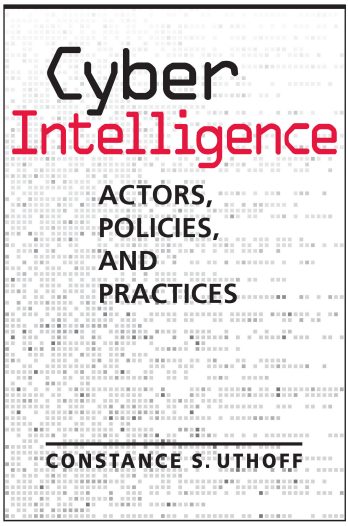
EXCERPTED FROM

Cyber Intelligence: Actors, Policies, and Practices



Constance S. Uthoff

ISBNs: 978-1-62637-965-7 hc
978-1-62637-966-4 pb

LYNNE RIENNER PUBLISHERS

1800 30th Street, Suite 314
Boulder, CO 80301 USA
telephone 303.444.6684
fax 303.444.0824

Contents

1

The Cyber Domain

Over the past decade, there has been a dramatic increase in online criminal activity. The world has witnessed not only the emergence of cyber operations that are a part of or related to international conflict, but also the pervasiveness of cyber attacks against critical infrastructure and the rise of ransomware. With each passing year, despite consistent warnings from US leaders, cyber incidents have increased in frequency, scope, and impact at such a scale that they challenge the future of US prosperity. They are a continuous threat to global, national, and economic security, and, as a result, are a growing cause for concern.

The potential for harm is so dire that, according to the 2018 National Cyber Strategy (NCS), the United States is "vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing." The nation's "dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk."[1]

This fragile state of national cybersecurity became starkly evident during the final month of 2020, when the cybersecurity company FireEye disclosed that it had been breached and its security tools stolen. A few days later, FireEye revealed that the intrusion, a supply chain breach involving the SolarWinds company, was much more significant than initially thought, with targets ranging from sensitive government agencies to high-profile information technology (IT) and Fortune 500

companies. Considered by the *New York Times* as one of "the greatest intelligence failures of modern times," and by Senator Chris Coons "as destructive and broad scale an engagement with our military systems, our intelligence systems as has happened in my lifetime," the attack, suspected to be tied to Russian intelligence, involved the compromise of a software upgrade from SolarWinds, a company that provides network-management systems to more than 300,000 clients.[2] Approximately 18,000 SolarWinds clients downloaded the infected updates, providing backdoor access to the hackers, who were then able to infiltrate, undetected for nine months, sensitive government and private company networks of their choosing. According to Tom Bossert, who served as the director of homeland security during the Trump administration, "While the Russians did not have the time to gain complete control over every network they hacked, they most certainly did gain it over hundreds of them. It will take years to know for certain which networks the Russians control and which ones they just occupy."[3] This is extremely concerning considering that the hackers had access to the US Treasury Department, the US Department of Commerce's National Telecommunications and Information Administration, the US Department of Health's National Institutes of Health (NIH), the Cybersecurity and Infrastructure Agency (CISA), the Department of Homeland Security (DHS), the US Department of State, many Fortune 500 companies, the top ten telecommunication companies, local and state governments, accounting firms, universities, colleges, and the Los Alamos National Laboratory.

Though the full impact of the damage could take years to fully assess, the hackers were able to view Microsoft source code. They were able to bypass Einstein, a US government intrusion detection tool. They stole red team tools from FireEye—tools that FireEye used to mimic adversary techniques and uncover vulnerabilities in an organization's infrastructure as a hacker would—and accessed email accounts from the Department of Justice. In short, the breach went undetected long enough for the hackers to examine and pull critical information from significant high-value targets. In its report, Microsoft confirmed that SolarWinds hackers accessed the source code of three of its products: Azure (its cloud computing service), Exchange (its mail and calendar server), and Intune (its cloud-based management solution).

