have the desired impact. Kinetic weapons would be better suited to have an influence on peace settlements. Cyberterrorism is unlikely to be capable of causing mistrust between two groups in peace talks.

Outbidding

> Groups engaged in outbidding use violence to convince the public that the terrorists have greater resolve to fight the enemy than rival groups, and therefore are worthy of support.[162]

Fourth, outbidding is a strategy used when there is a competition between two or more domestic parties for leadership of their side as well as a population that has uncertainty as to which groups best represent their interests.[163] Given that this strategy is once again focused on local populations, it is doubtful that cyberterrorism would be capable of pursuing an outbidding strategy. While using cyberspace in the form

---

[160] Ibid., 51.

[161] Ibid.

[162] Ibid.

[163] Ibid., 76.

of social media and propaganda may prove an effective tool to create uncertainty about certain parties, as argued in this paper this does not constitute as cyberterrorism.

Attrition

> In an attrition strategy, terrorists seek to persuade the enemy that the terrorists are strong enough to impose considerable costs if the enemy continues a particular policy.[164]

Attrition is likely the only strategy that will be of use to a terrorist using cyber weapons and once again limited to those countries which are developed and have a higher dependence on technology. An attrition strategy is focused on exhausting the enemy's resources and inflicting considerable costs. Concessions are more likely to be granted by the target if future costs from attacks are credible.[165] However, even this strategy is not perfect for terrorists to use cyberterrorism. While the costs of cyber-attacks can be immense, once a cyber-attack has occurred, the vulnerabilities can be patched making a future threat less credible, thus weakening the overall strategy of attrition. Given that high-level attacks require a vast amount of funds, intelligence, and time to be successful, it may be easier still to use kinetic weapons. With this knowledge, governments can focus on countermeasures related to strategies of attrition.

Counter-Cyberterrorism Measures

Kydd and Walter identify five counterstrategies available to a state engaged in a war of attrition. These counterstrategies remain relevant to cyberterrorism as well and are therefore worth mentioning.

> First, the targeted government can concede inessential issues in exchange for peace, a strategy that [Kydd and Walter] believe is frequently pursued though rarely admitted.[166]

When assessing the first counterstrategy, it should be noted that governments have a particular advantage when it comes to cyberterrorism. Cyberterrorism is a much more difficult means to threaten your enemy, since by doing so you take away the element of surprise and allow likely targets to prepare

[164] Ibid., 51.

[165] Ibid., 60.

[166] Ibid., 64.

or even disconnect. Unlike kinetic weapons used for terrorism, cyberterrorism depends on a connection being open between the attacker and the defender in order for the cyber-attack to succeed.

> Second, where the issue under dispute is important enough to the targeted state that it does not want to grant any concessions, the government may engage in retaliation.[167]

Similar to above, it's much harder to threaten a state with cyberterrorism. While a terrorist pursuing a cyber-attack could leave them vulnerable, it is unlikely that retaliation in cyberspace will do more than disrupt a terrorists capabilities. With that said, counter measures for states are not limited to the cyber domain. However, a state must be precise in their retaliation and absolutely sure they have correctly attributed the act, as the terrorist could be also simultaneously pursuing a strategy of provocation.[168]

> Third, a state can harden likely targets to minimize costs the terrorist organization can inflict.[169]

This strategy is one that is currently being pursued by governments around the world.[170] The reality is, cyberterrorism is only possible because vulnerabilities in these networks exist. If these vulnerabilities are removed, there can be no cyberterrorism. While impossible to fully secure all likely targets and often costly to do so,[171] this strategy is one of the better strategies to pursue.

> Fourth, states should seek to deny terrorists access to the most destructive weapons, especially nuclear and biological ones.[172]

This strategy, while focusing on the most destructive weapons, can be adjusted to focus on denying terrorists access to cyber weapons available on the black market. While it's impossible to deny computer science education required to develop these cyber weapons, the vulnerabilities these cyber weapons use, such as the zero-days used in the Stuxnet virus, are also for sale on the black market. Currently, Middle

---

[167] Ibid.

[168] Ibid.

[169] Ibid., 65.

[170] INSERT SOURCES HERE

[171] Matusitz and Minei, "Cyberterrorism: Its Effects on Health-Related Infrastructures," 168.

[172] Kydd and Walter, "The Strategies of Terrorism," 65.

