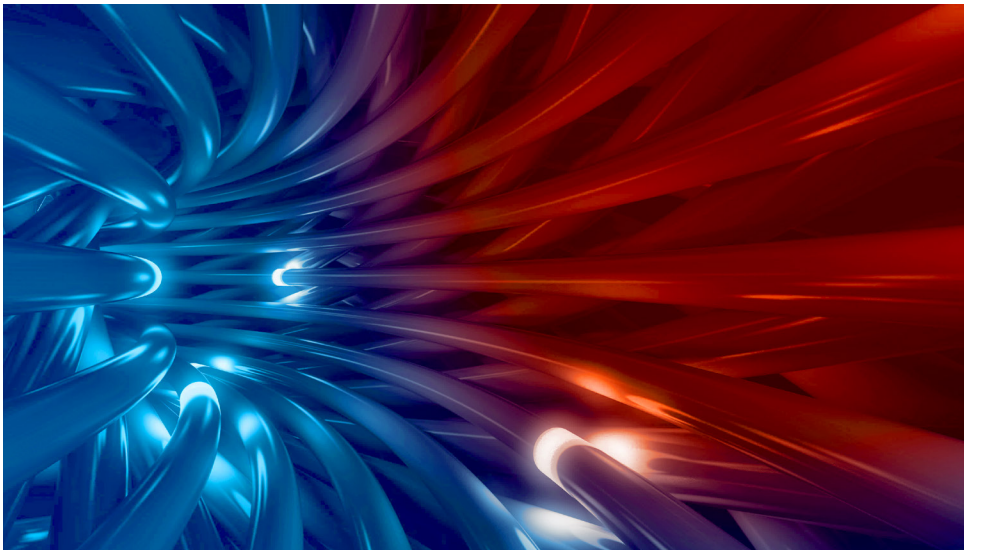
QUENTIN E. HODGSON, YULIYA SHOKH, JONATHAN BALK

Many Hands in the Cookie Jar

Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response



For more information on this publication, visit **www.rand.org/t/RRA1190-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0901-0

Limited Print and Electronic Distribution Rights

About This Report

The December 2020 revelations of a cyber espionage campaign targeting multiple government and private sector organizations in the United States highlighted the continuing challenge of cyber-enabled espionage. The so-called SolarWinds compromise was not the first time that a foreign nation had successfully infiltrated U.S. government networks to steal data and will likely not be the last. In the aftermath of the compromise, policymakers and lawmakers called for various response actions but with little concept of what forms of response might be effective and appropriate in the context of cyber-enabled espionage. This study, conducted from March to November 2021, examines prior examples of state-sponsored cyber espionage to see what forms of response the U.S. government considered, what actions it took, and whether those actions changed adversary behavior or affected other actors' behavior. We conclude that except in the unique circumstances surrounding the compromise of the Office of Personnel Management in 2015, response actions have had little effect on adversary behavior, including that of other actors. The report concludes by recommending the use of more-active forms of underutilized responses, such as counterintelligence. This research should be of interest to policymakers in the Executive Branch and analysts in the intelligence community.

The research reported here was completed in January 2022 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

We would like to acknowledge the support of Rich Girven, who first motivated the research for this project, and Michael McNerney and Michael Spirtas for their continued support. We also would like to thank Tom Wingfield and Peter Roady for their careful review and comments. Our thanks to the current and former government officials who were generous with their time and insights.

Summary

The focus of this report is on significant cyber incidents affecting U.S. government systems and networks. It seeks to address the following questions: What responses has the United States considered in the past to cyber compromises of U.S. government systems? Has the United States been able to materially affect adversary behavior through past responses? How should the United States respond to similar incidents in the future? Should the United States expect those responses to achieve its objectives in the future in light of prior responses?

Employing a qualitative approach encompassing a thorough literature review of publicly available sources and a limited set of interviews with former government officials involved in responding to prior incidents, we examine three cases of Russian cyber-enabled espionage and two cases of Chinese cyber-enabled espionage dating back to the Moonlight Maze compromise of multiple government agencies in the late 1990s up to the 2015 compromise of the Office of Personnel Management.

Policymakers have many response options. These include

- **economic:** sanctions against government officials, individual actors, private organizations; travel restrictions on individuals (applied unilaterally or in coalition with other countries)
- **political/diplomatic measures:** demarches, expelling foreign government officials
- **intelligence:** tracking Advanced Persistent Threats, counterintelligence operations, covert action, disclosure of malware and adversary tactics
- **law enforcement action:** asset seizure, court-ordered infrastructure take-down, arrest and prosecution
- **military:** cyber show of force, defensive cyber operations on government systems and in gray space (e.g., *hunt forward* or defensive response actions), offensive cyber operations against adversary actors and infrastructure, and traditional (noncyber) military operations.

The first thing to note is that the available response options are not limited to the cyber domain, and no one should expect them to be. However, the historical record suggests that the United States has felt constrained in its ability to respond vigorously against Russia or China because of the notion that espionage is a standard and accepted practice by nations and that the United States would not want to take steps to constrain its own ability to engage in similar intelligence activities in cyberspace. Additionally, policymakers assessed that breaches of confidentiality, although damaging in the long term, did not rise to the same level of acute damage to national security that another, more destructive form of cyber operation might entail. But the United States has proved especially vulnerable to cyber incidents, and a lack of response appears to have emboldened the Russians and Chinese to continue and expand their cyber espionage activities over the years.

The one instance we examined in which the United States appears to have made any impact on adversary behavior—the agreement between U.S. President Barack Obama and Chinese President Xi Jinping in 2015—was unique because the Chinese government was motivated to come to an agreement with the United States to prevent an embarrassing moment for China. Furthermore, the role of diplomacy should not be diminished, and more-recent multilateral efforts to call out malicious cyber behavior—including a coordinated set of declarations by the United States and its allies against China in July 2021—has the potential to lay a foundation for shaping international norms.

Additionally, improving the United States' ability to deter by denial—improving the cybersecurity of the U.S. government—remains an elusive but vital priority. The United States should pursue expanded diplomatic efforts, including with its partners and allies, to call out indiscriminate cyber espionage and establish guardrails for acceptable cyber espionage. It should also expand its use of active defense measures on U.S. government networks to hunt for adversary activity and should offer similar support to partners and allies. Finally, the United States should make better use of counterintelligence, particularly deception operations, to reduce the benefits that countries might derive from cyber espionage.

