The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking

Omry Haizler

This article will touch upon two main components of the United States' cybersphere and cyber warfare. First, it will review three cyber incidents during different time periods, as the US infrastructure, mechanisms, and policies were gradually evolving. It will analyze the conceptual, operational, and legislative evolution that led to the current decision-making paradigm and institutional structure of the US cybersphere. Secondly, the paper will examine the procedures and policies of the Intelligence Community (IC), and the US cyber operational structure. It will review the missions and background of the IC and its responsibilities before, during, and after a cyberattack, and will touch upon the IC's organizational architecture. The paper will also briefly review the current cyber threats in the United States and will elaborate on some of the fundamental strategies and policies that it uses to provide a suitable response. Lastly, it analyzes the cybersphere's macro-level, addressing the data coordination of the IC's agencies, as well as the federal, state, and private sector institutions during a cyber crisis.

Keywords: Moonlight Maze, Morris Worm, Stuxnet, cyberattacks, United States intelligence community, cyber crisis, cyber threats, internet governance, cyber policy, cyber strategy

Omry Haizler is a former IDF Officer and a Prime Minister's Office operative. He holds an MPA from Columbia University's School of International and Public Affairs (SIPA). He currently teaches at Columbia's School of Continuing Education.

History of Cyber Warfare

There are three historical stages of the evolution of cyber warfare: 1) the realization phase during the early era of the internet; 2) the takeoff phase during the interim period of pre- and post- 9/11 in which attacks were still mainly of an information-gathering nature; and 3) the modern militarization phase, during which cyber warfare may cause similar damage to US strategic capabilities and critical infrastructure as a kinetic attack on a colossal level. Figure 1 below describes these stages:[1]

Stages	Realization	Takeoff	Militarization
Timeframe	1980	1998–2003	2003–present
Dynamics	Attackers have advantage over defenders	Attackers have advantage over defenders	Attackers have advantage over defenders
Who Has Capabilities?	United States and few other superpowers	United States and Russia with many small actors	United States, Russia, China, and many more actors with substantial capabilities
Adversaries	Hackers	Hacktivists, patriot hackers, viruses, and worms	Neo-Hacktivists, espionage agents, malware, national militaries, spies, and their proxies, hacktivists
Major Incidents	Cuckoos Egg (1986), Morris Worm (1988), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot Hackers	Titan Rain, Estonia, Georgia, Buckshot Yankee Stuxnet
US Doctrine	Information warfare	Information operations	Cyber warfare

Figure 1: Phases of Cyber Conflict History

Attacks as Catalyzers for Institutional Evolution

Each of the above periods characterizes a fundamentally different doctrine, both with respect to technological progression and type of threats, and to the administration's cyber policies at each given time. Certain past attacks embodied future cyber challenges, serving as warning signs to institutions' vulnerabilities and lack of security. As society's dependency on technology

increased, the possible ramifications of inefficient security in a specific breach also increased.

1. Realization—the Morris Worm

This cyber incident acted as the first wake-up call to the American Intelligence Community (IC), policymakers, and academics. While it was not the first cyberattack on US computer systems—the 1986 Cuckoo's Egg hack involving the Soviet KGB was the first significant cyber espionage attack—it is widely considered the first large-scale attack, both in terms of the quick phase of events, its scale, and its implications. Launched as a prank from a lab at Cornell University, the Morris Worm was designed to infect as many machines as possible without being detected; the worm crashed 6000 computers—roughly 10 percent of the internet in 1988.[2] The US Government Accountability Office assessed the damage at $100,000–$10,000,000, illustrating the difficulty of assessing cyberattack damage, a problem prevalent even today.[3] Despite the severe ramifications, the incident provided an important warning to the IC, highlighting the potential dangers of highly connected computer networks and the need for institutionalized defensible capabilities and structures in the cybersphere.

