COUNTERTERRORISM LESSONS FOR CYBERSECURITY:

HOW A DECADE'S WORTH OF EXPERIENCE FIGHTING TERRORISM CAN PROVIDE INSIGHTS INTO MITIGATING THE THREAT OF CYBER ATTACKS

Master of Arts in Law and Diplomacy Capstone Project

Submitted by Benjamin C. Rosenbaum

April 25h, 2014

Supervised by: Professor William Martel

http://fletcher.tufts.edu

THE FLETCHER SCHOOL

Table of Contents

Abstract

Cyber attacks are an emerging, and often misunderstood, danger to national security. Although nascent and sophisticated threats emanating from cyberspace might appear overwhelming, remarkably, there are sufficient parallels between Jihadist terrorism and cyber attacks that can provide useful insights. Both tactics are nebulous, undefined threats that not only jeopardize wide sections of society, but also, make it straightforward for the perpetrators to conceal their identity. These shared attributes complicate efforts to establish a robust deterrence. Yet, the remote plausibility of high impact attacks underscore why these intricate security concerns cannot be ignored.

With these parallels in mind, this paper draws upon the lessons learned from over a decade of fighting terrorism, to endorse the following guidelines for cybersecurity policy and strategy: (1) do not ignore deterrence, but recognize that its applications are limited to fostering resilience and deterring nation-states, (2) synchronize government responses and create a federal office to guide strategic direction, (3) bolster the capabilities of the intelligence community to coordinate and unmask perpetrators, (4) raise public awareness to the best computer security practices and reduce threat inflation, (5) work with the private sector to incentivize cybersecurity and maintain trust, (6) engage internationally to promote global norms on cybersecurity and foster information sharing, and (7) determine the risks of potential cyber and non-cyber responses to an attack as a means to understand the long term implications of short term strategies.

Introduction

"*In discussions of things 'cyber'…rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon*."

– General Michael Hayden, Former Director of the Central Intelligence Agency and National Security Agency[1]

"*History never repeats itself, but sometimes it rhymes.*"

– attributed to Mark Twain[2]

Today, the world is more interconnected than ever before. The ubiquity of computer technologies and the internet have revolutionized the way in which we transfer, store, and access information. The digital age has brought along great advancements in almost all facets of society: from the way in which we communicate, do business, fight wars, and travel. Our reliance on technology has become integral to our everyday lives and there is every indication that this trend will increase well into the future.

Yet, as the 2010 National Security Strategy outlines, "the very technologies that empower us to lead and create also empower those who would disrupt and destroy."[3] Our dependence on cyberspace for critical infrastructure, national security, and public health creates a host of new vulnerabilities that may be susceptible to sabotage or exploitation.[4] The anonymity of cyberspace emboldens adversaries wishing to do harm without fear of retribution. The accessibility of cyberspace ensures that barriers to perpetrate an attack are low. Thus, there is

---

[1] Hayden, Michael V. "The Future of Things Cyber," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011). Pg. 3.
[2] Nye, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011). Pg. 22.
[3] White House, United States of America. "National Security Strategy of the United States 2010," (May 2010). Pg. 27.
[4] Department of Defense, United States of America. "Department of Defense Strategy for Operating in Cyberspace," (July 2011). Pg. 1.

broad agreement within the United States (US) government that attacks in the cyber domain constitute a genuine threat to national security.[5]

Despite the potential magnitude of cyber attacks, the field of cybersecurity, strategy, policy, and management remains in its very early stages.[6] The original design of the internet favored connectivity, interoperability, information flow, and 'ease of use' over security.[7] Additionally, the architects of the internet could not anticipate the vital role that their creation would play in the primary functions of society. Providing an excellent overview of the uncertainties surrounding cybersecurity, James Clapper, the US Director of National Intelligence, explains that the "world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks." He further emphasizes that the difficulty in conceptualizing cyber threats is compounded by the unpredictable and constantly evolving nature of cyber attacks.[8]

As policymakers try to make sense of how to combat threats emanating from the cyber realm, Joseph Nye, the former dean of the Harvard Kennedy School and current distinguished professor, argues that learning from past experiences can provide useful insights into how governments can best develop policies to respond to emerging threats.[9] Nye contends that as transformative technologies, there are relevant comparisons between the development of nuclear

---

[5] For instance, the 2013 worldwide threat assessment conducted by the US intelligence community referenced cyber attacks before discussions on other national security issues such as terrorism, weapons of mass destruction proliferation, and global health pandemics. Further, securing cyberspace was one of the leadings threats mentioned in the 2010 National Security Strategy. See: Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record," *Senate Select Committee on Intelligence.* (March 12, 2013). Pg. 1.

[6] Waldo, James. "Course Description," *IGA-236M*: *Technology, Security, and Conflict in the Cyber Age*. Harvard Kennedy School, Harvard University, Cambridge, MA. (January 2014). Accessed January 15, 2014. <http://www.hks.harvard.edu/degrees/teaching-courses/course-listing/iga-236m>.

[7] Department of Defense. "Department of Defense Strategy for Operating in Cyberspace," Pgs. 2-3.

[8] Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record," Pg. 1.

[9] Nye. "Nuclear Lessons for Cyber Security?" Pg. 19.

weapons and the emergence of cyber attacks. He highlights how lessons learned from the nuclear era can be applied to cybersecurity for issues related to managing technological change, securing civilian use, and promoting international cooperation.

Although nuclear weapons provide a useful analogy, especially as both threats involve the superiority of offense over defense, Nye recognizes that the differences between the two concepts are great since nuclear policy largely overlooks the prominence of transnational non-state actors in the cyber domain.[10] Nye's piece also acknowledges that the effects of cyber attacks can range from vandalism to acts of war whereas a nuclear strike is almost exclusively a catastrophic event with existential implications.[11]

I argue that the lessons learned from the last decade of fighting radical Islamist terrorism provide another useful—and perhaps, more appropriate—comparison to guide cybersecurity strategy. As post-Cold War threats, the concepts of terrorism and cyber attacks share many similarities, especially in areas where the nuclear weapons comparison falls short. For instance, the attacks of September 11th, 2001 (9/11) demonstrated that the geographic advantages of the US were insufficient to protect the homeland against a determined group of politically motivated non-state actors. Moreover, terrorism, like cyber threats, can be employed by a multitude of perpetrators against a wide range of targets. More broadly, both threats are asymmetric, entail significant constraints to deterrence, and perpetuate the latent risk of high impact incidents that can potentially jeopardize homeland security.

To develop this thesis, first, I explore both the comprehensive definitions and national security implications of each concept. Then, I identify issue areas where cyber attacks and

[10] Nye. "Nuclear Lessons for Cyber Security?" Pg. 36.
[11] Nye. "Nuclear Lessons for Cyber Security?" Pg. 22.

terrorism overlap and differ. Finally, I investigate how general lessons from the 'War on Terrorism' can guide the creation of a set of strategies to mitigate cyber threats.

Understanding Cyber Attacks

Definition

Attacks from the cyber realm are amorphous and theoretically endanger all entities reliant on computer systems and the internet. The broad range of potential targets include computer chips embedded in weapons and medical equipment, computing networks controlling the electrical grid and water purification systems, air traffic control stations, and hard drives storing sensitive national security information.[12] The potential threat is so vast, that there lacks an all-encompassing definition identifying the types of incidents that constitute a cyber attack. [13] Everything from online protests to industrial theft to sabotage of critical infrastructure to strikes against military targets have been at some point described as cyber attacks.[14] As Peter Singer and Allan Friedman eloquently state in their primer on cybersecurity, "essentially, what people too often do when discussing (cyber attacks) is bundle together a variety of like and unlike activities, simply because they involve Internet-related technology."[15]

To get to the heart of the definition, it is crucial to understand the nature of the cyber threat. In essence, there are only three ways in which it is possible to conduct an 'attack' on a computer system: steal its information, misuse its credentials, and hijack its resources. [16] Herbert

---

[12] Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploitation," *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Ed. Derek S. Reveron. Washington: Georgetown University Press, 2012. Pg. 38.
[13] Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowland, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack," *California Law Review*. (2012). Pg 7.
[14] Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014. Pg. 67.
[15] Singer and Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Pg. 68.
[16] Singer and Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Pg. 39.

Lin, a chief scientist at the National Research Council of the National Academies, describes the ramifications of these threats in detail. He explains that it is feasible for offensive cyber combatants to remotely shut down computer systems, manipulate the authenticity of data, or even, deny a user from being able to logon to their own devices.[17] Cyber attacks do not necessarily produce kinetic outcomes and, oftentimes, its victims do not realize that their systems are compromised. The threat of cyber is heightened in that it can take place at light speed and that the anonymity of cyberspace makes attribution difficult, if not impossible.

To better understand the milieu of threats, Yale Law School professor Oona Hathaway categorizes offensive cyber actions into three distinct, yet, interrelated models: cyber crime, cyber warfare, and cyber attack (see: Figure 1). On one end, she contends that cyber crime is exclusively the pursuit of non-state actors using computer means to conduct illegal acts.[18] On the other end, she asserts that cyber warfare entails attacks on computer systems conducted in the context of an armed conflict. Encompassing the nexus of crime and warfare, Hathaway formulates a compelling depiction of a cyber attack: any action taken by a state or non-state actor to subvert the intended functions of a computer system for political or national security purposes.[19]

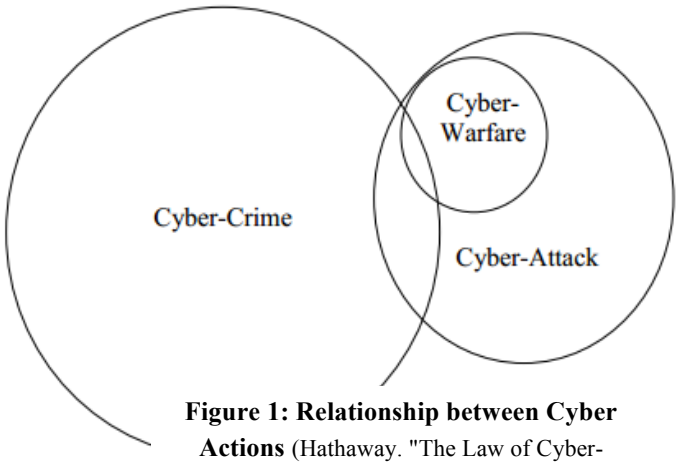

Figure 1: Relationship between Cyber Actions (Hathaway. "The Law of Cyber-Attack," Pg. 18.)