Contents

Tables

CHAPTER ONE

Introduction

On December 8, 2020, the cybersecurity firm FireEye, famous for its cyber incident response support to numerous companies and organizations, announced that it had been the victim of a cyber compromise itself.[1] Sophisticated cyber actors had stolen FireEye's Red team tools in an apparent attempt to learn how to exploit those tools to infiltrate other networks. A week later, on December 13, 2020, FireEye traced the vulnerability to an update in SolarWinds's information technology (IT) infrastructure management software tool, Orion. The vulnerability had persisted at least since spring 2020.[2] The White House convened a Cyber Unified Coordination Group (UCG) on December 15, 2020 to coordinate the response to the SolarWinds compromise,[3] and it quickly became evident that multiple government agencies and private sector companies were victims of the attack. Analysts concluded that Russian cyber actors—a so-called Advanced Persistent Threat (APT)—were likely responsible for the compromise, and the incoming Biden administration revealed that nine government agencies and 100 companies had been victims of the "indiscriminate effort to compromise the network management software used by both government and the private sector."[4] The Department of the Treasury, the National Nuclear Security Administration (NNSA, part of the Department of Energy) and the Department of Homeland Security (DHS) were among the victims.[5]

News of the SolarWinds compromise prompted widespread concern and varying reactions. Microsoft President Brad Smith called the operation "reckless" because it put thou-

[1] Kevin Mandia, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," *FireEye Stories*, blog post, December 8, 2020a.

[2] Kevin Mandia, "Global Intrusion Campaign Leverages Software Supply Chain Compromise," *FireEye Stories*, blog post, December 13, 2020b.

[3] The National Security Council tweeted out notification of the Cyber UCG (see National Security Council [@WHNSC45], "(1/3) Pursuant to Presidential Policy Directive-41 (26 July 2016) and its Annex, a Cyber Unified Coordination Group (UCG) has been established to ensure continued unity of effort across the United States Government in response to a significant cyber incident," Twitter post, December 15, 2020).

[4] White House, "Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021," transcript, Washington, D.C., February 17, 2021.

[5] Tapiwa Matthew Mutisi, "Microsoft President Brad Smith Calls SolarWinds Hack 'Act of Recklessness,'" *Innovation Village*, blog post, December 20, 2020.

sands of SolarWinds customers at risk.[6] Senator Richard Durbin said it was "virtually a declaration of war by Russia on the United States," a sentiment echoed by Senator Mitt Romney, who compared it with Russian bombers "flying undetected over the entire country."[7] Others urged caution in using such terms as "act of war" to describe what they saw as simple cyber-enabled espionage.[8] In the wake of the SolarWinds compromise, the White House issued two Executive Orders, including one on April 15, 2021 designed to address Russia's "harmful foreign activities,"[9] although the order refers to malicious cyber-enabled activities and not specifically espionage.

The SolarWinds compromise was not the first time the United States government has been the victim of a cyber compromise, and it likely will not be the last. The first documented case of computer network–enabled espionage occurred in the mid-1980s when a West German–based actor was discovered to have hacked into the Lawrence Berkeley National Laboratory network to search for nuclear secrets to pass to Soviet intelligence.[10] As the government and private sectors have come to rely increasingly on IT to conduct business, cyber-enabled espionage also has increased. Given this growth and the continued successful targeting of U.S. government systems and networks, we wanted to explore how the United States has responded to these incidents in the past. The SolarWinds compromise prompted several questions on the part of policymakers, lawmakers, and the public: Why are cyber espionage campaigns successfully continuing to target U.S. government systems and networks? Has the United States been able to materially affect adversary behavior through its response in the past? How should the United States respond to these incidents in the future? Should the United States expect those responses to achieve its objectives in the future? The challenge of countering cyber espionage is great, and previous efforts to motivate a change of behavior have yielded temporary results at best.[11]

---

[6] Brad Smith, "A Moment of Reckoning: The Need for a Strong Global Cybersecurity Response," *Microsoft on the Issues*, blog post, December 17, 2020.

[7] Maggie Miller, "Lawmakers Ask Whether Massive Hack Amounted to Act of War," *The Hill*, December 18, 2020.

[8] Tarah Wheeler, "The Danger in Calling the SolarWinds Breach an 'Act of War,'" *TechStream*, March 4, 2021.

[9] Joseph R. Biden, Jr., *Executive Order Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation*, Washington, D.C.: White House, April 15, 2021a.

[10] The astronomer at Lawrence-Berkeley who managed the laboratory's computer network documented his work to track down the intruder in an article and then a book. See Clifford Stoll, "Stalking the Wily Hacker," *Communications of the ACM*, Vol. 31, No 5, May 1988; and Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, New York: Doubleday, 1989.

[11] David E. Sanger, "Ignoring Sanctions, Russia Renews Broad Cybersurveillance Operation," *New York Times*, October 25, 2021.

Methodology

The focus of this report is on significant cyber incidents affecting U.S. government systems and networks. This is a deliberate selection of a subset of cyber incidents affecting the United States. We chose to focus on cyber incidents affecting U.S. government systems for several reasons: U.S. government systems and networks have been a focus of nation-state actors for several decades now, primarily for espionage purposes, so these types of cyber operations can be seen as legitimately part of the interaction between competitor states even though the U.S. government would seek to prevent them. This distinguishes such cyber operations from attacks on private sector networks (which also can be espionage, but the U.S. government classifies this form of espionage differently) and from attacks intended to have an effect beyond espionage, such as preparing for subsequent attack. This latter form of cyber operation is more often addressed in terms of a declaratory policy about acceptable and unacceptable behavior by other states and, at least for a period through the United Nations Group of Governmental Experts work from 2004 to 2017, was subject to a fragile agreement that such attacks would be considered inappropriate, if not illegal, under international law.

The United States government has invested considerable time and effort in trying to secure its networks and systems from cyber attacks, apparently to little avail. Improving the cybersecurity posture of the U.S. government has been a focus of numerous studies and initiatives, but the United States remains vulnerable.[12] Unfortunately, the SolarWinds compromise (and the unrelated, subsequent Microsoft Exchange Server vulnerabilities) is unlikely to be the last such incident affecting U.S. government systems—therefore, future incidents will likely lead to more calls for response. Understanding why and how the United States responds, and why that response has not achieved its objectives, is critical to finding a more productive way forward.