Eastern countries have illustrated interest in acquiring these zero day vulnerabilities, however they cannot match the higher prices offered by Western governments on these black markets.[173]

> Finally, states can strive to minimize the psychological costs of terrorism and the tendency people have to overact.[174]

The last counter-cyberterrorism strategy is worth looking into in more depth. While this strategy is not always as simple to pursue when kinetic weapons are used by terrorists given they garner a lot of media attention, cyber-attacks are less likely to have the same visual impact. This strategy is talked about in more detail in the next section.

The Non-Spectacle of Cyberterrorism

As has been illustrated in the literature review, the ability of cyber weapons to have the same terrorizing impact that kinetic weapons have is a highly debated issue. On the one hand, an act of cyberterrorism has not yet occurred and therefore there is no empirical evidence to evaluate the effectiveness of the psychological impact from these attacks. The case studies demonstrate that terror was not the result of either, even if there was an attempt to send a message or have far-reaching psychological impact. Stuxnet Virus was likely intended to deter further quests for nuclear weapons in Iran, and the cyber-attack on the Ukrainian power grid was likely designed to illustrate capability and send a message to the Ukrainian government or its people. Though they were likely not designed to cause terror in the same way a terrorist would design the cyber-attack. In order for a terror to occur, there needs to be an audience. However, with the cyber-attacks we have seen it is unlikely that these cyber-attacks can cause nearly as much of a spectacle as kinetic weapons, and therefore would receive less media coverage.

---

[173] Wilson, "Cyber Threats to Critical Information Infrastructure," 131.

[174] Kydd and Walter, "The Strategies of Terrorism," 65.

James E. Lukaszewski, a public relations consultant to the U.S. military, describes this symbiotic relationship between the media and terrorists: "Media coverage and terrorism are soul mates - virtually inseparable. They feed off each other. They together create a dance of death - the one for political or ideological motives, the other for commercial success."[175] Brigitte L. Nacos, a professor at Columbia University, uses a similar metaphor, providing a different perspective, "…the news media and terrorists are not involved in a love story; they are strange bedfellows in a marriage of convenience."[176] Targets are chosen by terrorists to create an extreme reaction, to create fear, to provoke others to react, and in their best-case scenario cause self-destructive behaviour.[177] Public opinion can be changed, media can spread terror, and publicity can facilitate terrorist media-related goals, including: receiving attention, recognition of grievances, demands, objectives, respectability and even legitimacy in some circles countries or regions.[178]

The media will always single out sources of violence, conflict, and bloodshed over anything else. Human beings are instinctively attracted to such coverage. Terrorists use this to their advantage knowing very well that the press will cover these stories. Communication is key to a terrorists goals, whether political or ideologically motivated, and there is no better way to do it now days then to exploit mass media. However, if cyberterrorism does not offer this same spectacle that attracts media coverage, it begins to make these cyber weapons less attractive.[179] The cyber-attack may result in just a minor inconvenience or fail, resulting in a lot of time, resources, and money that could have been better put towards a more sure method of causing not only violence, but terror. As Conway argues, "These

---

[175] James E. Lukaszewski, "The Media and the Terrorist: A Dance to Death," Presentation (Clearwater Beach, Florida: A Joint Meeting of the Airport Operations Council of America and the American Transportation Association, 1987), http://www.e911.com/speeches/mediaandterrorists.html.

[176] Brigitte L. Nacos, *Terrorism and Counterterrorism*, 4th ed. (New York: Longman/Pearson, 2012), 270.

[177] Randall D. Law, *Terrorism: A History* (Cambridge: Polity Press, 2009), 3.

[178] Nacos, *Terrorism and Counterterrorism*, 265.

[179] Conway, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism," 115.

observations betray a fundamental misunderstanding of the nature and purpose(s) of terrorism, particularly its attention-getting function. A terrorist attack with the potential to be hidden, portrayed as an accident, or otherwise remain unknown is unlikely to be viewed positively from a terrorism perspective."[180]

Furthermore, a terrorist attack that is portrayed as an accident, is a failure. Therefore, in a battle of attrition, this is a very effective method if a cyberterrorist attack does occur in the future. If there is no spectacle that is explicitly associated with the event, it can be downplayed as a technical glitch taking away any likely possibility to have a psychological impact on its intended audience. The added benefit of this counterstrategy, is that it would deter terrorists in the future from pursuing cyberterrorism as the effects would be less effective than kinetic weapons.

Other Advantages and Disadvantages of Cyberterrorism

Anonymity in cyberspace is two-fold for terrorists. First, it allows them to operate and execute a cyber-attack clandestinely. Even if they claim the attack as their own, the source of the attack which could reveal the terrorists location, may be difficult to locate, allowing the terrorist to strike again in the future without retaliation. Second, most actors in cyberspace wish to remain anonymous, therefore a terrorist organization can take advantage of the cyber-attack and claim it as their own in order to create prestige and terror.