The Morris Worm acted as a catalyzer for the first steps towards a more regulated cyberspace and led to dramatic changes, both conceptually and operationally:

Paradigm Shift: At the time of the incident, the internet was taking its first substantial steps and was considered a "friendly place," where everyone knows everyone. The Morris Worm made it clear that some people in cyberspace did not have the best interests in mind; the incident was the first time where cyber innovation shifted from focusing solely on interconnectivity to security concerns.

Operations: Established after the Morris Worm incident by the Defense Advanced Research Projects Agency (DARPA) at Carnegie Mellon University, the Computer Emergency Response Team (CERT) demonstrated the shift from ad hoc solutions to professional teams, which were trained and equipped to coordinate events and provide assessments and solutions to a given cyberattack.[4]

Regulations: Along with the conceptual shift in cybersecurity, Congress passed several laws in the years following the Morris Worm incident, including

the Electronic Communications Privacy Act of 1986 and the Computer Security Act of 1987 to ensure privacy in cyber domains through legal protections.[5] Additionally, Robert Tappan Morris who created the Morris Worm, was the first person to be convicted under the new Computer Fraud and Abuse Act of 1986.[6]

2. Takeoff—The Moonlight Maze

In 1998, US officials accidentally discovered a pattern of sustained probing of the Pentagon's computer systems, private universities, NASA, Energy Department, and research labs. Soon they learned that the probing had occurred continually for nearly two years. Thousands of unclassified, yet sensitive documents relating to technologies with military applications had been examined or stolen, including maps of military installations, troop configurations, and military hardware designs.[7] Although the Defense Department traced the trail back to a mainframe computer in the former Soviet Union, the sponsor of the attacks remains unknown. Russia denied any involvement, and the suspicions have never been conclusively proven.[8]

Moonlight Maze is widely considered the first large-scale cyberespionage attack by a well-funded and well-organized state actor. The attack was well planned as the attackers left "backdoors" to enable hackers to penetrate the system at different times, left few traces, and continued for a long time without detection.[9] Moonlight Maze highlighted the increasing role of state authorities in generating, sponsoring, or, at least, passively tolerating sophisticated and far-reaching espionage incidents. Moreover, it stressed the vulnerabilities of the infosphere, in which adversaries could not only cause disruption of service, but also could exploit sensitive information. It emphasized the crucial need for firewalls and encryptions and, above all, the difficulties of identifying and attributing an attack to a specific adversary. Moonlight Maze was an important progression in cyber warfare and cybersecurity due to its implications on future conflicts.[10] It pointed out the future shift in the modern battlefield from a kinetic war—in which enemies have names and physical locations, and in which attacks can be witnessed and assessed—into an asymmetrical warfare with offensive cyber operations, where attacks might be invisible, adversaries are unknown, and damage is hard to quantify. The incident led to dramatic shifts in the US administration's approach to cybersecurity.

Paradigm Shift: The awareness of terrorist threats and support of counterterrorism initiatives post 9/11 among policymakers were limited. The Moonlight Maze incident caused a rethinking of the US cyber defense strategy, cyber warfare attribution, cyber deterrence, and the current defense of sensitive, non-encrypted networks such as NIPERnet (Non-Secure Internet Protocol Router Network, the Pentagon's non-classified network). For the first time, political and constitutional questions were raised about security, privacy and notions of active monitoring and possible exposure to transnational threats.[11] Moonlight Maze caused the US agencies and government to realize that clear policies and strategies were needed for asymmetric warfare, the field of future intelligence gathering and espionage, and the technological implications they entail.

Legislative Acts: The Presidential Decision Directive 63 (PDD 63), regarding critical infrastructure protection, was, in part, the result of Moonlight Maze. This was a seminal policy document setting forth roles, responsibilities, and objectives for protecting the nation's utility, transportation, financial, and other essential infrastructure.[12] The PDD 63 led to two significant strategic implications. One was the creation of the National Incident Protection Center (NIPC), an inter-agency body with the power to safeguard the nation's civilian and governmental critical infrastructure from computer-based attacks.[13] The second was the creation of the Joint Task Force Computer Network Defense (JTF-CND), a body entrusted with taking the lead in coordinating a response to national cyberattacks and centralizing the defense of military networks.[14]

Operational: Led by the Department of Defense (DoD), incident response mechanisms were built and reporting institutions were established. Military reports would be handled at the local level through Network Operations and Security Centers (NOSCs) under the Defense Information Systems Agency (DISA). Handled as command and control mechanisms, regional CERTs are at the frontline of assessing impact on an individual and regional level. JTF-Computer Network Operations (CNO) and the DISA Global Network Operations and Security Center (GNOSC) are additional factors that expedite channeling of information.