We have chosen to focus our research on incidents attributed to the Russian Federation and the People's Republic of China. The United States faces multiple adversaries in cyberspace beyond Russia and China, including nation states like Iran and North Korea, and cybercriminal groups, but Russia and China are the so-called *pacing threats* identified as

[12] See Defense Science Board, *DSB Task Force Report on Cyber Defense Management*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2016; and Angus King and Mike Gallagher, *United States of America Cyberspace Solarium Commission: Final Report*, Arlington, Va., March 2020. For example, the Obama administration created the Cybersecurity National Action Plan after the Office of Personnel Management (OPM) compromise; the Trump administration issued an Executive Order on strengthening cybersecurity of federal networks and a national cyber strategy; and the Biden administration issued an Executive Order on federal cyber security after SolarWinds and the Microsoft Exchange Server compromises. See White House, Office of the Press Secretary, "Fact Sheet: Cybersecurity National Action Plan," press release, Washington, D.C., February 9, 2016; Donald J. Trump, "Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Washington, D.C.: *Federal Register*, Vol. 82, No. 93, May 16, 2017, pp. 22391–22397; Donald J. Trump, *National Cyber Strategy of the United States of America*, Washington, D.C.: White House, September 2018; and Joseph R. Biden, Jr., *Executive Order on Improving the Nation's Cybersecurity*, Washington, D.C.: White House, May 12, 2021b.

the most substantial threats to the United States in cyberspace.[13] Russia and China have targeted the United States through cyberspace for more than two decades. We chose case studies across this time span to determine whether there had been changes in adversary behavior over time and to see how the changes in U.S. government posture and policies may have affected response. Table 1.1 identifies case studies we considered for this research.

From these candidate case studies noted in Table 1.1., we selected Moonlight Maze, Titan Rain, Agent.btz, the State Department, White House, and the OPM compromises because these cases provide a breadth of activities over time from the late 1990s to 2015 and span presidential administrations. We also chose these cases because we determined that there was sufficient publicly available information to develop them sufficiently for analysis. To ensure that we could make the results of our analysis broadly available, we chose not to examine classified sources, which may provide additional insights into aspects of the operations themselves, U.S. government deliberations, and possible responses. This represents an area for further study.

Once we selected our case studies, we conducted a thorough literature review encompassing news reporting, policy statements, congressional testimony, cybersecurity firms' reports, and academic literature. Through this literature review, we identified policymakers involved in crafting and implementing responses to the selected cases, and we requested to interview them. The literature review helped us understand the broad outlines of the incidents, when they became known and what responses were implemented that were publicly known. The interviews supplemented this review by focusing on the options considered and either rejected or adopted to identify the factors policymakers considered and why they concluded the chosen courses of action would be effective. We conducted ten not-for-attribution interviews with people involved in the case studies. Some of the people we interviewed were involved in more than one case study. Table 1.2 indicates the number of interviews applicable to each case study; hence, the numbers total to more than ten.

The interviews supported filling in some gaps in our knowledge on the cases and to learn about the perspectives of participants in these events. However, given the limited number of interviews we were able to conduct, some gaps remain, and we may not have covered all the

TABLE 1.1
Case Studies Considered

Actor	Case Study
China	Titan Rain (2005), U.S. national laboratories (2007), OPM (2015), Hellsing (2015)[a]
Russia	Moonlight Maze (1998), Agent.btz (2008), State Department and White House (2014), SolarWinds (2020)

[a] Hellsing was a suspected Chinese-affiliated APT that targeted Southeast Asian, Indian and United States diplomatic organizations. See Council on Foreign Relations, "Hellsing," webpage, undated-b.

[13] Office of the Director of National Intelligence, *Annual Threat Assessment of the United States Intelligence Community*, Washington, D.C., April 9, 2021.

TABLE 1.2
Interviews Conducted Relevant to Case Studies

Case Study	Number of Interviews
Moonlight Maze	3
Titan Rain	1
Agent.btz	2
State Department and White House	2
OPM	5

relevant perspectives. For example, in some cases we were able to speak with policymakers but not those involved in operational response and vice versa, which means the interviews provide some perspective but not a complete picture or represent even necessarily the full array of policy or operational considerations. Interviewees were not always aware of all the deliberations or details of a case study, and in the older cases the passage of time means that interviewees could not always recall specific details, dates, or events. Finally, interviewees did not discuss classified information.

Organization of This Report

In Chapter Two, we briefly address the evolution of cyber espionage and the options available to policymakers, and we examine what would constitute a positive outcome for the United States. We then turn to the case studies. For each case study, we provide an overview of the incident, when it was detected, the scope of the attack, the policy options considered and selected, and any discernible change in adversary behavior. We conclude each chapter with some summary observations on Russian and Chinese cyber operations against U.S. government systems. The final chapter provides overarching conclusions and recommendations.

CHAPTER TWO

Cyber Espionage, Deterrence, and Response

Cyber espionage has become a political hot-button issue in recent years. The rhetoric can become heated and even overblown. Such words as *cyber war, act of war*, and other similar terms are bandied about to describe these events. The SolarWinds compromise was accompanied by similar language and, even when acknowledged as espionage (and not more malicious intent), was deemed "reckless" by Microsoft President Brad Smith, who went on to comment that it "is not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency."[1] A former director of the National Security Agency (NSA), Army GEN Keith Alexander, called cyber-enabled theft of intellectual property "the greatest transfer of wealth in history."[2] Public acknowledgment of how the internet could be exploited as a means of intelligence-gathering dates back at least to 1996, when the Defense Investigative Service (later the Defense Security Service and now the Defense Counterintelligence and Security Agency) warned that the internet was becoming the fastest-growing medium of espionage.[3]

The United States has a long history of spying and having to deal with foreign governments spying on it, from the first military operations under GEN George Washington, to the breaking of Japanese and German codes in World War II, up to the present day. Spying during the Cold War often meant careful development of contacts in positions to steal or copy valuable intelligence and pass it along, and efforts to eavesdrop on communications, or even the exploitation of technologies used in diplomatic missions.[4] The responses to foreign espionage have

[1] Jay Peters, "Microsoft President Sounds Alarm on 'Ongoing' SolarWinds Hack, Identifies 40 More Precise Targets," *The Verge*, December 17, 2020.

[2] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012.

[3] C. L. Staten, "Warning; Internet Used by Foreign Intelligence Operatives," *ENN Daily Report*, December 9, 1996.