While all incidents of cyber warfare represent a form of cyber attack, only cyber crimes with political implications follow this distinction. This can include the theft of tightly guarded

[17] Lin. "Operational Considerations in Cyber Attack and Cyber Exploitation," Pg. 38.
[18] Hathaway. "The Law of Cyber-Attack," Pg. 19.
[19] Hathaway. "The Law of Cyber-Attack," Pg. 10.

intellectual property as a means for US adversaries to achieve technological parody and avoid costly investments in research and development. In contrast, criminal incidents with purely financial motivations do not meet the threshold of this definition of a cyber attack.

It must also be emphasized that not all politically motivated offensive operations involving computer systems should be classified as a cyber attack. For instance, digitally controlling an Unmanned-Aerial Vehicle (UAV) to fire missiles at a terrorist target in Pakistan is best categorized as a high-tech form of conventional warfare, not a cyber attack.[20] Further, a terrorist group using *Google Maps* to survey the location of a target before a strike should also not be considered a form of an offensive cyber action. Neither of these aforementioned examples explicitly undermine nor disrupt the integrity, availability, or access of a computer system.

The Cyber Threat

There are a wide-variety of techniques to conduct a cyber attack. Distributed Denial of Service (DDOS) attacks overwhelm servers as a means to deny access to targeted websites, phishing attacks extract essential information by masquerading as trustworthy online entities, logic bombs and Trojan horses furtively infect programmatic code to cause malicious functions when certain conditions are met, and computer worms and viruses gain access into a digital network as a means to spread itself and manipulate information.[21] Cyber attacks do not just take place on the World Wide Web. Other mechanisms include inserting malware infected thumb

[20] Hathaway. "The Law of Cyber-Attack," Pg. 11.
[21] Government Accountability Office, United States of America. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," *GAO-13-187*. (February 2013). Pg. 6.

drives into computer hard drives and also simple social engineering techniques where perpetrators gain login and password information through human interaction.[22]

The most complex and dangerous cyber attacks are designated as Advanced Persistent Threats (APT). These technologically complicated methods often utilize a combination of tactics to gain entry into a computer system and exploit its target. The most successful APTs avoid all means of detection over an extended period of time and extract maximal information. Most victims do not realize that they are targeted until it is too late, and even then, they often do not even know who perpetrated the incident.[23]

The obstacles to enter the cyber domain are so low that the potential perpetrators of cyber attacks are diverse and far-reaching.[24] They include individual hackers and organizational insiders seeking to induce anarchy; corporations exploring ways to achieve a competitive advantage; hacktivists—bound by ideological unanimity—promoting political or social goals; criminal syndicates attempting to steal information; and terrorist organizations intending to sabotage, disrupt, and cause disorder. Increasingly, nation-states have followed the lead of the US to expand their armed forces into the cybersphere as a means to conduct economic espionage, gather intelligence, and attack adversaries.[25] Countries wishing to conceal their activities can also sponsor proxies to conduct attacks on their behalf.

That being said, there is a sharp learning curve separating the perpetrators of genuine cyber threats from cyber nuisances. While anyone with access to the internet can potentially write a computer virus to conduct a cyber attack, they are unlikely to cause significant damage

---

[22] Martel, William. "Understanding Cyber Threats," *DHP-P249: Foundations of International Cybersecurity*. Fletcher School of Law and Diplomacy, Tufts University, Medford, MA. (September 9, 2013).
[23] Martel, William. "Understanding Cyber Threats."
[24] Nye, Joseph S. "Cyber Power," *Belfer Center for Science and International Affairs*. (May 2010). Pg. 4.
[25] Center for Strategic and International Studies: Threat Working Group: Threat Working Group. "Threats Posed by the Internet," *CSIS Commission on Cybersecurity for the 44th Presidency.* (December 2008) Pg. 3.

because once a virus is detected, the target can adjust their defenses accordingly. Thus, relatively simple attacks quickly become obsolete. Further, critical infrastructure systems are built with numerous redundancies and resilience mechanisms. Even if one segment of a network is incapacitated, the overall system will likely continue to function as intended. Only the most militarily advanced nation-states maintain the technological infrastructure to gather and exploit zero day vulnerabilities, launch coordinated strikes, and thoroughly map the weaknesses of an adversaries cyber defenses.

Nevertheless, the emerging risks of a high impact cyber attack cannot be underestimated. There are three ways that sophisticated threats from the cyber realm present legitimate challenges to national security: streamlining espionage, endangering critical infrastructure, and supplementing conventional attacks.

The speed in which it is possible to furtively obtain access to massive quantities of information has substantially hindered the ability for both states and corporations to protect sensitive information. Adversaries have exploited vulnerabilities in information management systems to steal cutting-edge weapons designs and pioneering technologies. Consequently, it has been estimated that American corporations lose tens billions of dollars each year due to economic espionage.[26] Further, there is persuasive evidence that hackers directly affiliated with the Chinese government have conducted meticulously planned campaigns to steal large volumes of intellectual property as well as the blueprints to the US military's most advanced weapons systems.[27]

---

[26] The report by the Center for Strategic and International Studies posits that the US losses $100 billion annually due to cyber crime and economic espionage, but does not distinguish the specific costs related to the loss of intellectual property and sensitive weapons designs versus purely financial crimes. See: Lewis, James. "The Economic Impact of Cybercrime and Cyber Espionage," *Center for Strategic and International Studies*. (2013). Pg. 4.

[27] Stanglin, Doug. "Report: Chinese Hackers Breach Top Weapons Designs," *USA Today*. (May 18, 2013). Accessed April 12, 2014. < http://www.usatoday.com/story/news/nation/2013/05/28/chinese-hackers-

The architecture of modern critical infrastructure systems has been substantially transformed by computer networks to enhance the processes for remote control, data acquisition, automation, monitoring, information management, and communication between machines. While this has exponentially improved the efficiency and output of these systems, it has also left them vulnerable to sabotage and cyber attacks with kinetic outcomes. Notably, a test conducted on a power generator at the Idaho National Lab demonstrated that by remotely infiltrating the internal systems of the machine to change its cycle of operation, it is possible to cause the machine catch on fire and cease functioning.[28] In a real-world display of the susceptibility of critical infrastructure systems to cyber attack, American and Israeli cyber forces purportedly disrupted Iran's nuclear weapons program by infecting the Supervisory Control and Data Acquisition (SCADA) systems of the Natanz uranium enrichment plant with a computer virus popularly known as Stuxnet.[29]

Similar to critical infrastructure, warfare has also been revolutionized by digital technologies. Thus, cyber attacks can be launched in conjunction with a conventional assault to subvert critical defense systems and communication networks. In a demonstration of this viable scenario, it has been postulated that the Israeli Defense Forces launched a cyber attack to incapacitate Syrian air defense systems preceding airstrikes on an alleged nuclear complex east of Damascus in 2007.[30]

---

post-designs-breached-compromised/2364969/>. & Mandiant Intelligence. "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*. (2013).

[28] Singer, Peter W. "The Cyber Terror Bogeyman," *Brookings*. (November 2012). Accessed April 7, 2014. <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer>.

[29] In a different type of example, cyber attackers, believed to maintain close ties with the Russian government, launched a massive DDOS strike against Estonia in 2007 that temporarily debilitated the online banking systems, online media, and online government services of the Baltic state. See: Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2011. Pgs. 13-14.

[30] Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013. Pgs. 41-43.

Understanding Terrorism

Definition

Within the debate of what does and what does not constitute terrorism there are no shortages of definitions. For instance, an academic study conducted over twenty-five years ago compiled a list of 109 distinct explanations of terrorism. Even in the post-9/11 era, where counterterrorism is at the forefront of national security policy, the US government—let alone the international community—does not maintain a singular definition.[31] In reality, the only area where there does seem to be general consensus on the term is that its designation involves many negative connotations; therefore, the term is often used as a pejorative. [32]

Regardless, there are key traits that differentiate terrorism from other forms of violence. Acts of terrorism are political in nature and are designed to have far-reaching psychological repercussions that extend to an audience beyond the immediate victim or target.[33] A terrorist attack committed in a vacuum cannot exist. Terrorism must also be premeditated and intentional. If a known terrorist is approached by the police leading to a shoot-out, the act of violence is for self-preservation, even if the perpetrator also holds strong political views against law enforcement.[34] Further, perpetrators who target political figures for non-political reasons also do not meet the threshold of the definition.[35] For example, David Hinckley shooting Ronald Reagan in order to impress actress Jodie Foster is a crime unique to itself.

---

[31] Hoffman, Bruce. *Inside Terrorism: Revised and Expanded Edition*. New York: Columbia University Press, 2006. Pg. 31.
[32] Hoffman. *Inside Terrorism: Revised and Expanded Edition*. Pg. 31.
[33] Hoffman. *Inside Terrorism: Revised and Expanded Edition*. Pg. 40.
[34] For example, if military forces raided a known terrorist hideout, an ensuring firefight should not be considered as an act of terrorism in and of itself.
[35] Hoffman. *Inside Terrorism: Revised and Expanded Edition*. Pg. 35.

Terrorism is distinct in that its combatants are exclusively non-state actors, although states can still sponsor organizations to perpetrate acts of terror on their behalf.[36] This is not intended to be a moral judgment, but recognition that when states conduct violence internationally it is generally accepted as a form of warfare and when violence is dispensed domestically it is perceived as law enforcement.[37] Unlike states, it is easier for terrorists to overcome the constraints of international norms and conventions.[38] For the most extreme groups, there are no targets that are forbidden, including deliberately harming civilians.

Terrorism is also differs from guerilla warfare. Terrorists purposefully avoid engaging enemy military forces head on.[39] Instead, terrorists resort to irregular tactics such as hostage taking and the bombing of army barracks. Unlike insurgencies, terrorists also generally prefer to hide among civilians instead of holding autonomous territory. Even in areas where terrorists maintain powerbases (such as Hezbollah in Southern Lebanon, al-Qaida and its affiliates in the tribal region of Pakistan, and Hamas in the Gaza Strip), fighting among the people remains the terrorist norm.