3. Militarization—Stuxnet

The Stuxnet attack is considered one of the most sophisticated malware attacks publicly recorded. Although unverified, many experts argue that only

a nation-state could have created and launched the attack and many media outlets suggested it was a joint Israeli-American operation.[15] Considered as one most impactful cyberattacks involving sovereign countries, the malware damaged Iran's centrifuges and delayed its uranium enrichment efforts. Once inside the network, it used a variety of mechanisms to propagate to other machines within that network and gain privileges as soon as it had infected those machines. These mechanisms included both known and patched vulnerabilities, as well as four vulnerabilities that were unknown and unpatched when the worm was released (aka "zero-day" exploits).[16] While the international community remains unsure of the source and exact purpose of the virus, the incident raised awareness of networks' vulnerabilities.[17]

Identified in 2010, Stuxnet's impact and unclear origin highlight the difficulty in noticing an attack and suggest that at a nation level, it is impossible to fully defend all vital resources.[18] Therefore, it became crucial to understand the dynamics of battle-like situations in modern-age cyber warfare, in which even a colossal attack does not necessarily have an attributed attacker or a trace of any attack at all. This means that in modern non-kinetic battle fields, policymakers realize the effect of an attack (from denial of service to the destruction of a nation's critical infrastructures) without having a smoking gun or any legal or political tool to fight with. This phenomenon requires legislators and authorities to start formulating response options and detailed protocols now, rather than trying to develop ad hoc options later during a crisis.

The cyber warfare of post-2013 shifted the counterattack approach from an operational level[19] to a strategic-diplomatic one, where policy, international laws, internet governance, and agreements play a significant part in the overly-breached cyber environment. Three substantial internet governance agreements and collaborative efforts have taken place on a multinational level:

a. The United States-China Cyber Agreement: This agreement ensures that neither government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[20] While it is only a basic agreement that does not ensure a safe cyber environment between the two states, its importance stems from the ability to build upon it in future years and act as a gesture of goodwill.

b. The United Nations' World Summit on the Information Society process (WSIS+10): This summit renewed the Internet Governance Forum (IGF), a venue where member states, civil society, and the private sector debate internet policy, cybersecurity, surveillance, intellectual property, and copyright. Nations have strengthened diplomatic, open channels regarding cyber policy, reiterating their commitment to bridge the digital divide and improve access to information and communications technologies (ICTs), by recognizing the WSIS+10 document.[21]
c. The Safe Harbor Agreement: This agreement was signed between the US Department of Commerce and the European Union and regulates the way that US companies can export and handle the personal data of European citizens for the first time.[22]

US Cybersphere Operational Structure

Due to the complexity of coordination, fragmented responsibilities, and overlapping oversight, the multi-faceted cyberspace is saturated with military, think tanks, academia, private sector and government institutions, branches, and offices. At the national level is the Intelligence Community, which has both defensive and offensive capabilities and has the ultimate responsibility in addressing and monitoring modern cyber warfare. Whether it is an attack against military or government offices, or a significant attack against a private institution or critical infrastructure, the IC holds the operational responsibility for all aspects of the United States' cybersphere.

Established in 1981, the IC is a federation of seventeen US government agencies that work separately and together to conduct intelligence activities.[23] Member organizations include intelligence agencies, military intelligence, civilian intelligence, and analysis offices within federal executive departments, all headed by the director of National Intelligence who reports directly to the president.[24] While most of the associated agencies are offices or bureaus within federal executive departments, nine of them operate under the Department of Defense, and together spend 85 percent of the total US intelligence funds.