Although it has been argued that cyber-based weapons are relatively inexpensive to produce and use in comparison to kinetic weapons,[181] the case studies have painted a very different picture. While

---

[180] Ibid.

[181] Goodman, Kirk, and Kirk, "Cyberspace as a Medium for Terrorists," 196; Weimann, "Cyberterrorism: The Sum of All Fears?," 137; Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," 129; Cath Everett, "Who Is Responsible for Securing Critical Infrastructure?," *Computer Fraud & Security* 2010, no. 10 (2010): 6, http://dx.doi.org/10.1016/s1361-3723(10)70130-5; Matusitz, "Cyberterrorism: Postmodern State of Chaos," 119; Lewis, *Cyberwarfare and Its Impact on International Security*, 12; Sarah Gordon and Richard Ford, "Cyberterrorism?," *Computers & Security* 21, no. 7 (2002): 642, http://dx.doi.org/10.1016/s0167-4048(02)01116-1.

terrorist organizations such as Al-Qaeda have proven their ability to plan, be patient, resourceful, and acquire intelligence for an operation – such as with the attacks of 9/11 – Daniel Byman, has argued that "though Al Qaeda has strategies that on paper seem relatively well thought out, in practice these strategies have limits or are flawed."[182] It is likely that this problem is exacerbated in the cyber realm where the simplest of updates to a computer system could render an entire operation a failure.

Krepinevich argues that "cyber patriots" or terrorist organizations can be sponsored by states to administer a cyber-attack on their behalf creating plausible deniability.[183] This could serve the goals of both terrorist organizations and opposing states. For example, in order to achieve a state's goal through a cyber-attack they employ a terrorist organization and provide the means necessary to carry it out – thus solving the problem of limited funding, resources, skills, and intelligence that a terrorist organization may have available to them. The terrorist organization would be more than willing to declare that they were the attackers that caused the damage, the sponsoring state remains inconspicuous, and both of these actors' goals were achieved. However, this could arguable be considered cyberwarfare and countermeasures could be very different. Even the case where an attacking state or group uses a false banner, if they used a terrorist organization that would benefit from the infamy that came with a successful attack, the terrorist organization still may proclaim they were the ones responsible, even if they were not.

Deterrence from using cyber weapons depends on attribution. Reducing the risk and frequency at which cyber-attacks are used would require that anonymity be somehow made more difficult. Krepinevich argues,

> To be effective, a strategy of deterrence through punishment requires that the prospective attacker believe that he can be accurately identified by his target, that the target of the attack has both the capability and the will to retaliate, and that the costs incurred through a retaliatory

[182] Byman, *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know*, chap. 3.

[183] Krepinevich, *Cyberwarfare: A "Nuclear Option"?*, 50.

> attack (be it in the form of a cyber strike or more traditional military action) will exceed the benefits to be derived from the cyber-attack.[184]

While the issue of deterring terrorists is already complicated, the problem with attribution and digital evidence in cyberspace compounds the issue further, making deterrence in cyberspace seem unlikely. The problem of attribution proves to make counter measures difficult. Even successfully being able to trace a source may prove inconclusive when lead to an Internet café or university. In this case human and signal intelligence may be of significant use when combined with digital forensics in discovering the true identity of the attacker, but even this is not guaranteed to be successful.[185]

The Cyberterrorism Delusion

This paper has so far argued that the strategies of cyberterrorism can be limited in their effect in achievement of terrorists overall goals. Following this discussion, it is important that we take a step back and look at cyberterrorism as a whole. While we know that terrorists have shown interest in cyberterrorism, interest is not intent, nor does it demonstrate capability.

John Mueller and Mark G. Stewart have argued that the threat from terrorism is vastly over exaggerated, which have ultimately created distortions of perspective that inspired "a determined and expensive quest to ferret out, and even to create, the nearly nonexistent."[186] If we take cyberterrorism for what it really is, a means to achieving a terrorists goals, then we can apply Mueller and Stewart's argument here as well.

It's unclear if Al-Qaeda, the one known terrorist organization that is heavily focused on conducting terrorism in the West – and the U.S. more specifically – "has done much of anything since September 11

---

[184]Ibid., 47.

[185] Ibid., 51.