At its most basic level, terrorism can best be defined as a preplanned method of illegal violence (or a credible threat of violence) targeting civilians, property and even military forces (if not approached directly on the battlefield) that is carried out by a non-state actor in order to bring a political or social objective to the attention of a broad audience.

---

[36] This is not a new phenomenon. Just as Syria and Iran provide funding to Hamas and Hezbollah today, the Soviet Union provided training and monetary support to left-wing terrorist and ethno-national organizations during the 1970s and 1980s among countless other examples.

[37] That being said, this does not disregard or excuse the fact that in comparison to terrorism, significantly more civilians have been killed or displaced due to state actions. See: Cronin, Audrey K. *Ending Terrorism: Lessons for Defeating al-Qaeda*. New York: Routledge, 2008. Pg. 7.

[38] It should be recognized that terrorist organizations can be accused of committing war crimes; however, there has not been an established precedence to prosecute terrorists in the International Criminal Court. Ironically, this is primarily due to that fact that an agreed upon definition of terrorism could not be established by the court.

[39] Hoffman. *Inside Terrorism: Revised and Expanded Edition*. Pg. 35.

While this broad definition is useful for developing a framework to understand terrorism, it lacks the precision to clarify how different perpetrators employ the tactic. As terrorism expert Bruce Hoffman notes, "all terrorist groups seek targets that are rewarding from their point of view and employ tactics that are consonant with their overriding political aims." Thus, groups attempting to capture the support of a wide-ranging audience will have a different perspective on civilian casualties in comparison to a group inspired by religious doctrine. To illustrate, the motivations of the Irish Republican Army were entirely incongruent with al Qaeda's and so were their tactics.

Nevertheless, when terrorism is observed across different eras, a framework for identifying groups by collective ideologies does emerge.[40] Since the late 19th century, there have been four distinct 'waves' of terrorism: early 20th century anarchist movements, post-World War II anti-colonial groups, new-left organization that were prevalent during the 1960s and 1970s, and the religiously-inspired Jihadist extremists of today.[41]

Following Hoffman's logic, shared political aims beget shared tactics and objectives. Anarchists assassinated political leaders to induce global chaos. Anti-colonial groups killed law enforcement and military units to convince their ruling authorities to grant independence. New-left groups hijacked airlines and attacked embassies to bring international attention to the plight of the 3rd-world minority movements and the evils of capitalism. Present day faith based extremists, as examined in the next section, use religious fanaticism to justify attacks against civilians as a means to establish a new world order against secularization and modernity.

---

[40] Rapoport, David C. "The Four Waves of Modern Terrorism," *Attacking Terrorism: Elements of a Grand Strategy* Eds. Audrey K. Cronin and James M. Ludis. Washington: Georgetown University Press, 2004. Pgs. 46-73.

[41] This does not mean that all terrorists today are Jihadist extremists. In fact, domestic terrorist groups still exist on both the left (animal and environmental rights extremists) and the right (anti-abortion groups). Further, religiously inspired resistance movements like Hezbollah and Hamas, share many qualities with extremists from previous eras. Nonetheless, Rapport highlights that it is the Jihadist element of terrorism that is most dominant today. See: Rapoport, David C. "The Four Waves of Modern Terrorism," Pg. 47.

The Modern Terrorist Threat

Jihadist terrorists do not abide by the long held aphorism, originally attributed to RAND scholar Brian Jenkins, that "terrorists want a lot of people watching, not a lot of people dead." Instead, as Jenkins reassessed thirty years later, groups today "want a lot of people watching *and* a lot of people dead" [emphasis mine].[42] In modern times, ultraconservative religious doctrine and sanction from radical spiritual leaders has legitimized support for mass casualty incidents among extremists.

Terrorists today also no longer want to capture the hearts and minds of moderate audiences and attain international legitimacy.[43] In previous eras, even the head of the Palestinian Liberation Organization (PLO) would speak in front of the United Nations (UN) General Assembly while still championing terrorism. In contrast, not only are modern terrorists not concerned with converting moderate sympathizers, they also maintain little interest in seeking a seat at the negotiating table.[44] Rather, as ex-CIA Director James Woolsey once stated, contemporary "(terrorists) want to destroy the table *and* everyone sitting in it" [emphasis mine].[45]

Furthermore, modern terrorist groups are better financed, better trained, more transnational, and more difficult to penetrate than their predecessors.[46] Advances in communication technology ensure that extremist tactics and ideology can be spread to a global audience, increasing the likelihood of lone wolf terrorist incidents. Secure and anonymous

---

[42] Jenkins, Brian M. "The New Age of Terrorism," *Homeland Security Handbook*. Ed. David G. Kamien. New York: McGraw-Hill, 2006. Pg. 119.
[43] Howard, Russell D. and Nencheck, Margaret J. "The New Terrorism," *Terrorism and Counterterrorism: Understanding the New Security Environment. (4th Edition)*. Eds. Bruce Hoffman and Russell D. Howard. York: McGraw-Hill, 2012. Pg. 143.
[44] Howard, Russell D. and Nencheck, Margaret J. "The New Terrorism," Pg. 146.
[45] Public Broadcasting Service. "Plague War: Interview James Woolsey," *PBS Frontline*. Accessed March 3, 2014. <http://www.pbs.org/wgbh/pages/frontline/shows/plague/interviews/woolsey.html>.
[46] Howard, Russell D. and Nencheck, Margaret J. "The New Terrorism," Pg. 143.

connections over the internet provide a low cost, low risk means for groups to scout potential targets for conventional attacks, recruit new members, spread propaganda, share designs for weapons, and fundraise.[47] Terrorist training camps in failed states and income streams from legal and illegal sources also reduce reliance upon state sponsors.[48] The evolution of terrorism has fundamentally changed the nature of terrorist targets, tactics, and the perpetrators themselves.

With the norm against mass casualty incidents shattered, there are no longer targets that are 'off-limits' to an attack. In carefully crafted statements, Osama bin Laden made it exceedingly clear that all American citizens are legitimate targets due to the sins of their government.[49] Thus, transportation hubs, symbolic monuments, office buildings, and nuclear reactors, to name a few, all feasibly face the threat of a terrorist strike. Even more startling, coordinated strikes can endanger multiple targets at once and, as painfully established by 9/11, the murder of thousands has become an unfortunate reality.

In terms of tactics, modern terrorists have pursued both old and new techniques to perpetrate mass violence. To this day, data from the Global Terrorism Database confirms that terrorist groups prefer to use firearms and explosives over other weapons—just as they did two decades ago.[50] The primary difference, of course, is now guns and bombs are more likely to be directed against civilian targets instead of symbolic objects or entities of the state.

Moreover, terrorist groups also continue to innovate to pursue more deadly means. Box-cutters provided a sufficient tool for the perpetrators of 9/11 to hijack four airplanes and subsequently turn the machines into human missiles. Later, various groups would perfect the

---

[47] Singer, Peter W. "The Cyber Terror Bogeyman," *Brookings.*
[48] Howard, Russell D. and Nencheck, Margaret J. "The New Terrorism," Pg. 143.
[49] Nacos, Brigitte. *Terrorism and Counterterrorism*. Boston: Pearson Longman, 2012. Pg. 139.
[50] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2012). *Global Terrorism Database*. Accessed March 23, 2014. <http://www.start.umd.edu/gtd>.

technique of hiding time-delayed bombs that would detonate upon the arrival of first responders. Yet, two perfidious tactics above others demonstrate the potential for extremists to overcome heightened security and commit mass violence: suicide terrorism and weapons of mass destruction (WMD).[51]

Suicide terrorism is a preplanned method of politically motivated violence where the certain death of the perpetrator is necessary for the completion of the attack.[52] Terrorists can use a variety of methods to carry out a suicide attack that include detonating a bomb placed on their body, driving an explosive filled vehicle into their target, or flying an airplane into a building. Since the perpetrator does not care about survival, the suicide terrorist has no need for an escape plan and can infiltrate some the most hardened targets. Moreover, the terrorist can make 'last-minute adjustments' to overcome any setbacks and attack a target at its weakest point.[53] The impact of suicide terrorism can best be encapsulated by the statistic that, throughout history, this tactic has caused four times more deaths than any other forms of terrorism.[54]

WMDs are unique in terms of their expansive destructive capabilities against infrastructure and human life.[55] While chemical, biological, radiological, and nuclear weapons are fearsome, they are difficult to create without technological expertise, difficult to smuggle due

---

[51] This being a paper about cyber attacks it would be remiss not to mention that there is general agreement that terrorist groups currently lack the technological savvy to kill or maim via cyberspace. While extremist organizations have demonstrated the know-how to sabotage government websites through DDOS attacks, these incidents have not resulted in any kinetic damage and do not meet the violence threshold of a terrorist attack. See: Singer, Peter W. "The Cyber Terror Bogeyman."

[52] Bloom, Mia. *Dying to Kill: The Allure of Suicide Terrorism*. New York: Columbia University Press, 2007. Pg. 76.

[53] Pape, Robert A. "The Strategic Logic of Suicide Terrorism," *American Political Science Review*, no. 97. (2003). Pg. 346.

[54] Hoffman. *Inside Terrorism: Revised and Expanded Edition*. Pg. 133.

[55] This tactic is normally grouped into four different modalities: chemical weapons, (e.g., crude devices that spread blood gases, blistering agents, choking agents, and nerve agents), biological weapons (e.g., the release of both contagious and non-contagious pathogens such as anthrax, smallpox, and ricin), radiological weapons (e.g., explosives that disperse radioactive material), and nuclear weapons (e.g., a military-use or improvised device that releases energy as a result of a nuclear reaction). See: Tobey, William, and Bunn, Matthew. "Chemical and Biological Weapons," *IGA-232: Controlling the World's Most Dangerous Weapons*. Harvard Kennedy School, Harvard University, Cambridge, MA. (October 3, 2013).

to export controls and heightened security procedures, and difficult to turn into functional weapons.[56] As of yet, terrorist groups have not found a way to employ WMDs en masse.[57]

Nonetheless, prudent security policy makes it impractical and irresponsible to rule out the threat of WMD terrorism, especially as chilling documents discovered in an al Qaeda safe house in Afghanistan revealed that the organization was (and perhaps still is) interested in learning everything it can about constructing a nuclear device.[58] Further, the 2007 breach of a weapons-grade uranium storage facility in South Africa by four armed thieves demonstrates that it is impossible to ensure complete security of even the most hazardous WMD material.[59] Placing this threat into context, at a 2010 nuclear security symposium among world leaders, President Barack Obama declared the prospects of nuclear terrorism as "the single biggest threat to US security, both (in the) short-term, medium-term and long-term."[60]

Comparing the Concepts: Similarities

This section identifies the similarities between terrorism and cyber attacks to best highlight the key features where the two concepts overlap. Special attention is paid to the political and strategic implications of each issue.