Traditional intelligence gathering relies on a counterterrorism's intelligence cycle, which includes human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). While all disciplines are still needed to form an inclusive intelligence assessment, cyber and cryptology capabilities have

gained more recognition as the need for investment in human capital and resources rises and as the world's reliance on technology increases.

The IC focuses on three aspects of maintaining cybersecurity: organization, detection, and deterrence. Various organizations within the IC pursue different tasks.[25] The Office of the Director of National Intelligence (ODNI) heads a task force coordinating efforts to identify sources of future cyberattacks. The Department of Homeland Security (DHS) leads the protection of government computer systems. The DoD devises strategies for potential cyber counterattacks. The National Security Agency (NSA) monitors, detects, reports, and responds to cyber threats. The Federal Bureau of Investigation (FBI) leads national efforts to investigate and prosecute cybercrimes. Many other cyber organizations outside the IC's umbrella address cyber threats, the most prominent of which is the US Cyber Command (USCYBERCOM). During a crisis, the IC assesses intelligence within its seventeen agencies, and then formulates overall intelligence recommendations by the ODNI.

In 2015, James Clapper, the director of National Intelligence who oversees the IC and is responsible for the complex coordination between all the arms of the IC, released a risk-assessment in which cyber threats top the list of global threats,[26] ahead of physical terrorism for the first time since the attacks of September 11, 2001. Although cyberattacks against the United States are constant and on the rise,[27] Clapper referred to the possibility of a "cyber Armageddon" (aka "cyber Pearl Harbor," or "cyber 9/11") [28] as currently remote. Rather than a "cyber Armageddon" scenario that debilitates the entire US infrastructure, the IC predicts a different challenge. It foresees an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.[29] The global proliferation of malicious code increases the risk to American networks, sensitive infrastructure, and data. While a disruptive or destructive cyber operation against a private corporation, an industrial control system, or a defense system requires a potential adversary to have a significant level of expertise to execute it, it does not necessitate state-level financial abilities or world-class operational talent. A given actor, whether a nation-state or a non-state group, can purchase malware, spyware, zero-days, and other capabilities on the black market, and can pay experts to search for vulnerabilities and develop exploits. In a global environment brimming with adversaries, as well as a lack of international cyber laws and

clear regulations, these threats have created a dangerous and uncontrolled market, which serves multiple actors within the international system.[30]

Despite the increase in cyber activity by non-state actors, top US intelligence officials still believe that state actors are the greatest threat in cyberspace to US interests. The IC identifies several potential actors who may cause a cyber crisis, including nation-states with highly sophisticated cyber programs, such as Russia or China;[31] nations with lesser technical capabilities, but possibly more disruptive intent, such as Iran or North Korea; non-state actors with accessibility to significant resources and motivation to create cyber chaos; and profit-motivated criminals and ideologically-motivated hackers or extremists.

The various possible targets include:

a. The Private sector: This sector is identified not only as a victim of cyberattacks, but also as a participant in investigations and attribution. Given the importance of financial institutions (e.g., Goldman Sachs) to the economy in their dependency on technology, this sector is an important field to defend in case of a serious attack.[32]
b. Critical infrastructure: The critical infrastructure—the physical and virtual assets, systems, and networks vital to national and economic security, health, and safety—is vulnerable to cyberattacks by foreign governments, criminal entities, and lone actors. A large-scale attack could temporarily halt the supply of water, electricity, and gas; hinder transportation and communications; and cripple financial institutions.[33]
c. Government: Penetrating the US national decision-making apparatus and Intelligence Community will remain primary objectives for foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US research institutions dealing with defense, energy, finance, dual-use technology, and other areas will be a persistent threat to US interests.[34]
d. Military and government agencies: These are the front line of both defense and offense, as its infrastructure must defend the entire nation as well as its own resources in case of a full-scale cyber conflict. IC assumes that in a cyber crisis, this "contact-line" will be attacked and damaged.