[4] One of the most famous episodes of successful Soviet spying against the United States involved the integration of electronic devices in the IBM Selectric typewriters used in the U.S. Embassy in Moscow in the 1980s and became the subject of a massive NSA effort to find the bugs and remove them. See Sharon A. Maneki, *Learning from the Enemy: The GUNMAN Project*, 2nd ed., Fort George G. Meade, Md.: Center for Cryptologic History, National Security Agency, 2018.

often encompassed a mixture of damage limitation, attempts to improve security, and actions to expel or otherwise decrease the ability of a foreign power to sustain its spying operations.[5]

Counterintelligence—the detection, mitigation and countering of intelligence programs and activities—is prevalent throughout history.[6] Its application to cyberspace has been the subject of some academic research but has also been a part of the U.S. government's toolkit, including capabilities in the Federal Bureau of Investigation (FBI), the military services, and as part of the Office of the Director of National Intelligence.[7] The 2020 National Counterintelligence Strategy includes an objective to "counter foreign intelligence cyber and technical operations" but is understandably vague about how it will accomplish this beyond better integrating intelligence and security functions across government, increasing the cadre of trained cyber counterintelligence professionals, and growing the "cyber counterintelligence toolkit."[8] The definition of *cyber counterintelligence* is also a source of some confusion because it is sometimes defined as encompassing many features of traditional cybersecurity, such as employing intrusion detection and intrusion prevention systems, and training and awareness, in addition to more-active measures, such as deception techniques.[9] Other active defensive measures like *hunt operations*—active search on networks for indications of adversary activities—can also blur the line between cybersecurity and counterintelligence. The question also arises as to whether who conducts the activity categorizes it as counterintelligence as opposed to standard cybersecurity. In other words, if the FBI conducts the activity, is that different than if the Cybersecurity and Infrastructure Security Agency (CISA) does? Certainly, the authorities under which these organizations act are distinct, and their capabilities also differ.

Cyber-enabled espionage presents a particular challenge to policymakers because it can wreak considerable damage to national security for relatively little investment by the adversary. Previously, spies would have to meticulously copy or photograph documents or establish a relationship with a contact who could do the same (as occurred in the Aldrich Ames case).[10] The

---

[5] See, for example, Mark Mazzetti and Michael S. Schmidt, "Two Russian Compounds, Caught Up in History's Echoes," *New York Times*, December 29, 2016; and U.S. Senate, Select Committee on Intelligence, *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence*, Washington, D.C.: U.S. Government Printing Office, November 1, 1994.

[6] See, for example, U.S. Army, National Capital Region Field Office, "History of Army Counterintelligence," webpage, undated; and Raymond J. Batvinis, *The Origins of FBI Counterintelligence*, Lawrence, Kan.: University Press of Kansas, 2007.

[7] For a review of literature on cyber counterintelligence, see P. C. Duvenage, V. J. Jaquire, and S. H. von Solms, "Toward a Literature Review on Cyber Counterintelligence," *Journal of Information Warfare*, Vol. 17, No. 4, Fall 2018.

[8] National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America, 2020–2022*, Washington, D.C.: Office of the Director of National Intelligence, February 2020, p. 10.

[9] P. C. Duvenage, V. J. Jaquire, and S.H. von Solms, "A Cyber Counterintelligence Matrix for Outsmarting Your Adversaries," *Journal of Information Warfare*, Vol. 19, No. 1, March 2020.

[10] U.S. Senate, Select Committee on Intelligence, 1994.

introduction of computers and more centralized storage of information increased the scale of potential breaches by enabling the downloading of information to removeable media, but this approach still required physically accessing the systems and networks. With the advent of the internet and more connections across systems and networks, the perpetrators do not even have to set foot on U.S. territory. (This factor could extend to cyber-enabled espionage against classified networks, although as we shall see in the case of Agent.btz, accessing and then successfully exfiltrating that information is not a simple task.) This factor also poses challenges because malicious cyber operators, unlike spies, can operate safely from their own countries who often protect them from more traditional law enforcement or counterintelligence operations.

What Options Are Available to Policymakers?

There is a broad array of policy options available to respond. These include

- **economic:** sanctions against government officials, individual actors, and private organizations; travel restrictions on individuals (applied unilaterally or in coalition with other countries)
- **political/diplomatic measures:** demarches, expelling foreign government officials, recalling ambassador
- **intelligence:** tracking APTs, counterintelligence operations, covert action, releasing information on malware employed by the adversary[11]
- **law enforcement action:** asset seizure, court-ordered infrastructure takedown, arrest and prosecution or civil proceedings
- **military:** cyber show of force, defensive cyber operations on government systems and in gray space (e.g., *hunt forward* or defensive response actions), offensive cyber operations against adversary actors and infrastructure, and traditional (noncyber) military operations.

Not all these policy options will be seriously considered in each case of a cyber incident affecting U.S. government networks and systems, particularly if those incidents are assessed to be purely intended for espionage. We include this list here to show the array of potential options that might be considered, even if they may be rejected as too escalatory, disproportionate to the incident, or even illegal under international law. No response is also a form of response and also may convey a message to the adversary. The response options available are also not exclusive to the cyber domain. The United States has many tools available to respond and one should not expect that a cyber incident warrants only a cyber response: The most effective response could well fall outside the cyber domain.

[11] Note that many different government actors in both the intelligence community and beyond can publicly release malware employed by the adversary.

What Would Constitute a Positive Outcome?

As we considered the potential options available, the other side of the equation is understanding what the desirable outcomes would be. It is unlikely that the United States can expect a complete cessation of cyber espionage operations from Russia and China. We explain what to look for in terms of scope, scale, and character of change in an adversary's cyber espionage operations.

The first outcome would be a diminishing in the *scale* of cyber espionage operations. In this case we would expect to see a lower overall volume of cyber espionage operations directed at the United States, in particular targeting U.S. government systems and networks.

The second outcome, which is not exclusive from the first, would be a change in *scope* of the cyber espionage operations. This might include cyber espionage operations targeting less-sensitive systems and networks, or more selective targeting of government systems. For example, rather than seeking to target the NNSA and files related to nuclear warhead modernization, the United States might seek a shift in focus away from these sensitive areas to other areas in the Department of Energy's mandate (the parent agency of the NNSA). Although this kind of shift would still be unsatisfactory from a broad U.S. government perspective, it is still a potentially better outcome than no change in adversary behavior at all (or even more intensive cyber espionage operations by an adversary).