---

[56] Tobey, William, and Bunn, Matthew. "Chemical and Biological Weapons."
[57] Case in point: (a) the Aum Shinrikyo sarin gas attacks in Tokyo that killed thirteen almost two decades ago remains the most notable terrorist chemical attack, (b) although the 2001 anthrax attacks attracted enormous media coverage, they only directly resulted in five deaths and no other biological terrorist attacks have surpassed these totals, and (c) there has yet to be a verifiable instance of a terrorist group obtaining a nuclear device or even nuclear material.
[58] Nacos, Brigitte. *Terrorism and Counterterrorism*. Pg. 156.
[59] Zenko, Micah. "A Nuclear Site Is Breached," *Washington Post*. (December 20, 2007). Accessed April 24, 2014. <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/19/AR2007121901857.html>.
[60] Jackson, David. "Obama: Nuclear Terrorism is the 'Single Biggest Threat' to U.S.," *USAToday* (April 11, 2010). Accessed April 2, 2014. <http://content.usatoday.com/communities/theoval/post/2010/04/obama-kicks-off-nuclear-summit-with-five-leader-meetings/1#.UzuRBPldWSp>.

Lack of a Universal Definition

Terrorism is a concept easier described than discussed.[61] Not only has the nature of the threat evolved multiple times over the past century, the tactic also evokes many controversial political issues such as self determination, religious freedom, and human rights. As such, all attempts at an internationally agreed upon definition of terrorism have failed.[62] Any potential universal designation of terrorism will likely be so broad that it will be of little use.[63]

Cyber attacks are an incipient phenomenon and there is still much misunderstood and unknown about how best to succinctly describe the threat. Two government led attempts to define the concept that have resulted in markedly different conclusions. The US Joint Chiefs of Staff developed a narrow definition of a cyber attack, focusing on the warfare aspects of disrupting computer systems and the prevalence of force. The Shanghai Cooperation Organization (a Eurasian regional organization dominated by China and Russia), on the other hand, established an expansive definition of a cyber attack that included the use of cyber technology to foment political unrest.[64] The prospect for finding common ground between these two definitions does not appear to be likely.

The lack of clear, concise, and internationally sanctioned definitions for terrorism and cyber attacks complicate global efforts to combat these threats. For example, the UN Convention on International Terrorism resulted in a deadlock in most part due to the lack of

---

[61] Mockaitis, Thomas R. "Terrorism, Insurgency, and Organized Crime," *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011. Pg. 17.
[62] While the UN Security Council has passed multiple anti-terrorism resolutions, the world body does not yet maintain a specified list of terrorist groups. See: Graham, Kennedy. "The Security Council and Counterterrorism: Global and Regional Approaches to an Elusive Public Good," *Terrorism and Political Violence* 17, no. 1 (2005). Pg. 52. & Nacos, Brigitte. *Terrorism and Counterterrorism*. Pg. 47.
[63] Mockaitis, Thomas R. "Terrorism, Insurgency, and Organized Crime," Pg. 17.
[64] Hathaway. "The Law of Cyber-Attack," Pgs. 8-11.

agreement on what constitutes terrorism.[65] Likewise, Russia and China have refused to commit to the European Convention on Cyber Crime due to their disagreements on what encapsulates a cyber attack.[66]

Further, both concepts are mired with 'grey areas' that can be used to conflate issues and provide distractions from serious problems. Groups such as the PLO and even al Qaeda have long attempted to reduce the scope of the term terrorism and justify civilian casualties by defending their actions under the guise of freedom fighting and thwarting oppression. On the cyber front, alternatively, Chinese government officials have attempted to inflate the definition of a cyber attack to frame online anti-government criticisms as its own form of assault, thus rationalizing methods to silence dissidents.[67]

Everything is a Target

As previously discussed, religiously inspired Jihadist terrorists are not constrained by ideology or morals from attacking civilian and non-combatant targets. Additionally, suicide terrorism and the potential of WMD attacks reduce the ability to harden high-profile security targets. Thus, almost all aspects of everyday life are potentially vulnerable to attack; no matter whether someone is at their home, at work, or on vacation.

In a similar sense, any device that is connected to cyberspace is feasibly at risk of a cyber attack. This goes beyond personal computers to include mobile devices, cloud computing systems, and critical infrastructure architecture. The constant development of innovative and

[65] Deen Thalif. "Politics: U.N. Member States Struggle to Define Terrorism," *Inter Press Service News Agency*. (July 25, 2005). Accessed April 5, 2014. <http://www.ipsnews.net/2005/07/politics-un-member-states-struggle-to-define-terrorism/>.
[66] Nye. "Nuclear Lessons for Cyber Security?" Pg. 30.
[67] Singer and Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Pg. 68.

more intricate cyber attack methods ensure that the security of almost any computer system cannot be taken for granted.

Further, the consequences of a successful cyber attack are vast. Not only are over two billion people connected to the internet, but almost all sectors of contemporary society (including communications, transportation, health care, and national defense) rely on the proper functioning of industrial control systems that are run on computer networks.[68]

The far-reaching list of potential targets for both terrorists and cyber attackers make it impossible for policymakers to guarantee complete security. Further, active measures to increase security in public places are costly, inconvenient, and can potentially restrict freedoms. Even if certain vulnerabilities are made impenetrable, the almost unending menu of targets ensures that motivated adversaries will remain unfettered. For instance, the installation of metal detectors at airports during the 1970s did not lead to an end of terrorism. Instead, extremists shifted their punishments to other soft targets. While airplane hijackings decreased significantly during this era, the rates of kidnapping and embassy invasions greatly increased.[69]

The Attribution Conundrum

Unlike professional soldiers, terrorists generally do not wear uniforms or other identifying garb. Rather, most terrorists attempt to blend in with civilians in order to overcome security barriers before conducting an attack.[70] While historically terrorists went out of their way to claim their attacks—even sometimes contacting the media directly—this no longer remains the norm. For example, the perpetrators of the 2013 Boston Marathon bombings did not

[68] Martel, William. "Critical Infrastructure," *DHP-P249: Foundations of International Cybersecurity*. Fletcher School of Law and Diplomacy, Tufts University, Medford, MA. (November 21, 2013).
[69] Enders, Walter and Todd Sandler. *The Political Economy of Terrorism*. New York: Cambridge University Press, 2006. Pgs 111-132.
[70] Even when specific perpetrators are identified, that does not necessarily mean that they can be linked to a terrorist group.

leave a manifesto or make any attempt to identify themselves to the public. Instead, the widespread uncertainty behind the motives of the attack, especially during ensuing manhunt, paralyzed a region and enhanced feelings of insecurity due to the insidious nature of the threat of the unknown.

Anonymity is one of the most menacing characteristics of cyber attacks because the architecture of the internet makes it relatively straightforward for the perpetrators of cyber attacks to hide their identities.[71] Complex tactics like multi-stage attacks (where perpetrators infiltrate a computer's internal hard drive to launch attacks on other systems) and information systems like Tor networks (that mask internet communication) make it difficult, if not impossible, to trace the initial location of an attack.[72] Even if the original computer system behind an attack is identified, that still does not necessarily answer questions as to who owns the machine, where the machine is located, and which individual or individuals are behind the machine.[73] With a nod to the incognito nature of the internet, one of the most infamous and well-known hacktivist groups goes by the moniker 'Anonymous.'

Incidents lacking clear attribution create considerable political and strategic challenges. First and foremost, these incidents makes it more challenging to comprehend the true extent of the threat in question, specifically, whether an attack is part of a limited strike or a greater conspiracy. Additionally, attribution issues make it more complicated to prosecute and punish the perpetrators, while also, increasing the likelihood of a long and costly investigation process. Finally, obstacles to trace original perpetrators raise the probability that adversary states that

---

[71] Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38 no. 2. (Fall 2013). Pg. 46.
[72] Clark, David D. and Susan Landau. "Untangling Attribution," *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Ed. National Research Council. Washington, DC: The National Academies Press (2010). Pgs. 26-33.
[73] Clark, David D. and Susan Landau. "Untangling Attribution," Pgs. 25-26.

wish to avoid direct military confrontation will furtively sponsor extremist groups as a method to target common enemies while reducing opportunities for retaliation.

Deterrence Constraints

Deterrence theory revolves around the concept that an adversary's cost benefit analysis can be altered through a combination of offensive and defensive measures. Tactics revolve around the balance between issuing credible threats of punishment and denying access to potential targets. While this strategy proved integral in preventing nuclear confrontation during the Cold War, its applications to counterterrorism are constrained by the nature the terrorist threat.[74] On one extreme, it is near impossible to effectively develop a punishment that will dissuade a fundamentalist terrorist already willing to commit suicide for their cause.[75] Even if the perpetrator values his or her own survival, the lack of a return address makes it difficult to impose retribution.[76] As non-state actors, terrorists lack a capital city or public institutions that can be targeted and generally maintain a higher threshold to accept punishment in comparison to sovereign states.[77]

Moreover, even if potential terrorist targets existed, threatening to strike them would not necessarily affect the behavioral calculus of a group. Understanding what your adversary values is complex. It took decades for Washington and Moscow to refine and develop a comprehensive platform for deterrence during the Cold War. Today, there are a multitude of terrorist groups; each with unique ideologies, motivations, and leadership structures. In short, each terrorist

---

[74] Harvey, Frank and Alex Wilner. "Counter-Coercion, the Power of Failure, and the Practical Limits of Deterring Terrorism," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012. Pg. 109.
[75] Stein, Janice G. "Deterring Terrorism, Not Terrorists," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012. Pg. 47.
[76] Stein, Janice G. "Deterring Terrorism, Not Terrorists," Pg. 50.
[77] Lewis, James A. "Cross-Domain Deterrence and Credible Threats," *Center for Strategic and International Studies* (July 2010). Pg. 3.

group—let alone every lone wolf actor—will potentially respond to punishment in different ways.