[186] John Mueller and Mark Stewart, "The Terrorism Delusion," *International Security* 37, no. 1 (2012): 81–110; John Mueller and Mark Stewart, "How Safe Are We? Asking the Right Questions About Terrorism," *Foreign Affairs* (2016), https://www.foreignaffairs.com/articles/united-states/2016-08-15/how-safe-are-we.

except issue videos filled with empty, self-infatuated, and essentially delusional threats."[187] Even if we consider that Al-Qaeda has been working meticulously on developing their cyberterrorism capabilities, and put aside the fact that cyberterrorism as a strategy of attrition is currently limited, there is much that can go wrong during a cyber-attack that heavily outweighs the risk-reward cost-benefit analysis of a terrorist when deciding whether to use cyber weapons over kinetic weapons. That's not even to mention that it is unclear if at cyber-attack can cause terror.

Likewise, the threat of insiders and radicalized individuals is often overplayed. While the Maroochy Shire case illustrates the potential is there, we must not forget that red flags were raised that ended with Boden arrested. It is clear that high-level operations such as the Stuxnet Virus or even the cyber-attack on the Ukrainian power grid are unlikely to be possible by any radicalized individual or insider, similar to how an attack such as 9/11 is unlikely to be the result of a radicalized individual or insider. Shikha Dalmia illustrates this point perfectly, stating that terrorists need to be:

> Radicalized enough to die for their cause; Westernized enough to move around without raising red flags; ingenious enough to exploit loopholes in the security apparatus; meticulous enough to attend to the myriad logistical details that could torpedo the operation; self-sufficient enough to make all the preparations without enlisting outsiders who might give them away; disciplined enough to maintain complete secrecy; and – above all – psychologically tough enough to keep functioning at a high level without cracking in the face of their own impeding death.[188]

The Stuxnet Virus and cyber-attack on the Ukrainian power grid case studies have demonstrated that these high-level operations capable of causing physical damage or mass disruption require vast resources, intelligence, skill, and time. Most of these radicalized individuals and insiders – never mind professional terrorists – have the resources, capability to conduct the intelligence and carry out the attack, or time to achieve an act of cyberterrorism. Even with the help of a nation-state, as Krepinevich argues, everything still needs to go perfectly according to plan, and there is ultimately a lot that can go wrong. "The vast

[187] Mueller and Stewart, "The Terrorism Delusion," 90.

[188] Shikha Dalmia, "What Islamist Terrorist Threat? Al Qaeda Doesn't Have What It Takes to Hurt America," *The Reason Foundaiton* (Los Angeles, February 15, 2011), http://reason.org/news/show/what-islamist-terrorist-threat.

majority of even the craftiest terrorist conspirators", Mueller and Stewart argue, "fail to carry out their plots."[189]

CONCLUSION

A fear has risen that terrorists will pursue cyberterrorism. A word that has been associated with chaos and cascading failures across society from the click of a keyboard. While vulnerabilities are discovered on a daily basis and the costs and consequences from cyber-attacks have the potential to be high, terrorists may not have the capability or intent to adopt cyberterrorism in their strategies. In this paper, I have contended that the strategies of cyberterrorism may be limited to attrition in pursuit of policy change goals. The majority of common terrorist goals – regime change, territorial change, social control, and status quo maintenance -- and principal strategies – intimidation, provocation, spoiling, and outbidding – that Kydd and Walter outline are currently more concentrated locally where the dependence and reliability on technology is generally less than developed countries. Therefore, these strategies are unlikely to be useful for cyberterrorism.

In presenting this argument I have formulated a criteria based off Hoffman's definition of terrorism to bring cyberterrorism back to its roots. Cyberterrorism must first and foremost, albeit obvious, must be executed via cyberspace; second, it must be ineluctably political or ideological in aims and motives; third, it must be violent or threaten violence; fourth, it must be designed to have far-reaching psychological repercussions beyond the immediate victim or target; fifth, it must be conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and finally, it must be perpetrated by a subnational group or non-state entity. In

[189] Mueller and Stewart, "The Terrorism Delusion," 95.

conceptualizing cyberterrorism I have made a distinction that terrorists use of cyberspace to facilitate operations is not cyberterrorism. However, the Ukraine case study demonstrates that cyber operations alongside a kinetic operation may have a multiplier effect, increasing the impact of the event. This is one area that requires further study.