Following the breach, Director of National Intelligence Avril Haines remarked that it "was pretty alarming" that FireEye, a private cybersecurity company, had uncovered the SolarWinds breach instead of a member of the US intelligence community.[4] It left Senator Richard Blumenthal "downright scared," and Representative Jim Langevin stated

"We need to do a much better job marshaling all-source intelligence to defeat cyber threats. For a campaign as pervasive as SolarWinds, there are doubtless clues that go far beyond zeroes and ones, and our intelligence community must spend more of an effort connecting those dots."[5]

Cyber intelligence, which includes the collection and analysis of "all sources of intelligence on foreign actors' cyber programs, intentions, capabilities and their impact or potential effects on U.S. national security interests," is key to identifying and understanding cyber threats and enabling US response options.[6] In short, it is meant to "connect the dots."

This book examines the role of cyber intelligence in identifying, preventing, and countering current and emerging threats. Though the United States has premier cyber intelligence capabilities, there are also gaps that need to be addressed, as reflected by the recent SolarWinds breach. By highlighting some of the recent challenges to US cybersecurity, and examining policy, practice, and players, this book also illustrates the need for additional cyber intelligence integration and collaboration among the public and private sectors, especially in the areas of analysis, threat intelligence sharing, and strategic coordinated response. With an understanding that there is a range of perspectives around intelligence and cyber intelligence practices, it is meant to provide a context for discourse and study. This is an introductory work, and it is not intended to be the final view on these topics.

Key Terms and Concepts

Definitions are useful as they offer a common understanding of a concept or idea. Some cybersecurity terms overlap or are defined differently throughout industries and across the world. In order to provide a common understanding of concepts that will be discussed throughout the book, a few definitions are listed here. To offer consistency, when possible the definitions are pulled directly from official documents from the US Department of Justice, the Department of Defense, or other agencies.

Cyber intelligence is defined by the 2014 National Intelligence Strategy (NIS) as the "collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign information systems."[7]

Important distinctions between the NIS definition of cyber intelligence and the wide range of definitions among private sector organizations are explored in greater depth in Chapter 3.

Cyber espionage is "the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization."[8] Cyber espionage is not the same as cyber intelligence; rather it is a function of cyber intelligence similar to other collection activities. Though it is common for countries to spy on each other, in the United States espionage is a violation of 18 US Code 792–798 and Article 106, Uniform Code of Military Justice.

Cyber crime or **computer crime** refers to "any illegal activity for which a computer is used as its primary means of commission, transmission, or storage."[9] There are a variety of US laws that address cyber crimes ranging from intellectual property theft to child pornography to identity theft. The Budapest Convention on Cybercrime was the first international treaty to address cyber crime.

Cyber terrorism is defined by the Federal Bureau of Investigation (FBI) as a "premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and subnational groups."[10] (Some consider this a subset of cyber crime.)

A **cyber attack** is "an attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network [or an] attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[11]

A **computer network attack** is a related term used by the Department of Defense defined as "actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[12]

Similarly, **offensive cyber operations** (OCOs) are "intended to project power by the application of force in and through cyberspace."[13] There have been various attempts to establish an international consensus regarding armed attacks in cyberspace. The *Tallinn Manual* is a good reference for this topic.

The National Institute for Standards and Technology (NIST) defines a **cyber incident** or **cyber breach** as an "occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies."[14]

In light of the SolarWinds attack, which activated the National Cyber Incident Response Plan in accordance with Presidential Policy Directive 41, understanding the terms outlined in the plan is key to also understanding the various US federal and private sector response roles following a significant cyber incident.

A **cyber incident** is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of the directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."[15]

A **significant cyber incident** is "a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[16] (The SolarWinds breach was classified as a significant cyber incident.)

Structure of the Book

Chapter 2 introduces the threat landscape and explores patterns of escalating cyber aggression. Cyber incidents have increased in cost, scope, and severity at an alarming rate and threaten national security. Cybersecurity and deterrence strategies have not been able to protect private sector corporations and critical services. In fact, many are consistently targeted by nation-state cyber actors or their proxies at a rate they are not able to afford or withstand alone. By summarizing the scope of attacks across industry and geography, this chapter reinforces the need for expanded cyber intelligence. This chapter intentionally covers a plethora of breaches to firmly illustrate how egregious cyber threat actors have been.