The third outcome would be a change in *character* of the cyber espionage operations. This might include less invasive or destructive forms of cyber espionage operations—focusing for example on exfiltration of files (violating confidentiality of a system and data rather than manipulating records or having a more adverse effect on system functions (e.g., an integrity attack) or denying the United States access to systems, data, and functions (e.g., an availability attack). This outcome may be less apparent because most cyber espionage operations against U.S. government systems and networks to date have been confidentiality attacks—designed to steal information but not affect system functions or deny system access to the United States. Therefore, deterring the evolution of cyber espionage into more-destructive forms of cyber operations is also a desirable outcome.

We also note that these outcomes characterize a change in adversary behavior. It is possible that the United States would seek to retaliate against an adversary to inflict some punishment while not necessarily expecting the adversary to change its behavior. That said, it would appear more likely that reprisal would be intended to have an influence on an adversary's decision calculus in the future—to demonstrate there are consequences to actions and to underpin deterrence by demonstrating there are costs the adversary should expect—rather than purely to satisfy an urge to "do something" and punish the adversary.[12]

[12] Thomas Schelling discusses these concepts at length, including the history of violent diplomacy, in his seminal work, *Arms and Influence*.

CHAPTER THREE

Russia Case Studies

Moonlight Maze

Moonlight Maze is the code name for the FBI investigation beginning in July 1998 into intrusions into a variety of government agencies. The first intrusions were detected in October 1996, including at one of the Air Force's ranges in New Mexico. In 1996, the intruders used a backdoor to transmit data via a covert channel that used protocols, such as Internet Control Message Protocol, to function as a file transfer without using the File Transfer Protocol.[1] In January 1998, security experts first spotted the intrusions when Air Force and Army computer crime investigators tracked attacks to an internet service provider in Russia.[2] Victims of the Moonlight Maze intrusions were in several countries, including the United Kingdom, Canada, Brazil, Germany, and the United States. The targets of the intrusions in the United States were the U.S. Department of Defense (DoD), National Aeronautics and Space Administration (NASA), Department of Energy, Wright Patterson Air Force Base, the Los Alamos and Sandia National Laboratories, the Air Force Institute of Technology, the Army Research Laboratory, and naval research institutions.[3] The intrusions lasted for more than a year and, at the time, were described as "the longest-running and most widespread attack we've seen."[4]

The full extent of the Moonlight Maze intrusions has not been publicly revealed, but the intrusions were clearly extensive. In his Senate testimony, Michael A. Vatis, then–director of the FBI's National Infrastructure Protection Center, stated that the intruders stole "unclassified but still sensitive information about essentially defense technical research matters," such as bidding documents and contracts.[5] One media source reported that stolen documents "could include classified naval codes and information on missile-guidance systems,"

1 Nikolay Pankov, "Moonlight Maze: Lessons from History," *Kaspersky Daily*, April 3, 2017.

2 Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law*, Vol. 12, No. 5, 2001.

3 Chris Doman, "The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History," blog post, July 7, 2016.

4 Bob Drogin, "Yearlong Hacker Attack Nets Sensitive U.S. Data," *Los Angeles Times*, October 7, 1999.

5 Michael A. Vatis, director of the FBI's National Infrastructure Protection Center, in statement before a Senate subcommittee, as quoted in Drogin, 1999.

according to intelligence sources familiar with the case.[6] In the few years immediately following the intrusions, one official noted that it was "difficult to tell what the damage is" because no systems were shut down, but file listings were taken and people's directories were surveyed. Intruders also installed tools to enable the adversary's access later.[7] Over the next two decades, the extent of impact from the intrusions continued to be described in no more detail but as the theft of "vast amounts" of information, "many thousands of pages," and "the height of the documents stolen—if printed out and piled up—would triple the height of the Washington Monument."[8]

Initially, U.S. law enforcement tracked the attacks passively "because 'hack-backs' could have been construed as an act of war, if the intruders were state-sponsored."[9] An interagency group set up a *honeypot* website to attract the hackers. When the hackers exfiltrated data from the honeypot, they also took a beacon with them that the interagency group could track.[10]

The first public confirmation occurred in October 1999, when Vatis, in testimony before a Senate subcommittee, said that "the intrusions appear to have originated in Russia."[11] In 2001, the *Wall Street Journal* reported that the Department of State "formally pressed Russia . . . for help" in 2000 after investigators determined that the attacks appeared to have originated from seven Russian internet addresses.[12] One interviewee recalled that once the U.S. government had gathered enough information pointing to a source in Russia, the FBI made the decision to reach out to Russian investigators.[13]

Russian investigators initially cooperated and provided useful information: "That surprised people."[14] Then, a spokesman for Russia's intelligence service denied culpability and the early days of cooperation from the Russians quickly ceased.[15] Russian officials did respond to

---

6 Gregory Vistica, "'We're in the Middle of a Cyberwar,'" *Newsweek*, Vol. 134, No. 12, September 20, 1999.

7 NASA Inspector General Roberta Gross as quoted in Drogin, 1999.

8 Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review*, Vol. 64, Winter 2009, p. 141; Doman, 2016; and "Hack May Have Exposed Deep U.S. Secrets; Damage Yet Known," Associated Press, December 15, 2020.

9 Dion Stempfley, a former Pentagon computer security analyst, as quoted in Vernon Loeb, "NSA Adviser Says Cyber-Assaults On Pentagon Persist with Few Clues," *Washington Post*, May 7, 2001.

10 Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster, 2016.

11 Drogin, 1999.

12 Ted Bridis, "E-Espionage Rekindles Cold-War Tensions—U.S. Tries to Identify Hackers; Millions of Documents Are Stolen," *Wall Street Journal*, June 2001; Loeb, 2001.

13 We conducted ten not-for-attribution interviews with people involved in the case studies during our study period from March to November 2021. Those interviews are noted throughout this report.

14 Interview with former senior official, 2021. See also Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York: Anchor Books, 2020, pp. 74–76.