There are currently no public cases of cyberterrorism. The case studies selected however can be used to draw parallels and illustrate: the vulnerabilities present in computer systems and industrial control systems; that cyber-attacks can be violent and have effects in the physical world; the threat of insiders; the importance of security protocols and controls in place; that high-level cyber-attacks capable of being violent and causing terror requires vast resources, intelligence, skill, and time; and that developed countries may be more vulnerable to cyber-attacks. An analysis of which countries are more vulnerable to cyber-attacks is a necessary next step. It may very well be that developing nations who have begun placing more and more of its operations online are more vulnerable if the proper security measures are not in place. This is why information sharing and best practices is important for cybersecurity.

These cases illustrate that the threat from cyberterrorism is real but can be vastly overstated. Most of the damage or disruption caused by the cyber-attack was quickly undone, therefore the potential threat could be considerable but the actual threat is significantly lower. While attrition has proven to be the only likely strategy that cyberterrorists could pursue, its overall effectiveness is unconvincing and counterterrorism measures could make it even less effective. First, cyberterrorism attacks are unlikely to be repeated as the vulnerabilities from that specific attack are patched up, making future threats of cyberterrorism less credible. Second, if a terrorist attempts to threaten cyberterrorism, governments can immediately search for vulnerabilities and patch them, essentially making the attack fail – this may be easier said than done in most cases though warning always provides the chance to gain an advantage. In some cases you can simply go offline since an established connection is required for cyberterrorism to ultimately work. Third, Cyberterrorism is only possible because of vulnerabilities, by hardening systems

and patching vulnerabilities – the chances of cyberterrorism occurring is decreased. This is one of the ongoing efforts by governments around the world. Fourth, it is also critical that governments are constantly removing zero day vulnerabilities from the market to prevent terrorists from obtaining them – they are key in a successful surprise cyber-attack. Fifth, if worst comes to worst and a cyber-attack has proven successful, one of the most effective strategies against cyber-terrorism is simply denying that the event was caused by terrorism. Regardless of a terrorist organizations claim, if the cyber-attack is downplayed by governments as just a "glitch" in the system, it can take away the desired impact of terrorists and deter future attempts at cyberterrorism.

Even if a terrorist successfully conducted a cyber-attack and claimed to be the perpetrators, cyber-attacks have yet to demonstrate they can actually cause terror – an essential element for a terrorist attack to be considered a success. Given that high-level cyber-attacks capable of being violent requires vast resources, intelligence, skill, and time – ultimately too much can go wrong in conducting a cyber-attack and the costs-benefit analysis weighs heavily towards terrorist use of kinetic weapons for the time being.

REFERENCES

Abrams, Marshall, and Joe Weiss. *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*, 2008. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Bank of America - Merrill Lynch Global Research. *You've Been Hacked! – Global Cybersecurity Primer*, 2015. http://xxlsec.com/wp-content/uploads/2015/06/BankOfAmericaCyberReport.pdf.

Barzashka, Ivanka. "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme." *The RUSI Journal* 158, no. 2 (2013): 48–56. http://www.tandfonline.com/doi/abs/10.1080/03071847.2013.787735.

von Behr, Ines, Anais Reding, Charlie Edwards, and Luke Gribbon. *Radicalisation in the Digital Era*. Brussels, 2013. http://www.rand.org/pubs/research_reports/RR453.html.

Berntzen, Lars Erik, and Sveinung Sandberg. "The Collective Nature of Lone Wolf Terrorism: Anders Behring Breivik and the Anti-Islamic Social Movement." *Terrorism and Political Violence* 26, no. 5 (2014): 759–779. http://www.tandfonline.com/doi/abs/10.1080/09546553.2013.767245.

Byman, Daniel. *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know*. *Intelligence and National Security*. Kobo Ed. New York: Oxford University Press, 2016.

Canadian Association for Security and Intelligence Studies. "Private Sector and Critical Infrastructure." In *The Cyber Challenge*. Ottawa: CASIS, 2016. http://www.casis-acers.ca/wp-content/uploads/2016/11/Final-Summary-Highlights-from-the-CASIS-2016-Annual-Symposium.pdf.

Center for Terroranalyse. *The Threat from Solo Terrorism and Lone Wolf Terrorism*, 2011. https://www.pet.dk/~/media/Engelsk/the_threat_from_solo_terrorism_and_lone_wolf_terrorism_-_engelsk_version_pdf.ashx.

Chaikin, David. "Network Investigations of Cyber Attacks: The Limits of Digital Evidence." *Crime, Law and Social Change* 46, no. 4–5 (2006): 239–256.

Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from Stuxnet." *Computer* 44, no. 4 (2011): 91–93.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. *Terrorism and Political Violence*. Vol. 23. New York: HarperCollins Publishers, 2012.