The Intelligence Community Policies

The IC conducts a variety of intelligence operations on a daily basis. The United States is under constant cyberattack from both state and non-state

actors. On the national intelligence level, being under cyberattack means not only a defensive effort, but also designing various operational options for retaliation. Given its size, the IC interacts and collaborates with agencies on the operational level (military, DoD, DHS) and the state and federal level (private sector on a large scale, Department of State, White House).

The IC's strategic preparation goals[35] include:

a. Building and maintaining ready forces and capabilities to conduct cyberspace operations;
b. Defending its own information network, securing data, and mitigating risks to missions;
c. Preparing to defend US homeland and US vital interests against disruptive or destructive cyberattacks of significant consequence;
d. Building and maintaining viable cyber options and planning to use those options to control conflict escalation and to actively extract information to prepare "target banks";
e. Building and maintaining robust international alliances and partnerships to deter shared threats and increase international security and stability.

IC's policy of cyberattack response is as follows:

a. Identifying attacks: As part of the modern cyber battlefield, sophisticated attackers will attempt to conceal the attack. Just as in a conventional conflict, intelligence is needed to prepare the battle ground and accurately assess the probability of success and utility for any kind of operation.[36]
b. Informing: Although the IC has significant offensive abilities, its main role is to assess, inform, and report. The IC must inform the operational arms it collaborates with and the State Department. That is, under attack, the IC's success is measured by the precautions it gave prior to the attack and by its responsiveness, communication, and guidance during the attack.
c. Providing options: The IC must provide a set of options to decision makers and enable strategic flexibility by providing valuable information. The IC administers guidance during attack and provides strategic-operational and political leeway with its recommendations and intelligence assessment.
d. Damage Assessment: Unlike the conventional battlefield, a cyberattack may be hard to detect at times, even if it is a large-scale attack. The IC must assess the damage caused so that it can provide policymakers with the ability to retaliate in a measurable manner. This does not necessarily require operational efforts during an attack, but rather assessment,

coordination, and information-sharing with other offices so that there is an efficient flow of information.

Multidimensional Cyber Response

The IC's role overlaps in many ways with different institutions, governmental departments, and military units, many of which is out of its jurisdiction. While it does not singularly have responsibility for cyber response at the national or state level, the IC demands a complex chain of information flow and hierarchy. Other institutions that provide cyber responses are:

a. Department of Homeland Security: As part of its role to protect the United States' territories and respond to terrorist attacks, man-made accidents, and natural disasters, the DHS is in charge of Coast Guard Intelligence (CGI) and the Office of Intelligence and Analysis (I&A). The latter is responsible for managing the collection, analysis, and fusion of intelligence. The Office of I&A disseminates intelligence throughout the DHS and to the other members of the IC community, and is the first responder at the state, local, and tribal levels.[37] The ODNI is responsible for an efficient information flow between the rest of the intelligence community and the DHS in order to create synergy of information during a cyberattack.
b. Department of Defense (DoD): Considered the focal point for the intelligence community's operational source and leading nine of its agencies, including the NSA, the DoD is the ODNI's main source of cyber intelligence. As such, the Director of National Intelligence (DNI) often reports to decision makers and the White House based on the intelligence received from the DoD. In addition, the NSA and CYBERCOM, led by Admiral Michael Rogers, and the DNI, work closely together during an attack. It is necessary that the operational data stream be processed through the ODNI and received as policy recommendations at the federal level.
c. State Department: The government is dependent on the IC during a cyber crisis. Unlike in conventional conflicts, it is safe to assume that decision makers often do not know what has happened and do not know the origin of an attack in a cyber crisis scenario. It is up to the IC to provide an intelligence assessment in a timely manner and to pass on the data. Small centers that are trusted to evaluate and coordinate serve as liaisons between state institutions and the cyber intelligence field, such as the National Cybersecurity and Communications Integration Center