15 Bridis, 2001.

U.S. inquiries that "the telephone numbers associated with the sites were inactive."[16] In May 2001, the State Department confirmed that U.S. diplomats had issued a demarche to Russia.[17]

The demarche notwithstanding, one interviewee noted that "there was little . . . response to Moonlight Maze" at the time.[18] Accusing Russian actors would have relied on scant evidence beyond identifying Russian internet protocol (IP) addresses as the sources of the intrusions. But policymakers were reluctant to attribute the intrusions to the Russian government, or they at least felt that they had insufficient proof based only on the origin of the intrusions in Russia. One policymaker recalled that "we didn't consider retaliatory or diplomatic action . . . [but] focused on defensive measures partly because we were doing [cyber espionage] too, and more of it and more effectively, and didn't want to draw attention to it."[19] Alternatively, another interviewee noted that DoD only reacted to high-visibility events, such as Moonlight Maze, and did not take a more active stance against cyber intrusions. Cyber defense was not a discussion that gathered any import with senior leaders at the time "unless there was a burning bridge . . . unless you had an attack or loss of a great amount of data."[20] DoD also implemented other actions of a purely defensive nature, including changing passwords and looking for and updating "unused ancient code" that was vulnerable to exploitation.[21]

Crafting a coherent response was also complicated by questions about data access and what information was available to support decisionmaking. "I wanted a holistic view of the Internet, a big board," one interviewee recalled, but "there wasn't one." This interviewee identified a useful technology in the private sector that DoD subsequently purchased. Another interviewee recalled that few people "could know what we were doing and were aware and responding to what we were doing."[22]

The government's organizational structure presented still more challenges as the nature of discussions around responses differed across the operational (e.g., DoD), intelligence (e.g., NSA), and law enforcement communities (e.g., FBI). Although the operational side "[was] in reactive mode [and] not thinking about what the end goal of the intrusion was," something else could have been happening on the intelligence side, but the operators "didn't have access to that information."[23] The operational side focused on protecting weapon systems and sensitive information and did not have analysis of what the adversary extracted or of what value that information could be. Interviewees also recalled that the tools and capabilities available at the time of the intrusions were "highly classified" and accessible "only for intelligence

16 NSA consultant James Adams as quoted in Loeb, 2001.

17 Loeb, 2001.

18 Interview with former senior official, 2021.

19 Interview with former senior official, 2021.

20 Interview with former senior official, 2021.

21 Interview with former senior official, 2021.

22 Interview with former senior official, 2021.

23 Interview with former senior official, 2021.

applications" at the NSA; "non-black world parts of the DoD" only had access to rudimentary tools and capabilities and, therefore, had to rely on intelligence agencies to address the challenge of Moonlight Maze.[24] The mission of law enforcement was "to detect, warn, and respond in investigating and issuing analysis for victims to use to protect themselves."[25]

Some interviewees and cybersecurity researchers said they believe that the actors behind Moonlight Maze have continued to operate against the United States under different guises. The Moonlight Maze intrusions stopped briefly in 1999 after the FBI team returned from its April 1999 trip to Moscow but appear to have started up again just a few months later.[26] Although a direct causal link is not clearly available, it would seem that the exposure of the intrusions led the Russians to choose to temporarily halt their activities and likely to reassess their operational approach and potentially improve stealth. Two months after the FBI's trip to Moscow, Joint Task Force-Computer Network Defense detected another intrusion into military servers, which had slightly different signatures and codes that were harder to break.[27] In 2017, one group of researchers concluded that the actors behind Moonlight Maze evolved to develop new tools and became the modern APT group Turla (also known as Venomous Bear or Snake).[28] This factor could indicate that information-sharing with the Russian government alerted it to the need for improved cyber espionage tradecraft and operational security.

The Moonlight Maze intrusions occurred at a time when "most communication [between malicious actors] wasn't encrypted, patterns [were] easily discernible, and assets such as malicious filenames were frequently used. There was a clear routine to the operation spanning several years and dozens of networks."[29] For one of the interviewees, Moonlight Maze provided the first indication that another country had the same cyber capabilities as the United States—another actor was using sophisticated hacking skills for espionage purposes in a systematic, large-scale way.[30] Although public revelations of the cyber intrusions began to appear in 1999, the cyber campaign appears to have persisted until 2003. Moreover, the malicious actor's behavior or targeting did not appear to change at the time. Interviewees posited that the perpetrators behind Moonlight Maze never stopped their activities. One interviewee surmised that the intrusion has lasted for more than 20 years and is the campaign Russia continues to use to gather information against the United States.

The United States employed diplomatic and investigative avenues to engage the Russian government. Russia was highly cooperative at first, even acknowledging (albeit likely without

[24] Interview with former senior official, 2021; Kaplan, 2016.

[25] Interview with former senior official, 2021.

[26] Greenberg, 2020, p. 76; Kaplan, 2016, p. 88.

[27] Kaplan, 2016, p. 88.

[28] Juan Andres Guerrero-Saade, Costin Raiu, Daniel Moore, and Thomas Rid, *Penquins Moonlit Maze: The Dawn of Nation-State Digital Espionage*, London: Kaspersky Lab, King's College London, 2017.

[29] Guerrero-Saade et al., 2017.

[30] Interview with former senior official, 2021.

official approval) the likelihood that Russian government operators were responsible. The circumstances quickly changed, however, and Russian cooperation ceased. The United States also employed techniques to track the intruders back to their origins. The United States did not, however, employ other response options either to limit the utility of the information stolen or to deter future cyber espionage.

Agent.btz

Agent.btz is the code name assigned to an intrusion that DoD detected in October 2008 that also infected computer networks around the world (e.g., in the United States, Russia, Spain, Italy, Kazakhstan, Germany, Poland, Latvia, Lithuania, United Kingdom, and Ukraine).[31] In the United States, Agent.btz was detected on DoD's classified networks, the Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communication System (JWICS), in the U.S. Central Command's operational areas.[32] According to our interviews and public information, it does not appear that Agent.btz led to successful exfiltration of data, in particular, from classified networks. But that the malware could extract something from U.S. government's most-sensitive networks was still a concern.[33] Defense officials would not describe the extent of the damage inflicted, although there was a concerted effort at the beginning to try to count the number of affected computers. One interviewee noted that such efforts were largely immaterial and distracting from the focus of response because the number of infected computers was likely to change daily, and DoD at the time did not have a holistic understanding of how many devices it had on each of these networks. Additionally, the malware may have "circulated among nongovernmental U.S. computers for months" before affecting the Pentagon's network.[34] According to our interviews, Agent.btz was "a result of [our] lack of awareness of danger and our own carelessness."[35]

The Agent.btz malware first showed up on military computers of a NATO country's government in June 2008.[36] In October 2008, NSA's Advanced Networks Operations team detected the intrusion on SIPRNet and later on JWICS. The same month, DoD launched Operation Buckshot Yankee to find, restrict, mitigate, and begin to remove the malware from computer systems and to prevent it from escaping from classified to unclassified networks.[37]

---

[31] Council on Foreign Relations, "Cyber Operations Tracker: Operations by Country," webpage, undated-a.

[32] Ellen Nakashima, "Cyber-Intruder Sparks Response, Debate," *Washington Post*, December 8, 2011.

[33] Interview with former senior official, 2021.