"The Internet was not designed with the goal of deterrence in mind" declare leading cyber scholars David Clark and Susan Landau.[78] The attribution of cyber attacks, as mentioned above, is a complicated process that might never produce definitive answers that identify the perpetrators. The confidence in which the most sophisticated cyber attackers believe that they can mask their identities makes it probable, if not expected, that they will not be deterred by the fear of direct punishment. Further, in terms of purely defensive based strategies, the incapacity to secure all potential targets against cyber attack also reinforces the difficulty of constructing a credible deterrence by denial.

The inability to develop all-encompassing strategies to deter terrorists and cyber attackers makes it increasingly difficult for policymakers to neutralize either threat. Moreover, attempting to punish vague, misunderstood threats can potentially lead to inferior outcomes. Combating terrorists interspersed among civilians will inevitably result in civilian casualties and can potentially harden a group's resolve to conduct terrorism. Likewise, incorrectly identifying the perpetrators of a cyber attack can tempt the true assailants to become more assertive and conduct increasingly brazen attacks.

Potential for Low Probability, High Impact Attacks

The vast majority of terrorist attacks, while perfidious, do not result in any fatalities.[79] However, this does not alleviate the possibility for unanticipated or rare incidents with perilous results. The most relevant past example of this sort of outlier terrorist incident is 9/11. Not only did this disastrous event surpass Pearly Harbor as the deadliest attack on American soil, but it

[78] Clark, David D. and Susan Landau. "Untangling Attribution," Pgs. 25.
[79] National Consortium for the Study of Terrorism and Responses to Terrorism. *Global Terrorism Database*.

also triggered an economic loss of $200 billion.[80] Perhaps even more catastrophic, the detonation of a terrorist nuclear device in a major metropolitan area can potentially cause hundreds of thousands of casualties, crash financial markets, and incur a over $1 trillion in physical damages alone.[81]

Although it is difficult to estimate the recurrence of cyber attacks, 48,562 cyber incidents were reported to the US Computer Emergency Readiness Team (US-CERT) in 2012.[82] While the magnitude of cyber attacks might appear calamitous when applied on a worldwide scale, the lion's share of attacks either fail or cause negligible damage. Nevertheless, the effects of a high impact attack remain real. For example, the possibility cannot be discounted that a cyber attack sabotaging vulnerabilities in the SCADA systems of critical infrastructure can disrupt the power grid, shut down a nuclear reactor, open a dam, delay air travel, and even contaminate water supplies. Further, financial markets across the world are dependent on electronic transactions and access to online bank accounts. If these networks were temporarily incapacitated by a cyber attack and people could not retrieve or invest their financial holdings, consumer confidence would be dealt a harsh blow—as would the health of the global economy.

The latent risk of high impact incidents compels policymakers to treat both concepts as national security threats, even though the vast majority of terrorist and cyber attacks are inconsequential on a national scale. Further, developing strategies to anticipate and mitigate the threat of low probability incidents is costly, imperfect, and difficult to verify success. After

---

[80] This does not even take into account the over $3 trillion that were spent on post 9/11 responses such as enhanced security measures and funding wars in Afghanistan and Iraq. Source: Carter, Shan, and Amanda Cox. "One 9/11 Tally: $3.3 Trillion," *New York Times*. (September 8, 2011). Accessed October 7, 2013. <http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0>.

[81] Allison, Graham. "Nuclear Deterrence in the Age of Nuclear Terrorism," *MIT: Technology Review*. (October 20, 2008). Accessed April 3, 2014. <http://www.hks.harvard.edu/news-events/news/news-archive/nuclear-deterrence-in-age-of-terrorism>.

[82] United States Government Accountability Office. "High-Risk Series," *Report to Congressional Committees*. (February 2013). Pg. 184.

suffering from a 'failure of imagination' pre-9/11, the US government doubled the budget of its intelligence agencies as a means to better predict potential national security vulnerabilities.[83] At the same time, the US spends billions of dollars each year combating potential nuclear terrorists and funding programs to secure nuclear storage facilities throughout the world.[84] While in comparison to potential disaster, this might appear to be money well spent, in reality evaluating the efficacy of these programs is complicated. Over a decade since 9/11, an equivalent (or worse) terrorist attack has yet to take place. While this might be due to the revamped counterterrorism programs implemented by the US government in the years since, without the benefit of hindsight it is also feasible that the potential for another catastrophic terrorist incident was overestimated in the first place Thus, policymakers face the difficult to decision of allocating limited resources wisely, while also protecting against the unpredictable. This balance is accentuated during times of hemorrhaging defense budgets and stagnation in government employment.

Comparing the Concepts: Differences

No analogy is perfect and comparing the two concepts too literally without understanding their differences can lead to detrimental outcomes.[85] This section identifies where there are stark contrasts between terrorism and cyber attacks.

---

[83] MacAskill, Ewen, and Jonathan Watts. "US intelligence spending has doubled since 9/11, top secret budget reveals," *The Guardian*. (August 29, 2013). Accessed April 3, 2014. <http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget>.
[84] Exact numbers on what the US spends to combat nuclear terrorism is difficult to ascertain. According to the Carnigie Endowment for International Peace, the US in 2008 spent of total $52.4 billion on nuclear security with over $5 billion spent on nuclear threat reduction. This does not include money spent on classified intelligence programs. See: Schwartz, Stephen I., and Deepti Choubey. "Nuclear Security Spending: Assessing Costs, Examining Priorities," *Carnegie Endowment for International Peace*. (2009). Pg. 7.
[85] Nye. "Nuclear Lessons for Cyber Security?" Pg. 35.

Different Designations

The definitions of terrorism and cyber attacks differ as a means to distinguish the concepts from other threat such as classic state-versus-state warfare and purely criminal activities. Cyber attacks must initiate in the digital realm and target the functions of a computer system before there are any physical consequences, whereas the theoretical setting of a terrorist attack is immaterial to its definition.[86] Alternatively, terrorist attacks must be conducted by non-state actors and result in destruction (or threats of destruction), while cyber attacks can be perpetrated by both state and non-state actors. Further, cyber attacks can also encumber non-kinetic political activities such as espionage, theft, and website defacement.

Different Feasible Outcomes

The potential consequences of terrorism and cyber attacks are also dissimilar. First, the kinetic outcomes of cyber attacks are far less perilous than that of terrorism. While critical infrastructure systems remain vulnerable to attack, they are already built with a variety of protection mechanisms to survive natural disasters and routine outages. A cyber attack might shut down these systems temporarily—and cause great inconvenience—but the likelihood of inflicting a Pearl Harbor-esque casualty count through cyber alone remains remote. In fact, the number of deaths attributed to cyber attacks (even indirectly) is zero.[87] In contrast, the kinetic outcomes of terrorism are tangible and treacherous. In the decade since 9/11, terrorist attacks have killed over 90,000 people.[88]

---

[86] Singer and Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Pg. 68.
[87] Atherton, Kelsey D. "Cyber Attacks Are America's Top Security Threat. That's Better News Than It Sounds," *Popular Science*. (March 14, 2013). Accessed April 6, 2014. <http://www.popsci.com/technology/article/2013-03/cyber-attacks-were-named-top-security-threat-%E2%80%99s-better-news-it-sounds>.
[88] National Consortium for the Study of Terrorism and Responses to Terrorism. *Global Terrorism Database*.

While less catastrophic to human life, cyber attacks exhibit other hazardous qualities. Attacks in cyberspace take place at supersonic speeds and victims might be oblivious that anything is out of the ordinary. To demonstrate, one of the ingenious techniques of the Stuxnet attack was that the malicious computer virus cloaked its identity for months, tricking Iranian authorities into believing that their faulty centrifuges were the result of human error. Conversely, the kinetic nature of terrorism ensures that the victim's awareness of an attack is immediate, and naturally, the incident cannot continue undetected.

Different Perpetrator Capabilities

The most threatening cyber attacks, like APTs, are complex and require substantial investment to foster the cutting edge technological capabilities in order to avoid discovery and exploit access. For instance, the development and implementation of the Stuxnet virus involved the coordinated efforts of cyber experts, nuclear physicists, engineers, and intelligence analysts.[89] As of yet, the only potential perpetrators of these types of incidents are states with advanced military resources and technological expertise.[90] On the contrary, while tactics vary, large scale acts of terrorism do not necessitate extensive training or expertise. Access to guns and homemade explosives make it possible for a motivated individual to cause widespread destruction. Case in point, the 1995 Oklahoma City bombing and 2009 Fort Hood shooting—the second and third deadliest domestic terrorist attacks—were both perpetrated by love wolves not directly affiliated with any terrorist organization or state entity.

[89] Singer, Peter W. "The Cyber Terror Bogeyman."
[90] Only five countries have been identified as maintaining advanced offensive cyber capabilities: the US, China, France, Russia, and Israel. See: McAfee. "Virtually Here: The Age of Cyber Warfare," *McAfee Virtual Criminology Report* (2009). Pg. 13.

Counterterrorism Lessons for Cybersecurity

Since the attacks of 9/11, the US government has reorganized its national security strategy to confront and mitigate the threat of Jihadist terrorism at its core. The transformational shift did not occur without growing pangs. The rapid expansion and reorganization of the federal homeland security apparatus resulted in mismanagement and a bloated bureaucracy; scandals over torture and civilian casualties spawned waves of anti-American sentiment abroad; and the War in Iraq put the US at odds with some of its closest historical allies and eventually bred domestic disillusionment when intelligence assessments of Saddam Hussein's WMD program were proven incorrect. These problems were exacerbated as al Qaeda and likeminded terrorist groups remained active abroad.

Yet, over a decade after 9/11, the US learned from both its success and mistakes to develop a more mature and dynamic counterterrorism strategy with fruitful results. To highlight, the US has averted international debacles and government overreach domestically, while also, improving methods to surgically root out terrorist threats through robust intelligence and innovations such as UAVs. Osama bin Laden is dead, at least forty-five terrorism plots have been foiled at home, and broad public support has emerged for the Obama administration's counterterrorism policies.[91] Most importantly, the horrors of 9/11 have not been replicated.