(NCCIC), the United States Computer Emergency Readiness Team (US-CERT), and the Cyber Threat Intelligence Integration Center (CTIIC). Stationed in the Office of the Director of National Intelligence, the latter will mirror the efforts and assessments for counterterrorism information sharing during cyberattacks.[38]

d. Private Sector: Infrastructure cyber breaches and attacks have been defined as the number one threat of the United States in 2015 by the DNI. The Information Sharing and Analysis Center (ISAC) is the main actor in overseeing private sector cyber threats, as ISAC assists federal and local governments with information pertaining to cyber threats. Private sector cyber crises may affect national interests (e.g., the Sony incident), and thus, in collaboration with DHS, Department of State, and the FBI, the private sector demands that an operational intelligence approach be taken at the national level.

Conclusions

The history of cyber warfare poses many lessons, and may indicate the progression and direction of the cybersphere, as well as the comprehensive attention required by the field at all levels. Cyber warfare's natural evolution is an important tool to assess mistakes and project the future of the infosphere, privacy regulations, cyber espionage, and cybersecurity needs. Policymakers are addressing the cybersphere today more seriously than ever before, and institutions at all levels are directing substantial resources to address cyber threats. Intelligence agencies constantly are perfecting their defensive and offensive cyber capabilities. Private institutions, especially in the fields of medicine, finance, critical infrastructure, and energy, in addition to data-driven corporations, allocate more resources and human power to data protection and cybersecurity than ever before. Lastly, the American government is aware of the risks to its own networks, and while breaches are more common than ever, investments to nurture a more defensible cyber space are at an all-time peak.

There are several fundamental policy realizations at the international level. Most policymakers and legislators do not have a comprehensive capacity to address international cyberattacks. For example, there is not an all-inclusive definition for "acts of war" in the non-kinetic sphere, and the existing definitions are unclear and not shared and agreed upon at the international

level. Moreover, retaliation mechanisms for a financial cyber crisis are not in place, preventing nation-states from attributing large-scale attacks to specific attackers and allowing other actors to avoid accountability. International collaboration at all levels, especially in the financial, diplomatic, and the judiciary fronts, are in need, as a lack of collaboration may prevent a stable foundation upon which accountability mechanisms can be formed. Despite the growing multisector investments in cybersecurity, more sophisticated attacks have taken place in the last three years than previously. Therefore, it appears that only multinational, substantial, and binding cyber agreements and progressive internet governance legislation will allow for a substantially safer cybersphere.

On the security front, the IC forms narrative and operational recommendations to policymakers, due to its coordination ability and vast jurisdiction. The biggest challenge during a cyberattack is to identify and connect the different dots for generating a responsible and measurable response. Without a body like the IC, the abundance of data would get lost in a maze of information. Just like in a kinetic battlefield, the defense line will eventually be penetrated, given a persistent attacker. Unlike the classic battlefield, however, a given cyberattack may not be seen, attribution may not be plausible, and the impact may not be noticeable. Cyber terrorism may become a growing concern with time and may require greater international intelligence collaborations than ever. Internal national intelligence security agencies may be forced to change disciplines and shift their strategic attention. It is thus plausible to project that in the future, nuclear weapons will no longer be the ultimate and greatest threat.

Notes

1 Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

2 Ted Eisenberg et al., "The Cornell Commission: On Morris and the Worm," *Communications of the ACM* 32, no. 6 (1989): 706–709, http://portal.acm.org/citation.cfm?id=63526.63530.

3 During the Morris appeal process, the US Court of Appeals estimated the cost of removing the virus from each installation was in the range of $200–$53,000. Possibly based on these numbers, Harvard spokesman Clifford Stoll estimated the total economic impact was between $100,000 to $10,000,000.