Clem, Angela, Sagar Galwankar, and George Buck. "Health Implications of Cyber-Terrorism." *Prehospital and Disaster Medicine* 18, no. 3 (2003): 272–275. http://www.journals.cambridge.org/abstract_S1049023X00001163.

Collin, Barry. "Future of Cyberterrorism: The Physical and Virtual Worlds Converge." *Crime and Justice International* 13, no. 2 (1997). http://www.cjimagazine.com/archives/cji4c18.html?id=415.

Committee, Fundamental Challenges, Review Dod, Physical Sciences, Council Isbn, This Pdf, National Academies Press, and National Academy. *Realizing the Potential of C4I: Fundamental Challenges*, 1999.

Conway, Maura. "Against Cyberterrorism." *Communications of the ACM* 54, no. 2 (2011): 26–28. http://dx.doi.org/10.1145/1897816.1897829.

———. “Hackers as Terrorists? Why It Doesn’t Compute.” *Computer Fraud & Security* 2003, no. 12 (2003): 10–13. http://dx.doi.org/10.1016/s1361-3723(03)00007-1.

———. “Reality Check: Assessing the (Un)Likelihood of Cyberterrorism.” In *Cyberterrorism: Understanding, Assessment, and Response*, edited by Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, 103–121. New York: Springer, 2014.

Cooper, Michael, Michael Schmidt, and Eric Schmitt. “Boston Suspects Seen as Self-Taught, Fueled by Web.” *New York Times*, April 23, 2013. http://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html?hp&pagewanted=all.

Cox, Christopher. “Cyber Capabilities and Intent of Terrorist Forces.” *Information Security Journal: A Global Perspective* 24, no. 1–3 (2015): 31–38. http://www.tandfonline.com/doi/full/10.1080/19393555.2014.998846.

Dalmia, Shikha. “What Islamist Terrorist Threat? Al Qaeda Doesn’t Have What It Takes to Hurt America.” *The Reason Foundaiton*. Los Angeles, February 15, 2011. http://reason.org/news/show/what-islamist-terrorist-threat.

Denning, Dorothy. “Cyberterrorism: The Logic Bomb versus the Truck Bomb.” *Global Dialogue* 2, no. 4 (2000): 29–37.

———. “Stuxnet: What Has Changed?” *Future Internet* 4, no. 4 (2012): 672–687. http://www.mdpi.com/1999-5903/4/3/672/.

E-ISAC, and SANS. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, D.C., 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Embar-Seddon, Ayn. “Cyberterrorism: Are We Under Siege?” *American Behavioral Scientist* 45, no. 6 (2002): 1033–1043. http://dx.doi.org/10.1177/0002764202045006007.

Everett, Cath. “Who Is Responsible for Securing Critical Infrastructure?” *Computer Fraud & Security* 2010, no. 10 (2010): 5–8. http://dx.doi.org/10.1016/s1361-3723(10)70130-5.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Cupertino, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (2011): 23–40.

Federal Bureau of Investigation (FBI). “The Cyber Threat: Using Intelligence to Predict and Prevent.” Last modified 2010. Accessed November 2, 2016. https://archives.fbi.gov/archives/news/stories/2010/march/cyberintel030410.

Flemming, Peter; Stohl, Michael. “Myths and Realities of Cyber Terrorism.” In *Countering Terrorism Through International Cooperation*, edited by Alex P. Schmid, 70–105. Vienna: International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program, 2001. http://www.comm.ucsb.edu/faculty/mstohl/Myths and Realities of Cyberterrorism.pdf.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (2013): 41–73. http://dx.doi.org/10.1162/isec_a_00136.

Geers, Kenneth. “The Cyber Threat to National Critical Infrastructures: Beyond Theory.” *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 124–130. http://dx.doi.org/10.1080/15567281.2010.536735.

Gendron, Angela. “Cyber Threats and Multiplier Effects: Canada at Risk.” *Canadian Foreign Policy* 19, no. 2 (2013): 178. http://www.tandfonline.com/doi/abs/10.1080/11926422.2013.808578.

Goodman, Seymour E, Jessica C Kirk, and Megan H Kirk. “Cyberspace as a Medium for Terrorists.” *Technological Forecasting and Social Change* 74, no. 2 (2007): 193–210. http://dx.doi.org/10.1016/j.techfore.2006.07.007.

Gordon, Sarah, and Richard Ford. “Cyberterrorism?” *Computers & Security* 21, no. 7 (2002): 636–647. http://dx.doi.org/10.1016/s0167-4048(02)01116-1.