Chapter 3 examines the various applications of cyber intelligence in the public and private sectors and discusses some key concepts related to cyber intelligence. For the purpose of this book, *cyber intelligence* and *cyber threat intelligence* are defined as a process, but also a product, of collection, processing, analysis, and dissemination (the intelligence cycle). While this book offers a look at various approaches to cyber intelligence across industries, it is important to note that it is not an

instruction manual, but rather an examination of the application of cyber intelligence in both the public and private sectors.

Today, cyber intelligence is critical to ensuring that national security strategy objectives are met and that national security leaders remain informed about events at home and around the world. National security strategies often provide insight into intelligence (and cyber intelligence) priorities and their role in advancing US objectives. To this end, Chapter 4 offers a review of US strategic security documents spanning four presidencies to illustrate crucial developments that have influenced the expansion of cyber intelligence.

Since the National Security Act of 1947 was enacted, the intelligence community has continued to evolve along with developments in technology. A look at some of the elements of the intelligence community can help to demonstrate how the United States has become a leader in global cyber intelligence and how the country's future prosperity and security are dependent upon its continued evolution and success. Recognizing that all agencies within the intelligence community contribute to national security, Chapters 5 to 8 focus primarily on the history and various activities of the director of national intelligence (DNI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation as they relate to cyber intelligence. These chapters provide a snapshot of the roles and accomplishments of various leaders of the intelligence community (the DNI), an intelligence agency that falls under the Department of Defense (the NSA), one that is independent (the CIA), and one that is an element of another agency (the FBI). The intelligence community operates in a shroud of mystery, so unfortunately these chapters can offer only a peek into some of the work that has reportedly been done by some of the world's most esteemed intelligence professionals.

Especially after the terrorist attacks of September 11, 2001, information sharing across the intelligence community and with the private sector took on a new priority, one that has expanded with the growing sophistication and scope of cyber threat actors. More than ever, information sharing is fundamental to protecting corporations, critical services, and national assets. Chapter 9 examines some of the US policies and strategies that support, shape, and facilitate cyber intelligence sharing, briefly summarizing some of the agencies involved in sharing and some of the challenges that prevent it.

Chapter 10 explores the role of counterintelligence as a critical piece to addressing the comprehensive threats to national security in relation to cyber threats and cyber threat actors. Cyber intelligence informs about cyber threats, threat actors, and their capabilities, tactics,

and intent, but the intelligence it provides is meant to be actionable. Cyber counterintelligence and other response options across the instruments of national power must offer effective responses to deter malign cyber threat actors. This chapter also explores US cyber counterintelligence and strategic response, and examines the scope of actions and elements of power at the disposal of the US government to address current and emerging cyber threats and threat actors.

In 2011 the US Department of Defense's Strategy for Operating in Cyberspace announced a new fighting domain: cyberspace. Battles, as a result, can officially be fought in and through cyberspace much like air, land, and sea. Around the same time, the United States set up US Cyber Command. To be expected, many nations adopted a similar approach to militarizing cyberspace; since then, the threats to national security and military superiority have expanded. The next chapters look at various challenges to national security, including nation-state threat actors and nonstate threat actors, and explore the role of cyber counterintelligence in addressing some of these challenges.

Maintaining military superiority in all domains requires superiority in cyberspace, especially today. Cyberspace supremacy requires continuous cyber intelligence support and the right tools to provide knowledge and access to foreign networks. For decades, the United States has been a dominant military force and held a significant advantage in cyberspace, one that is no longer ensured. To illustrate this evolution, Chapter 11 focuses on events and details surrounding various conflicts that have employed a component of cyber operations, starting with the Gulf War. As a result of the dependence of the United States on cyberspace, its adversaries are becoming increasingly capable of damaging critical services and its military, economy, and society. Nation-states employ a wide range of tools and techniques and engage in persistent campaigns to erode US power. For example, investigations into Russia's involvement in recent US presidential elections have revealed that the Kremlin has launched prolific cyber attacks against the US populace at a scale not seen before. Iran has threatened to retaliate against the United States for the 2020 drone strike against General Qasem Soleimani, with members of the intelligence community warning that attacks could include damaging cyber operations against critical infrastructure. To comprehend adversary capabilities, campaigns, and intent more fully, Chapter 11 examines key nation-state competitors Russia, China, Iran, and North Korea in greater depth.