[34] Julian Barnes, "Pentagon Computer Networks Attacked; The Cyber-Strike on Key Sites Is Thought to Be from Inside Russia," *Los Angeles Times*, November 28, 2008.

[35] Interviews with former senior officials, 2021.

[36] Nakashima, 2011.

[37] Interviews with former senior officials, 2021; Guerrero-Saade et al., 2017.

In November 2008, DoD banned the use of thumb drives across its systems worldwide.[38] Ultimately, it took 14 months to remove the malware from the Pentagon's networks.[39]

Speculation in the media that the attack "may have originated in Russia" began as early as November 28, 2008.[40] Some sources referred to intelligence sources who said there was evidence of "Russian government involvement," while others cited U.S. officials who said that "a foreign spy agency was responsible."[41] Meanwhile, the malware "called out to a listening post" that Russia's *Federalnaia Sluzbha Bizopastnoci* (or Federal Security Services [FSB]) used for internal control purposes and thus garnered the attention of the team that discovered it.[42] The NSA and DoD concluded that the malware originated in Russia, although the intrusion was deemed classified at the time and official sources never issued any public statements acknowledging or attributing the attack.[43]

The Agent.btz intrusion sparked debates among U.S. defense experts and senior government officials over response options that included rules of engagement for Strategic and Cyber Commands to defend "critical privately owned computer systems."[44] For example, Joint Functional Component Command-Network Warfare proposed options to use offensive capabilities to neutralize the malware on nonmilitary networks, including those in other countries. However, senior officials rejected this response because Agent.btz "appeared to be an act of espionage, not an outright attack, and didn't justify such an aggressive response."[45]

More than the experience with Moonlight Maze, the Agent.btz intrusion further fueled debates over response options because it involved a variety of government agencies with domestic- and foreign-focused missions. Ultimately, the agencies' competing views and priorities stalled plans to protect privately owned critical computer systems. The Department of Justice feared setting a legal precedent for military action in response to hacking domestic networks; the CIA did not want the military to interfere in the CIA's foreign operations; the Department of State worried the military would accidentally disrupt a server in a friendly country without seeking consent; and DHS wanted to remain the leading agency in securing the nation against cyber threats.[46] In October 2010, two years after the first detection of the Agent.btz intrusion in U.S. military networks and the subsequent debates surrounding the

38 Nakashima, 2011.

39 Council on Foreign Relations, undated-a.

40 See, for example, Barnes, 2008.

41 Rebecca Grant, "The Cyber Menace," *Air Force Magazine*, March 1, 2009; and Phil Stewart and Jim Wolf, "Agent.btz Worm Won't Die After 2008 Attack on Military," Reuters, June 17, 2011.

42 Interview with former senior official, 2021.

43 Interview with former senior official, 2021.

44 Nakashima, 2011.

45 Nakashima, 2011.

46 Nakashima, 2011.

U.S. response, DoD and DHS took steps "to enhance the nation's cybersecurity."[47] The Pentagon and DHS pledged to work together in this area; the Pentagon signed an order for the military to defend its own networks and directed the creation of the U.S. Cyber Command in June 2009 to execute this task and conduct potential offensive operations in cyberspace.

Like Moonlight Maze, the classified nature of Agent.btz created information barriers to response. Interviewees recalled that everything was classified at the time. These officials said that they had to tell people what to do but could not tell them why. Some of those involved in the initial response did eventually receive access to information to understand the potential danger. Unlike Moonlight Maze, the tactic to counter Agent.btz made people uncomfortable because it involved allowing the malware to persist long enough to determine how it operated and to develop a countermeasure to shut it down. "We had to use a different tactic to counter the intrusion," one interviewee explained, "let it go, let it communicate with the listening post, propagate, send out the message, so that we could track it and put it to sleep."[48] Countering this malware forced the response teams to expand their circle of knowledge and to use nontraditional defense techniques. The NSA had been aware of Agent.btz prior to its infecting DoD computers and was able to develop a countermeasure and deploy it quickly. The more traditional approach of developing a signature to load into antivirus software was seen as too slow and unlikely to provide lasting protection because the adversary continually modified the malware to evade detection.

As with Moonlight Maze, the debate over who was responsible for Agent.btz also went on. One interviewee remembered intelligence assessments that determined the origins of the malware with high confidence. Yet opinions were split over whether the intrusion was deliberate and what the adversary intended to achieve. One interviewee believed that the malware was intended "as a control mechanism in Eastern Europe" and not as a deliberate attempt by the Russians to penetrate classified U.S. networks. "We did this to ourselves," the interviewee noted, alluding to the fact that poor cybersecurity practices caused the malware to be introduced into classified networks.[49] Another official concluded that the Russians were using the malware to gather intelligence on U.S. operations in Afghanistan.

Agent.btz was also still a case of espionage, and the response options were seen as constrained because "we do it too."[50] Post-Agent.btz assessments also concluded that the U.S. government needed to get better at defense, because it's "not that hard" and "it gives you more options for deterrence."[51] However, although the United States has a variety of legal, diplomatic, intelligence, law enforcement, financial, and military options, it is difficult to support an offensive military option. As one interviewee said, the United States is "worried about

[47] Nakashima, 2011.

[48] Interview with former senior official, 2021.

[49] Interview with former senior official, 2021.

[50] Interview with former senior official, 2021.

[51] Interview with former senior official, 2021.

throwing stones when you're living in a glass house."[52] Interviewees also noted that incidents like this continue to happen and are handled in a more routine manner, although much of the response may not be readily apparent.

In contrast to the response to Moonlight Maze, Russia's response to Agent.btz officially denounced the allegation that Russia may have been involved, emphasized Russia's commitment to international law and order, and berated the United States for not doing the same.[53] On December 4, 2008, the Russian Ministry of Foreign Affairs announced that Russia is "actively promoting the idea of forming a universal international legal regime of ensuring information safety that corresponds to the interests of each member of the international community." The statement also noted that the United States voted against adopting the Russian draft resolution to this effect at the 63rd session of the United Nations General Assembly.[54]

Despite the many similarities between U.S. responses to Moonlight Maze and Agent.btz, Agent.btz employed an intrusion tactic different from that in Moonlight Maze (using removable storage media to deliver the malware) and against a new set of targets (secure, classified military computer networks) prompting the need for an improvised operational solution and response. It appears that the poor cybersecurity practices, such as using removeable media to transfer files back and forth between classified and unclassified networks, led decisionmakers to conclude that the incident was as much the United States' fault as Russia's—therefore, a strong response would be seen as inappropriate. The lack of a holistic information picture was also still a problem. Interviewees emphasized that they needed to see the whole network but could not because of the federated nature of DoD networks. "We don't have a radar picture for cyber," one interviewee noted, "every attack is a surprise."[55] Additionally, because Agent.btz and the response to it were classified at the time, to the public it may have seemed that the United States did not take more aggressive action to respond to the adversary.[56] Yet Russia released a strongly worded public statement denying involvement in the intrusion and condemning the United States for suggesting such involvement. At the same time, interviewees indicated that the experience of Operation Buckshot Yankee prompted then–Secretary of Defense Robert Gates to direct the creation of Cyber Command, bringing together the defensive mission of Joint Task Force-Global Network Operations and the offensive mission of Joint Functional Component Command–Network Warfare, building on the cryptologi-

[52] Interview with former senior official, 2021.