This section explores how specific lessons learned from fighting terrorism since 9/11 can be applied to shape future cybersecurity strategy and policy. To conduct this analysis, I

[91] Avlon, John. "Forty-Five Foiled Terror Plots Since 9/11," *Newsweek Magazine: The Daily Beast.* (September 8, 2011). Accessed April 18, 2014. <http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-foiled-in-last-10-years.html>. & Wilson, Scott and Jon Cohen. "Poll Finds Broad Support for Obama's Counterterrorism Policies," *Washington Post.* (February 8, 2012). Accessed April 18, 2014. <http://www.washingtonpost.com/politics/poll-finds-broad-support-for-obamas-counterterrorism-policies/2012/02/07/gIQAFrSEyQ_story.html>

incorporate specific examples of successful counterterrorism programs as well as the opinions of leading counterterrorism and cybersecurity experts.

Lesson 1: Limited Deterrence Should Not Be Discounted

While deterrence by itself is insufficient to combat terrorism, it can still play an effective role as one spoke of a greater counterterrorism strategy. Specifically, there are two areas where deterrence can be particularly effective: obstructing state sponsors of terrorism and demonstrating that attacks are futile through bolstered resilience.

In comparison with radical non-state actors, nation-states are easier to scrutinize, easier to target, and face a greater motivation to avoid implication in a large scale terrorist incident.[92] As evidence, the US government was able to stifle Libya from backing radical groups —and eventually convince the Qadaffi regime to quit supporting terrorism altogether—through a combination of economic carrots and sticks.

Beyond actions against state actors, deterrence by denial is generally more valuable than deterrence by punishment. Defensive strategies are less intrusive and are also less likely to result in unintended negative consequences.[93] In addition to hardening at-risk targets, the US has nurtured resilience by developing and publicizing disaster planning and emergency response systems. This acts as a public signal to prospective terrorists that the consequences of their actions will be not be lasting.[94]

---

[92] Trager, Robert F. and Dessislava P. Zagorcheva. "Deterring Terrorism: It Can Be Done." *International Security* 30 no. 3 (Winter 2005/06). Pg. 97.
[93] Wenger, Andreas and Alex Wilner. "Deterring Terrorism: Moving Forward," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012. Pg. 322.
[94] Kroenig, Matthew and Barry Pavel. "How to Deter Terrorism," *Center for Strategic and International Studies: The Washington Quarterly* 35, no. 2 (Spring 2012). Pg. 30.

Applicability of Lesson 1 to Cybersecurity

Offensive actions to credibly deter threats from the cyber realm are limited. International norms on how to proportionally respond to a cyber attack—be it a kinetic attack or a retaliatory cyber strike—are ill-defined and likely to lead to considerable uncertainty, especially when the perpetrators are uncertain or an adversary's goals are unclear. Nonetheless, it is plausible that clearly defined 'red-lines' can effectively deter nation-states from harboring cyber attackers and, also, from conducting cyber attacks on their own accord.

Bolstering the resilience of computer systems also marks a genuine opportunity to foster deterrence. Limited security breaches should be accepted as an inevitable—but not necessarily catastrophic—event.[95] Thus, the federal government should incentivize investments in the redundancy and continuity of service of cyber systems. Another means to reinforce resiliency is to reiterate to the general public that the temporary incapacitation of critical systems is an unavoidable, but survivable reality.[96] By demonstrating that our computer networks can tolerate intrusions and maintain functionality during a cyber attack, it will discourage the efforts of future perpetrators.

Lesson 2: The Government Must Synchronize Its Response

Taking a 'Whole-of-Government' approach to counterterrorism requires bureaucracy-wide reorganization as a means to streamline strategic direction, avoid duplication of work, prioritize budgets, coordinate responses, and share information with the private sector and allies abroad.

---

[95] Nye, Joseph S. "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly 5, no. 4 (Winter 2011). Pg. 25.

[96] Demchak, Chris. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Ed. Derek S. Reveron. Washington: Georgetown University Press, 2012. Pg. 130.

Recognizing that a piecemeal approach to counterterrorism was no longer acceptable, DHS was launched after 9/11. This nascent organization consolidated twenty-two departments that were previously independent or part of larger agencies and was organized into four major directorates: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection. While intentions were in the right place, the most drastic security sector reorganization since 1947 was initially fraught with turf battles, mismanagement, and disorganization that were most notably manifested during the bungled response to Hurricane Katrina.[97] It was not until DHS was reformed to grant its member agencies more independence—while still reporting to the Secretary of Homeland Security—that the organization was able to competently perform its intended mission.

Applicability of Lesson 2 to Cybersecurity

While DHS maintains a cybersecurity division within its Infrastructure Protection Directorate, the FBI manages the National Cyber Investigative Joint Task Force (NCIJTF), and the Department of Defense operates US Cyber Command, there is currently no singular federal agency or department that coordinates or guides US cybersecurity policy and strategy. Accordingly, organizational problems include a lack of strategic focus, overlapping missions, and diffuse responsibility.[98]

To solve these problems, a National Office for Cyberspace established under the umbrella of the National Security Council should be created. This office, as originally proposed by a presidential commission on cybersecurity, can provide overall strategic direction; monitor

[97] Nacos, Brigitte. *Terrorism and Counterterrorism*. Pgs. 239-240.
[98] Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency," *CSIS Commission on Cybersecurity for the 44th Presidency.* (December 2008). Pg. 34.

and assess the effectiveness of federal programs; act as a collaborative network among key agencies; provide a focal point to engage the private sector; and oversee the protection of civil liberties.[99] As not to become too cumbersome, this office should act more as a clearinghouse for information and allow existing agencies to maintain their current responsibilities.

Lesson 3: The Intelligence Community Will Play a Principle Role

Current and accurate intelligence is the first line of defense against terrorism.[100] Good intelligence is key to understanding the behavioral patterns and thought calculus of an adversary, obtaining awareness to vulnerable targets, and, most importantly, thwarting terrorist plots before they can be launched. Unfortunately, leading up to 9/11, the US intelligence community was hampered by poor practices of information sharing, insufficient human intelligence, a lack of state-of-the-art technology, and a shortage of linguists.[101] At the recommendations of the 9/11 Commission, the intelligence community was consolidated and centralized under the Office of the Director of National Intelligence. Moreover, the National Counterterrorism Center (NCTC) was launched to reduce barriers between agencies to allow for greater information sharing.[102]

Shifting from a 'need-to-know' culture toward a 'need-to-share' paradigm has resulted in a much improved counterterrorism apparatus.[103] NCTC in particular has provided a positive model for interagency coordination as well as cultivating solid links between analysts and government decision makers.[104] In fact, persuasive evidence suggests that the majority of failed

---

[99] Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency," Pg. 38.
[100] Nacos, Brigitte. *Terrorism and Counterterrorism*. Pgs. 244.
[101] Nacos, Brigitte. *Terrorism and Counterterrorism*. Pgs. 246-248.
[102] Art, Robert J. and Louise Richardson. *Democracy and Counterterrorism: Lessons from the Past*. Washington: United States Institute of Peace Press, 2007. Pg. 588.
[103] Budinger, Zoe Baird and Jeffrey H. Smith. "Ten Years After 9/11: A Status Report on Information Sharing," *Senate Committee on Homeland Security & Governmental Affairs.* (October 12, 2011). Pg. 3.
[104] Cline, Lawrence E. "Interagency Decision Making," *Fighting Back: What Governments Can Do About Terrorism.* Ed. Paul Shemella. Stanford: Stanford University Press, 2011. Pg. 173.

terrorist plots have been foiled through a combination of conventional law enforcement and domestic intelligence collection.[105]

Applicability of Lesson 3 to Cybersecurity

In a battlefield rife with vulnerabilities and unidentifiable perpetrators, knowledge is power and accurate intelligence is paramount. Currently, the NCIJTF acts a focal point for the intelligence community and law enforcement to coordinate and share information regarding domestic cyber threat investigations.[106] While this is a positive first step, cyber attacks are a worldwide conundrum. The mission of the NCIJTF should be expanded to match the reality that international incidents can quickly escalate into domestic threats. Further, significant resources should also be allocated to enhance cyber-forensic capabilities and all-source intelligence gathering methods. The intelligence community can play a leading role in unmasking perpetrators.

Lesson 4: Raise Public Awareness

Of all the counterterrorism tools within a government's arsenal, ordinary citizens, in the end, are the most important.[107] With a multitude of soft targets that are beyond the means of government protection, the public maintains an integral role to remain vigilant and frustrate, if not foil, attacks in progress. For example, impending terrorist attacks at Fort Hood, Times Square, and an airplane bound to Detroit were foiled by the actions of an attentive gun shop

[105] Dahl, Erik J. "The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States," *Studies in Conflict & Terrorism* 34 no. 8 (2011). Pg. 621.
[106] For more information on the NCIJTF see: http://www.fbi.gov/about-us/investigate/cyber/ncijtf
[107] Shemella, Paul. "Tools for Strategies for Combating Terrorism," *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011. Pg. 145.

clerk, an observant street vender, and quick-acting passengers, respectively.[108] An educated public will also be more accepting of enhanced security measures.[109] That being said, communicating risk must be done carefully as not to overstate threats and increase fear.

Applicability of Lesson 4 to Cybersecurity

To strengthen the overall cyber defenses of the US, the general public must collectively adopt 'best practices' in terms of computer security.[110] Federally funded directives to encourage private citizens to update their virus protection software and safeguard their passwords must become ubiquitous, akin to the 'If You See Something, Say Something" anti-terrorism campaign. Current efforts at public awareness, like 'National Cybersecurity Awareness Month,' are not enough.[111]

Additionally, prominent policymakers must be careful in how they frame cyber threats. Exaggerating risk can unnecessarily amplify public apprehension and, if repeated frequently, can harbor public apathy. Specifically, statements by the heads of the CIA and DHS that used Pearl Harbor and 9/11 as metaphors to impending cyber dangers were misguided as they grossly misrepresented the capacity for malicious cyber attacks to kill thousands.[112] Rather than relying

---

[108] To clarify, this references a failed attempt by Naser Abdo in 2011 to attack Fort Hood, not the 2009 shooting that resulted in thirteen deaths. See: Eoyang, Mieke and Aki Peritz. "America's Goldilocks Moment in the Fight Against al Qaeda," Third Way: Digest. (February 2013). Pg. 5.

[109] Shemella, Paul. "Conclusion," *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011. Pg. 373.

[110] Lin, Herbert. "A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity," *Bulletin of the Atomic Scientists* 68, no. 75 (2012). Pg. 78.