4 Eisenberg et al, "The Cornell Commission: On Morris and the Worm."

5 Michael Rustad and Diane D'Angelo, "The Path of Internet Law: An Annotated Guide to Legal Landmarks," in *Duke Law & Technology Review 2011*, ed. Beatrice Hahn (Durham: Duke University School of Law, 2011).
6 United States v. Morris, (2d Cir. 1991), upholding the conviction of a computer science graduate student under the Computer Fraud and Abuse Act.
7 *Hearing before Committee on Governmental Affairs, US Senate* (March 2, 2000) (testimony of James Adams, Chief Executive Officer Infrastructure Defense, Inc).
8 Adam Elkus, "Moonlight Maze" in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*
9 Ryan Richard Gelinas, "Cyberdeterrence and the Problem of Attribution," (master's thesis, Georgetown University, 2010), http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf.
10 Marcia McGowan, "15 Years After Presidential Decision Directive" (PPD) 63," *Booz Allen*, May 22, 2013, http://www.boozallen.com/content/boozallen/en_US/media-center/company-news/2013/05/15-years-after-pdd63-blog-post.html.
11 "Moonlight Maze," *Frontline*, PBS, April 24, 2003, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.
12 Office of the Press Secretary, "Fact Sheet: Protecting America's Critical Infrastructures PDD 63," May 22, 1998, http://fas.org/irp/offdocs/pdd-63.htm.
13 Ibid.
14 Ibid.
15 Kim Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon* (New York: Crown Publishing, 2014).
16 Ralph Langner, "Stuxnet's Secret Twin: The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized," *Foreign Policy*, November 21, 2013, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.
17 Ibid.
18 Irving Lachow, "The Stuxnet enigma: Implications for the future of cybersecurity," *Georgetown Journal of International Affairs Special Issue: Cybersecurity* (2011): 118–126.
19 For example, creating more institutions that monitor, coordinate, regulate, assess, defend, and attack.
20 Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement," *Council on Foreign Relations*, January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.
21 Guest Blogger, "The Top Five Cyber Policy Developments of 2015: The WSIS+10 Review," *Net Politics* (blog), Council on Foreign Relations, December 22, 2015 http://blogs.cfr.org/cyber/2015/12/22/the-top-five-cyber-policy-issues-of-2015-the-wsis10-review/.
22 Federal Trade Commission "US-EU Safe Harbor Framework," July 25, 2016, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

23 Executive Order No.12333, United States Intelligence Activities (December 4, 1981), Central Intelligence Agency, https://www.cia.gov/about-cia/eo12333.html.
24 "The Organizational Arrangements for the Intelligence Community," *Federation of American Scientists*, February 23, 1996, http://fas.org/irp/offdocs/int009.html.
25 Eric Rosenbach and Aki J. Peritz, "Cyber Security and the Intelligence Community," in *Confrontation or Collaboration? Congress and the Intelligence Community*, ed. Eric Rosenbach (Harvard Kennedy School: Belfer Center for Science and International Affairs, 2009).
26 *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Security Committee*, (February 26, 2015) (statement of James R. Clapper, Director of National Intelligence). http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_ FINAL.pdf.
27 "Norse Intelligence Platform," Norse, http://map.norsecorp.com.
28 Kristen Eichensehr, "Cybersecurity in the Intelligence Community's 2015 Worldwide Threat Assessment," *JustSecurity*, March 6, 2015, https://www.justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/.
29 Ibid.
30 Department of Defense, "The DoD Cyber Strategy," April 17, 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_ DoD_Cyber_ Strategy_for_web.pdf.
31 Mark Pomerleau, "IC leaders: Future cyber attacks will do real damage," *Defense Systems*, September 11, 2015, https://defensesystems.com/articles/2015/09/11/ic-leaders-map-out-nation-state-cyber-threats.aspx.
32 Ibid.
33 Andrew Meola, "Cyber attacks against our critical infrastructure are likely to increase," *Business Insider*, May 26, 2016, http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5.
34 Ibid.
35 Ibid.
36 Aaron Brantly, "Defining the role of intelligence in cyber," in *Understanding the Intelligence Cycle* ed. Mark Phythian (London and New York, England: Routledge, 2013).
37 Ibid.
38 Richard Bejtlich, "What are the prospects for the Cyber Threat Intelligence Integration Center?" *Brookings*, February 19, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/19-cyber-security-center-bejlich.