Government of Massachusetts. *After Action Report for the Response to the 2013 Boston Marathon Bombings*. Boston, 2014. http://www.mass.gov/eopss/docs/mema/after-action-report-for-the-response-to-the-2013-boston-marathon-bombings.pdf.

Green, Joshua. “The Myth of Cyberterrorism.” *Washington Monthly*, 2002. http://werzit.com/intel/regions/cyber/articles/archives/Myth of Cyberterrorism.pdf.

Guinchard, Audrey. “Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy.” *Journal of Strategic Security* 4, no. 2 (2011): 75–96. http://dx.doi.org/10.5038/1944-0472.4.2.5.

Hardy, Keiran. “Operation Titstorm: Hacktivism or Cyberterrorism.” *UNSW Law Journal* 33, no. 2 (2010): 474–502. http://www.austlii.edu.au/au/journals/UNSWLawJl/2010/21.pdf.

Heickerö, Roland. “Cyber Terrorism: Electronic Jihad.” *Strategic Analysis* 38, no. 4 (2014): 554–565. http://www.tandfonline.com/doi/abs/10.1080/09700161.2014.918435.

Hoffman, Bruce. *Inside Terrorism: Revised and Expanded Edition*. New York: Columbia University Press, 2006.

ICS-CERT. “Cyber-Attack Against Ukrainian Critical Infrastructure (IR-ALERT-H-16-056-01).” *Industrial Control Systems Cyber Emergency Response Team*. Last modified 2016. Accessed November 10, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Jones, Andrew. “Cyber Terrorism: Fact or Fiction.” *Computer Fraud & Security* 2005, no. 6 (2005): 4–7. http://dx.doi.org/10.1016/s1361-3723(05)70220-7.

Kaspersky Lab. “Kaspersky Lab Provides Its Insights on Stuxnet Worm.” *Virus News*, September 24, 2010. http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

Kenney, Michael. “Cyber-Terrorism in a Post-Stuxnet World.” *Orbis* 59, no. 1 (2015): 111–128. http://linkinghub.elsevier.com/retrieve/pii/S0030438714000787.

Khan, Fahad Ullah. “States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis.” *Strategic Studies* 31, no. 3 (2011): 91–108.

Krepinevich, Andrew F. *Cyberwarfare: A “Nuclear Option”?* Washington, D.C.: Center for Strategic and Budgetary Assessments, 2012.

Kydd, Andrew H., and Barbara F. Walter. “The Strategies of Terrorism.” *International Security* 31, no. 1 (2006): 49–80.

Lachow, Irving. “The Stuxnet Enigma: Implications for the Future of Cybersecurity.” *Georgetown Journal of International Affairs – Special Issue: International Engagement on Cyber* 1 (2011): 118–127.

Law, Randall D. *Terrorism: A History*. Cambridge: Polity Press, 2009.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, D.C., 2002. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

———. *Cyberwarfare and Its Impact on International Security*. New York: United Nations Publications, 2010. https://www.un.org/disarmament/publications/occasionalpapers/no-19/.

———. “The War on Hype: The Deadly Terror Lurking Around the Corner May Not Be Such a Big, Ominous Threat after All.” *San Francisco Chronicle*, February 19, 2006. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/02/19/INGDDH8E2V1.DTL.

Lukaszewski, James E. “The Media and the Terrorist: A Dance to Death.” Presentation. Clearwater Beach, Florida: A Joint Meeting of the Airport Operations Council of America and the American Transportation Association, 1987. http://www.e911.com/speeches/mediaandterrorists.html.

Macaulay, Tyson. *RIoT Control: Understanding and Managing Risks and the Internet of Things*. Cambridge: Morgan Kaufmann, 2016.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. “Stuxnet Under the Microscope.” *Eset* (2010): 1–85. http://ece.wpi.edu/~dchasaki/papers/Stuxnet_Under_the_Microscope.pdf.

Matusitz, Jonathan. “Cyberterrorism: Postmodern State of Chaos.” *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 115–123. http://dx.doi.org/10.1080/15567281.2010.536733.

Matusitz, Jonathan, and Elizabeth Minei. “Cyberterrorism: Its Effects on Health-Related Infrastructures.” *Journal of Digital Forensic Practice* 2, no. 4 (2009): 161–171. http://www.tandfonline.com/doi/abs/10.1080/15567280802678657.

McQuade, Samuel C. *Understanding and Managing Cybercrime*. Boston: Pearson Education, 2006.