[111] For more information on National Cybersecurity Awareness Month see: https://www.dhs.gov/national-cyber-security-awareness-month

[112] Ryan, Jason. "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," *ABCNews.* (February 11, 2011). Accessed April 20, 2014. <http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905&page=2>. & Reuters. "U.S. homeland chief: cyber 9/11 could happen 'imminently,'" *Reuters: Washington*. (January 24, 2013). Accessed April 20, 2014. <http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+reuters\technologyNews+(Reuters+Technology+News)>.

upon imprudent and alarmist comparisons, policymakers must be more tempered and realistic when quantifying the cyber threat.[113]

Lesson 5: Enlist the Private Sector

Private sector outreach is an important national security component to shore up security loopholes and bolster alertness to suspicious activities. Counterterrorism is no exception. Of particular concern, an amalgamation of biotechnology firms, pesticide companies, and nuclear energy consortiums control an assortment of sensitive materials that must be prevented from landing in the wrong hands. A strong private-public partnership can certify that security controls are up to date and that relationships are in place so that private organizations can report unusual behavior. In 2005, the FBI launched the Domestic Security Alliance Council as a mechanism to formalize information sharing with the private sector and investigate threats impacting American businesses.[114]

Applicability of Lesson 5 to Cybersecurity

As the 2010 White House National Security Strategy implicates, the government cannot confront the cybersecurity challenge alone; collaboration with the private sector is imperative.[115] Yet, despite frequent emphasis on information sharing and coordination, engagement with the private sector remains flawed.[116] While firms do not want to host malevolent actors on their computer networks, private enterprises lack sufficient incentives to publically identify their own

[113] Peritz, Aki. "Declaring War on Cyber Metaphors," *Huffington Post*. (March 9, 2011). Accessed April 20, 2014. <http://www.huffingtonpost.com/aki-peritz/declaring-war-on-cyber-me_b_833775.html>.
[114] For more information on the Domestic Security Alliance Council see: http://www.fbi.gov/about-us/partnerships_and_outreach/
[115] White House, United States of America. "National Security Strategy of the United States 2010." Pg. 28.
[116] Government Accountability Office, United States of America. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," Pg. 53.

vulnerabilities.[117] Further, private organizations on the whole do not allocate adequate resources to cybersecurity.[118] Government initiatives, like US-CERT, must be broadened to facilitate strategic communication and mend network breaches. More drastic measures to incentivize cybersecurity and foster trust should also be explored.

Lesson 6: Engage Internationally

Jihadist terrorism is an international phenomenon that requires an international response. An isolationist approach to counterterrorism would have significantly crippled the capacity of the US to identify, isolate, and eliminate extremist groups.[119] While definitional issues might prohibit a universal treaty on counterterrorism, many avenues remain to engage internationally.

First, the US has been able to wield its global hegemon to induce widespread commitment to legal measures that criminalize terrorist recruitment and fundraising. Second, the US has worked closely with its allies to bankroll and train their counterterrorism forces. Third, the US has colluded with regional organizations such as the European Union and INTERPOL to coordinate counterterrorism operations.[120] Finally, and arguably most importantly, the US has widened its cooperation with foreign states on matters of counterterrorism intelligence.[121] This emphasis on information sharing has proven fruitful. For instance, a 2010 al Qaeda plot to bomb two cargo planes with plastic explosives stored in seemingly innocuous ink cartridges was foiled by warnings from Saudi Arabian intelligence officials.[122] Further, thousands of terrorism

---

[117] Rosenzweig, Paul. "Cyber Deterrence Organization," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. Draft Post-Workshop Version (July, 2010). Pg. 13.
[118] Center for Strategic and International Studies: Threat Working Group. "Threats Posed by the Internet," Pg. 26.
[119] Art, Robert J. and Louise Richardson. *Democracy and Counterterrorism: Lessons from the Past*. Pg. 586.
[120] Graham, Kennedy. "The Security Council and Counterterrorism: Global and Regional Approaches to an Elusive Public Good," Pg. 52.
[121] Art, Robert J. and Louise Richardson. *Democracy and Counterterrorism: Lessons from the Past*. Pg. 586.
[122] Schmitt, Eric and Scott Shane. "Saudis Warned U.S. of Attack Before Parcel Bomb Plot," *New York Times.* (November 5, 2010). Accessed April 22, 2014.

suspects have been arrested due to cooperation between US intelligence agencies and their counterparts abroad.[123]

Applicability of Lesson 6 to Cybersecurity

The interconnectedness, speed, and boundless nature of cyberspace illustrate why cybersecurity must be treated as a global issue. However, a comprehensive internationally sanctioned treaty to regulate cyberspace seems unlikely in the current state of global affairs.[124] Nonetheless, opportunities for international engagement should not be ignored. The US must establish internationally recognized norms on the most valuable cybersecurity practices and encourage widespread adherence to legal standards that codify the investigation and prosecution of cyber attackers into national laws. The US can compel cybersecurity upgrades through economic incentives and by establishing benchmarks to participate in multilateral initiatives.[125] Moreover, the US must improve coordination and cooperation with foreign law enforcement and intelligence agencies in regards to cybersecurity.[126] Energetic engagement abroad can reduce the risks of miscalculation and collectively enhance security worldwide.[127]

Lesson 7: Ad Hoc Planning Can Produce Long Term Consequences

Not only was the US caught off guard by 9/11, but previous to the attacks there was a lack of strategic foresight to prepare an in-depth strategy to combat Jihadist terrorism. Specifically, formalized plans were not in place to detain enemy combatants captured in

---

<http://www.nytimes.com/2010/11/06/world/middleeast/06terror.html?_r=1&partner=rss&emc=rss&pagewanted=all>.

[123] Nacos, Brigitte. *Terrorism and Counterterrorism*. Pg. 251.

[124] Nye, Joseph S. "Cyber Power," Pg. 18.

[125] Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency," Pg. 20.

[126] As the GAO plainly states, "federal agencies had not demonstrated an ability to coordinate their international activities and project clear policies on a consistent basis." See: Government Accountability Office, United States of America. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," Pg. 79.

[127] Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency," Pg. 20.

Afghanistan or interrogate suspected terrorists withholding sensitive information. In retrospect, subsequent decisions to open an improvised detention facility at Guantánamo Bay and approve interrogation techniques that bordered the description of torture were rash and ineffectual.[128] Consequently, al Qaeda and its allies took advantage of these self defeating blunders to create emotive and effective propaganda tools.

Applicability of Lesson 7 to Cybersecurity

To support the decision making process in the event of a cyber attack, the US must first recognize the panoply of foreseeable cyber threats and assemble strategies to confront these hypothetical outcomes. Once a catalogue of potential cyber and non-cyber responses are developed, red-teaming and other war game simulations must be conducted to determine the risks and repercussions of the options on the table.[129] While it is impossible to prepare for every circumstance, the better security leaders are able to understand the consequences of their actions, the more likely overreaction can be avoided.

Conclusion

The Cold War has been over for a quarter of a century. What has emerged is a national security picture that is more complex, where security concerns are less straightforward and susceptibility to violence has become a global phenomenon.[130] While the US has spent the last

[128] Eoyang, Mieke and Aki Peritz. "America's Goldilocks Moment in the Fight Against al Qaeda," Pgs. 2-3.
[129] Rosenzweig, Paul. "Cyber Deterrence Organization," Pg. 24.
[130] United States Intelligence Community. "Protecting America,"*intelligence.gov*. (April 2014). Accessed April 7, 2014. <http://www.intelligence.gov/mission/protecting-america.html>.

decade combating the threat of terrorism, many US officials, including the head of the FBI, have gone on record to state that this menace will be eclipsed by cyber attacks in the near future.[131]

Although cyber threats often appear both frightening and misunderstood, it should not be forgotten that so was Jihadist terrorism following 9/11. In fact, the many parallels between the two concepts can place cybersecurity strategy into perspective. As the lessons learned from counterterrorism have demonstrated, cyber threats can be mitigated by designing strategies for limited deterrence, reorganizing government, and crisis management. Further, opportunities to engage the general public, the private sector, and the international community can also prove effective. That being said, the distinctions between the two concepts guarantee that cybersecurity will remain unique. The connectivity, anonymity, and increasing dependence on cyberspace will pose new security conundrums that must be reconciled.

Developing a robust cybersecurity strategy will not be easy. Mistakes will be made and successes will often go unreported. To combat cyber attackers, policymakers will have to draw upon all elements of American military, diplomatic, and cultural power to cultivate a strategy that unearths the delicate balance between protecting civil liberties while maintaining vigilance, promoting information sharing while not compromising sensitive intelligence, combating state perpetrators without definitive evidence of their guilt, and raising public awareness without inflating fear.

Cyber attacks are a nascent threat, but within the proper context, they are not an unprecedented threat. Accordingly, the enormous achievements in counterterrorism a decade after 9/11 bode well for the future conditions of cybersecurity.

---

[131] Johnson, Kevin. "FBI director: Cybercriminals are the new enemy," *USA Today*. (November 14, 2013). Accessed April 7, 2014. <http://www.usatoday.com/story/news/nation/2013/11/14/fbi-comey-cyber-attacks/3527405/>.

Work Cited

Allison, Graham. "Nuclear Deterrence in the Age of Nuclear Terrorism," *MIT: Technology Review*. (October 20, 2008). Accessed April 3, 2014. <http://www.hks.harvard.edu/news-events/news/news-archive/nuclear-deterrence-in-age-of-terrorism>.

Art, Robert J. and Louise Richardson. *Democracy and Counterterrorism: Lessons from the Past*. Washington: United States Institute of Peace Press, 2007.

Atherton, Kelsey D. "Cyber Attacks Are America's Top Security Threat. That's Better News Than It Sounds," *Popular Science*. (March 14, 2013). Accessed April 6, 2014. <http://www.popsci.com/technology/article/2013-03/cyber-attacks-were-named-top-security-threat-%E2%80%99s-better-news-it-sounds>.

Avlon, John. "Forty-Five Foiled Terror Plots Since 9/11," *Newsweek Magazine: The Daily Beast.* (September 8, 2011). Accessed April 18, 2014. <http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-foiled-in-last-10-years.html>.

Bloom, Mia. *Dying to Kill: The Allure of Suicide Terrorism*. New York: Columbia University Press, 2007.