Chapter 12 examines various nonstate threat actors, the threats they present, and the cost related to their crimes. Dark Web activity is on the rise. Insiders and external hackers have compromised US intelligence

agencies and have dumped an overwhelming amount of national secrets onto the internet, at great cost to global security. For example, the WannaCry ransomware breach was possible because of information leaked from the National Security Agency. Some organized crime groups are highly funded and capable, and at times offer services to other criminals, terrorists, and nation-state cyber actors. Though not as popular as in the past, individuals and hacking collectives can and still do cause significant damage to their victims.

Cyber intelligence is rife with challenges, especially considering the rate of change in cyberspace. Today, the US intelligence community and private sector cybersecurity professionals are concerned about a variety of issues including contamination of the supply chain, insider threats, workforce shortages, data overload, going dark, and warrantless encryption, as well as gaps in warning and the consequences of security leaks. The issues facing the public and private sectors will grow ever more challenging given the anticipated near-future technology explosion. Chapter 13 reviews a handful of issues currently facing both the intelligence community and private sector organizations and examines the implications for cyber intelligence, offering some official perspectives on addressing these concerns.

Case studies can be used to encourage critical thinking and engage individuals in dialogue about complex issues. Chapter 14 explores three nation-state campaigns and looks at how countries use cyberspace to meet their strategic objectives. The case studies examine Operation Olympic Games, the Mandiant APT 1 report, and the Democratic National Committee (DNC) breach. These examples also highlight critical challenges facing cyber intelligence and cybersecurity professionals and illustrate the lack of strategic responses needed to fully address nation-state cyber threats.

According to General Keith Alexander, former head of the NSA and US Cyber Command, there are several simultaneously evolving opportunities and challenges that are critical to the future of US economic, military, and national security.[17] Given that the United States has been lagging in the development and implementation of some of these innovations, Chapter 15 examines emerging technologies and explores what they mean for the country's future and the role of cyber intelligence. Machine learning, artificial intelligence, 5G, and quantum computing are some of the areas addressed in this chapter. The implementation and potential convergence of advanced, disruptive technologies will demand an increase in and evolution of cyber intelligence in order to inform on adversary intentions and guide leadership into the unknown but highly

advanced future. Final thoughts summarizing the future of cyber intelligence are included in this chapter.

Notes

1. US Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018.
2. David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack," *New York Times,* January 2, 2021.
3. Veronica Stracqualursi, "Ex-DHS Adviser Under Trump Calls for Urgent Action to Address Suspected Russian Cyberattack," December 17, 2020.
4. Sanger, Perlroth, and Barnes, "Billions Spent on U.S. Defenses Failed to Detect."
5. Mariam Baksh, "The Hack Roundup: Biden Orders Intel Assessment of Suspected Russian Malfeasance," January 22, 2021.
6. Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America,* 2019.
7. James R. Clapper, *National Intelligence Strategy of the United States of America,* Office of the Director of National Intelligence, 2014, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf.
8. *Oxford English and Spanish Dictionary,* "Cyber Espionage," n.d., https://www.lexico.com/definition/cyberespionage.
9. *Legal Dictionary,* "Cyber Crime," n.d., legaldictionary.net.
10. Serge Krasavin, "What Is Cyber Terrorism?" n.d., https://www.crime-research.org/library/Cyber-terrorism.htm
11. *FFIEC IT Examination Handbook,* "Cyber Attack," n.d., https://ithandbook.ffiec.gov/glossary/c/cyber-attack.aspx.
12. Military Factory, "Computer Network Operations," n.d., https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=1179.
13. US Department of Defense, "Joint Publication 3-12 R," *Cyberspace Operations: Offensive Cyber Operations,* February 5, 2013.
14. National Institute of Science and Technology, Small Business Cybersecurity Corner, "Glossary," n.d., https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.
15. US Department of Homeland Security, "National Cyber Incident Response Plan," December 2016.
16. Ibid.
17. *Proceedings,* "An Interview with Two Top Cyber Warriors," July 2020.