Michael, George. “Counterinsurgency and Lone Wolf Terrorism.” *Terrorism and Political Violence* 26, no. 1 (2014): 45–57. http://www.tandfonline.com/doi/abs/10.1080/09546553.2014.849912.

Mueller, John, and Mark Stewart. “How Safe Are We? Asking the Right Questions About Terrorism.” *Foreign Affairs* (2016). https://www.foreignaffairs.com/articles/united-states/2016-08-15/how-safe-are-we.

———. “The Terrorism Delusion.” *International Security* 37, no. 1 (2012): 81–110.

Nacos, Brigitte L. *Terrorism and Counterterrorism*. 4th ed. New York: Longman/Pearson, 2012.

Nesser, Petter. “Research Note: Single Actor Terrorism: Scope , Characteristics and Explanations.” *Perspectives on Terrorism* 6, no. 6 (2012): 61–73. http://www.terrorismanalysts.com/pt/articles/issues/PTv6i6.pdf.

Rid, Thomas. “Think Again: Cyberwar.” *Foreign Policy* 192 (2012): 58–61. http://foreignpolicy.com/2012/02/27/think-again-cyberwar/.

Shaw, William T. *Cybersecurity for SCADA Systems*. Tulsa: PennWell Corporation, 2006.

Shoniregun, Charles A. *Synchronizing Internet Protocol Security*. New York: Springer, 2007.

Singer, P.W, and Allan Friedman. *Cybersecurity and Cyberwar*. New York: Oxford University Press, 2014.

Slay, Jill, and Michael Miller. "Lessons Learned from the Marchoory Water Breach." In *Critical Infrastructure Protection*, edited by Eric Goetz and Sujeet Shenoi, 73–82. Boston: Springer, 2008. http://www.springer.com/us/book/9780387754611.

Smith, Tony. "Hacker Jailed for Revenge Sewage Attacks." *WWW The Register*, October 31, 2001. http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

Stern, Jessica. "Obama and Terrorism: Like It or Not, the War Goes On." *Foreign Affairs* 94, no. 5 (2015): 62–70. https://www.foreignaffairs.com/articles/obama-and-terrorism.

Stohl, Michael. "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?" *Crime, Law and Social Change* 46, no. 4–5 (2006): 223–238. http://dx.doi.org/10.1007/s10611-007-9061-9.

Symantec. *Internet Security Threat Report*. Vol. 21, 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16707960&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2.

Taylor, Paul, and Tim Jordan. *Hacktivism and Cyberwars: Rebels with a Cause?* New York: Routledge, 2004. papers3://publication/uuid/50380B27-672A-4D1A-89C0-6FC517868773.

Thomas, Douglas. "Cyber Terrorism and Critical Infrastructure Protection," 2002. http://www-bcf.usc.edu/~douglast/testimony.pdf.

Tsukayama, Hayley, Mark Berman, and Jerry Markon. "Gunman Who Killed 49 in Orlando Nightclub Had Pledged Allegiance to ISIS." *The Washington Post*, June 13, 2016. https://www.washingtonpost.com/news/post-nation/wp/2016/06/12/orlando-nightclub-shooting-about-20-dead-in-domestic-terror-incident-at-gay-club/?hpid=hp_hp-top-table-high_orlando-banner%3Ahomepage%2Fstory&utm_term=.5576d5b796e7.

Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism* 28, no. 2 (2005): 129–149. http://dx.doi.org/10.1080/10576100590905110.

———. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3, no. 2 (2012): 75–90.

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk*. *Risk Management*. Santa Monica, CA: RAND Corporation - Center for Terrorism Risk Management Policy, 2005. http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG388.pdf.

Wilson, Clay. "Cyber Threats to Critical Information Infrastructure." In *Cyberterrorism: Understanding, Assessment, and Response*, edited by Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, 123–136. New York: Springer, 2014.

World Health Organization. *Global Status Report on Violence Prevention 2014*. *World Health Organization*, 2014. http://www.who.int/violence_injury_prevention/violence/status_report/2014/en/.

Yannakogeorgos, Panayotis A. “Rethinking the Threat of Cyberterrorism.” In *Cyberterrorism: Understanding, Assessment, and Response*, edited by Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, 43–62. New York: Springer, 2014.

Zetter, Kim. *Countdown to Zero Day : Stuxnet and the Launch of the World’s First Digital Weapon*. Kobo Ed. New York: Crown Publishers, 2014.

———. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *Wired*. Boone, IA, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.