Budinger, Zoe Baird and Jeffrey H. Smith. "Ten Years After 9/11: A Status Report on Information Sharing," *Senate Committee on Homeland Security & Governmental Affairs.* (October 12, 2011).

Carter, Shan, and Amanda Cox. "One 9/11 Tally: $3.3 Trillion," *New York Times*. (September 8, 2011). Accessed October 7, 2013. <http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0>.

Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency," *CSIS Commission on Cybersecurity for the 44th Presidency.* (December 2008).

Center for Strategic and International Studies: Threat Working Group. "Threats Posed by the Internet," *CSIS Commission on Cybersecurity for the 44th Presidency.* (December 2008).

Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record," *Senate Select Committee on Intelligence.* (March 12, 2013).

Clark, David D. and Susan Landau. "Untangling Attribution," *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Ed. National Research Council. Washington, DC: The National Academies Press (2010).

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2011. Pgs. 13-14.

Cline, Lawrence E. "Interagency Decision Making," *Fighting Back: What Governments Can Do About Terrorism.* Ed. Paul Shemella. Stanford: Stanford University Press, 2011.

Cronin, Audrey K. *Ending Terrorism*: *Lessons for Defeating al-Qaeda*. New York: Routledge, 2008.

Dahl, Erik J. "The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States," *Studies in Conflict & Terrorism* 34 no. 8 (2011).

Deen Thalif. “Politics: U.N. Member States Struggle to Define Terrorism,” *Inter Press Service News Agency*. (July 25, 2005). Accessed April 5, 2014. <http://www.ipsnews.net/2005/07/politics-un-member-states-struggle-to-define-terrorism/>.

Department of Defense, United States of America. “Department of Defense Strategy for Operating in Cyberspace,” (July 2011).

Demchak, Chris. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Ed. Derek S. Reveron. Washington: Georgetown University Press, 2012. Pg. 130.

Enders, Walter and Todd Sandler. *The Political Economy of Terrorism*. New York: Cambridge University Press, 2006.

Eoyang, Mieke and Aki Peritz. “America’s Goldilocks Moment in the Fight Against al Qaeda,” Third Way: Digest. (February 2013).

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security* 38 no. 2. (Fall 2013).

Government Accountability Office, United States of America. “Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented,” *GAO-13-187*. (February 2013).

Graham, Kennedy. “The Security Council and Counterterrorism: Global and Regional Approaches to an Elusive Public Good,” *Terrorism and Political Violence* 17, no. 1 (2005).

Harvey, Frank and Alex Wilner. "Counter-Coercion, the Power of Failure, and the Practical Limits of Deterring Terrorism," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowland, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack," *California Law Review*. (2012).

Hayden, Michael V. “The Future of Things Cyber,” *Strategic Studies Quarterly* 5, no. 1 (Spring 2011).

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

Howard, Russell D. and Nencheck, Margaret J. “The New Terrorism,” *Terrorism and Counterterrorism: Understanding the New Security Environment. (4th Edition)*. Eds. Bruce Hoffman and Russell D. Howard. York: McGraw-Hill, 2012.

Jackson, David. “Obama: Nuclear Terrorism is the ‘Single Biggest Threat’ to U.S.,” *USAToday* (April 11, 2010). Accessed April 2, 2014. <http://content.usatoday.com/communities/theoval/post/2010/04/obama-kicks-off-nuclear-summit-with-five-leader-meetings/1#.UzuRBPldWSp>.

Jenkins, Brian M. “The New Age of Terrorism,” *Homeland Security Handbook*. Ed. David G. Kamien. New York: McGraw-Hill, 2006.

Johnson, Kevin. “FBI director: Cybercriminals are the new enemy,” *USA Today*. (November 14, 2013). Accessed April 7, 2014. <http://www.usatoday.com/story/news/nation/2013/11/14/fbi-comey-cyber-attacks/3527405/>.

Kroenig, Matthew and Barry Pavel. “How to Deter Terrorism,” *Center for Strategic and International Studies: The Washington Quarterly* 35, no. 2 (Spring 2012).

Lewis, James A. “Cross-Domain Deterrence and Credible Threats,” *Center for Strategic and International Studies* (July 2010).

Lewis, James A. “The Economic Impact of Cybercrime and Cyber Espionage,” *Center for Strategic and International Studies*. (2013).

Lin, Herbert. “A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity,” *Bulletin of the Atomic Scientists* 68, no. 75 (2012).

Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploitation," *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Ed. Derek S. Reveron. Washington: Georgetown University Press, 2012.

Nacos, Brigitte. *Terrorism and Counterterrorism*. Boston: Pearson Longman, 2012.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2012). *Global Terrorism Database*. Accessed March 23, 2014. <http://www.start.umd.edu/gtd>.

Nye, Joseph S. “Cyber Power,” *Belfer Center for Science and International Affairs*. (May 2010).

Nye, Joseph S. “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly 5, no. 4 (Winter 2011).

MacAskill, Ewen, and Jonathan Watts. “US intelligence spending has doubled since 9/11, top secret budget reveals,” *The Guardian*. (August 29, 2013). Accessed April 3, 2014. <http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget>.

Mandiant Intelligence. “APT1: Exposing One of China’s Cyber Espionage Units,” *Mandiant*. (2013).

Martel, William. “Critical Infrastructure,” *DHP-P249: Foundations of International Cybersecurity*. Fletcher School of Law and Diplomacy, Tufts University, Medford, MA. (November 21, 2013).

Martel, William. “Understanding Cyber Threats,” *DHP-P249: Foundations of International Cybersecurity*. Fletcher School of Law and Diplomacy, Tufts University, Medford, MA. (September 9, 2013).

McAfee. “Virtually Here: The Age of Cyber Warfare,” McAfee Virtual Criminology Report (2009).

Mockaitis, Thomas R. “Terrorism, Insurgency, and Organized Crime,” *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011.

Pape, Robert A. “The Strategic Logic of Suicide Terrorism,” *American Political Science Review*, no. 97. (2003).

Peritz, Aki. “Declaring War on Cyber Metaphors,” *Huffington Post*. (March 9, 2011). Accessed April 20, 2014. <http://www.huffingtonpost.com/aki-peritz/declaring-war-on-cyber-me_b_833775.html>.

Public Broadcasting Service. “Plague War: Interview James Woolsey,” *PBS Frontline*. Accessed March 3, 2014. <http://www.pbs.org/wgbh/pages/frontline/shows/plague/interviews/woolsey.html>.

Rapoport, David C. "The Four Waves of Modern Terrorism," *Attacking Terrorism: Elements of a Grand Strategy* Eds. Audrey K. Cronin and James M. Ludis. Washington: Georgetown University Press, 2004.

Reuters. “U.S. homeland chief: cyber 9/11 could happen ‘imminently,’” *Reuters: Washington*. (January 24, 2013). Accessed April 20, 2014. <http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+reuters\technologyNews+(Reuters+Technology+News)>.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.

Rosenzweig, Paul. “Cyber Deterrence Organization,” *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. Draft Post-Workshop Version (July, 2010).

Ryan, Jason. “CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor,” *ABCNews.* (February 11, 2011). Accessed April 20, 2014. <http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905&page=2>.

Schwartz, Stephen I., and Deepti Choubey. “Nuclear Security Spending: Assessing Costs, Examining Priorities,” *Carnegie Endowment for International Peace*. (2009).

Schmitt, Eric and Scott Shane. “Saudis Warned U.S. of Attack Before Parcel Bomb Plot,” *New York Times.* (November 5, 2010). Accessed April 22, 2014. <http://www.nytimes.com/2010/11/06/world/middleeast/06terror.html?_r=1&partner=rss&emc=rss&pagewanted=all>.

Shemella, Paul. “Conclusion,” *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011.

Shemella, Paul. “Tools for Strategies for Combating Terrorism,” *Fighting Back: What Governments Can Do About Terrorism*. Ed. Paul Shemella. Stanford: Stanford University Press, 2011.

Singer, Peter W. “The Cyber Terror Bogeyman,” Brookings. (November 2012). Accessed April 7, 2014. <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer>.

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Stanglin, Doug. “Report: Chinese Hackers Breach Top Weapons Designs,” USA Today. (May 18, 2013). Accessed April 12, 2014.

<http://www.usatoday.com/story/news/nation/2013/05/28/chinese-hackers-post-designs-breached-compromised/2364969/>.

Stein, Janice G. "Deterring Terrorism, Not Terrorists," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012.

Tobey, William, and Bunn, Matthew. "Chemical and Biological Weapons," *IGA-232: Controlling the World's Most Dangerous Weapons*. Harvard Kennedy School, Harvard University, Cambridge, MA. (October 3, 2013).

Trager, Robert F. and Dessislava P. Zagorcheva. "Deterring Terrorism: It Can Be Done." *International Security* 30 no. 3 (Winter 2005/06).

United States Government Accountability Office. "High-Risk Series," *Report to Congressional Committees*. (February 2013).

United States Intelligence Community. "Protecting America,"*intelligence.gov*. (April 2014). Accessed April 7, 2014. <http://www.intelligence.gov/mission/protecting-america.html>.

Waldo, James. "Course Description," *IGA-236M*: *Technology, Security, and Conflict in the Cyber Age*. Harvard Kennedy School, Harvard University, Cambridge, MA. (January 2014). Accessed January 15, 2014. <http://www.hks.harvard.edu/degrees/teaching-courses/course-listing/iga-236m>.

Wenger, Andreas and Alex Wilner. "Deterring Terrorism: Moving Forward," *Deterring Terrorism: Theory and Practice* Eds. Andreas Wenger and Alex Wilner. Stanford: Stanford University Press, 2012. Pg. 322.

White House, United States of America. "National Security Strategy of the United States 2010," (May 2010).

Wilson, Scott and Jon Cohen. "Poll Finds Broad Support for Obama's Counterterrorism Policies," *Washington Post.* (February 8, 2012). Accessed April 18, 2014. <http://www.washingtonpost.com/politics/poll-finds-broad-support-for-obamas-counterterrorism-policies/2012/02/07/gIQAFrSEyQ_story.html>.

Zenko, Micah. "A Nuclear Site Is Breached," *Washington Post*. (December 20, 2007). Accessed April 24, 2014. <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/19/AR2007121901857.html>.