[53] It should also be noted that by this point, the Russian presidency had transitioned from Boris Yeltsin during the Moonlight Maze incident to Vladimir Putin during Agent.btz.

[54] Ministry of Foreign Affairs of the Russian Federation, "Kommentarii Departamenta Informatsii I Pechati MID Rossii v Sviazi s Soobsheniyami SMI o Kiberatakakh na Komp'uterniye Seti Pentagona [Russian MFA Information and Press Department Commentary Regarding Media Reports about Cyber Attacks on Pentagon computer networks]," Moscow: Press-sluzhba [Press Department], December 4, 2008.

[55] Interview with former senior official, 2021.

[56] It is also unclear what impact this lack of public response may have had on the thinking of other actors, such as the Chinese government.

cal infrastructure of the NSA. The creation of Cyber Command prompted a reaction from Russia, whereas the actions undertaken to respond to Agent.btz were primarily defensive and not aimed at responding to Russian cyber activity.

Agent.btz was a concerning incident because it appeared on classified networks, and it was not initially clear whether the migration to those networks was intentional or the adversary had been able to exfiltrate classified information. The uncertainty surrounding the adversary's intentions, followed by the realization that the incident was as much the result of poor cybersecurity practices, led policymakers to constrain the overall U.S. response, focusing largely on remediation of networks and implementing new policies to try to prevent similar incidents in the future. According to interviewees, the incident was a motivation for creating Cyber Command from the two legacy cyber operations organizations, which did signal to U.S. adversaries that the United States was becoming more serious about treating cyberspace as an operational domain. The creation of Cyber Command, however, did not have an appreciable impact on Russian cyber espionage.

White House and State Department

Sometime before October 2014, APT actors compromised State Department networks, then penetrated White House computer systems and gained access to unclassified but sensitive information, including President Barack Obama's emails and his schedule.[57] Officials did not disclose the number or sensitivity of President Obama's compromised emails.[58] As a result of the compromise, the White House and the State Department partially shut down their email systems, forcing officials involved in the Iranian nuclear negotiations in November 2014 to maintain contact through personal email accounts. The intrusion was routed through computers around the world and was considered to be "among the most sophisticated attacks ever launched against U.S. government systems," according to unnamed government sources.[59]

The precise time frame of the State Department breach is unknown. Our interviews indicated that first alerts of the intrusion came from the intelligence community. The White House noticed suspicious activity on its network in early to mid-October 2014 and evicted

[57] Thomas Brewster, "Russians Hacked White House via State Department, Claims Report," *Forbes*, April 8, 2015; Michael M. Schmidt and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *New York Times*, April 26, 2015; and David Jackson and William M. Welch, "CNN: Russians Hacked White House Computers," *USA Today*, April 7, 2015.

[58] Schmidt and Sanger, 2015.

[59] Evan Perez and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House," CNN, April 8, 2015.

hackers from its email system at the end of October 2014.[60] However, some media outlets cited sources that believed the hackers were still in the State Department network in April 2015.[61]

Public attribution was conflicting and inconsistent. Private cybersecurity firms have named the APT group CozyDuke (also known as The Dukes, CozyBear, CozyCar, and Office Monkeys) as the perpetrators of this intrusion.[62] Administration officials declined to attribute the intrusion to or blame it on Russia.[63] Government investigators from the FBI, U.S. Secret Service, and the U.S. intelligence community "found tell-tale codes and other markers" that they believed belonged to "hackers working for the Russian government."[64] Other government officials quoted in media reports referenced Russia's involvement but stopped short of direct attribution. One official cited "Russian hackers" in the State Department case.[65] Other anonymous sources thought "the attack was consistent with a state-sponsored effort," and that the U.S. government believed Russia was "one of the most likely threats."[66] "Russian hackers" or "Russian-backed hackers" were the likely culprit, according to media reporting.[67] In addition to lack of public attribution, a news outlet reported in April 2015 that senior White House officials knew about the intrusion for months before publicly confirming that the compromises had occurred the previous year.[68]

The official U.S. response did not help clarify matters. The Obama administration refused to reveal its conclusions about who was responsible for the intrusion.[69] Federal investigators concluded that "it's not in our best interests to identify the entity that may be responsible for the specific activity of concern."[70] Subsequent White House statements and press releases did not address responses to these compromises. However, on January 13, 2015, the White House issued a press release on new cybersecurity efforts and an Executive Order on April 1, 2015, on cyber-enabled activities.[71] Whether the State Department and White House compromises motivated these efforts in some way is unclear, but the timing indicates some potential link.

---

60 Brewster, 2015.

61 Perez and Prokupecz, 2015.

62 Kurt Baumgartner and Costin Raiu, "The CozyDuke APT," *Securelist by Kaspersky*, April 21, 2015. CozyDuke may be the same as APT29, which has been affiliated with Russian intelligence.

63 Jackson and Welch, 2015.

64 Brewster, 2015.

65 Perez and Prokupecz, 2015.

66 "White House Computer Network 'Hacked,'" BBC, October 29, 2014.

67 Perez and Prokupecz, 2015; Jackson and Welch, 2015; Brewster, 2015.

68 Schmidt and Sanger, 2015; and Jackson and Welch, 2015.

69 See, for example, Schmidt and Sanger, 2015.

70 White House spokesman Josh Earnest as quoted in Schmidt and Sanger, 2015.

71 White House, Office of the Press Secretary, "Securing Cyberspace—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," press release, Washington, D.C., January 13, 2015; and Barack Obama, *Executive Order—Blocking the Property of Certain Persons Engaging in*

According to our interviews, the accesses and tools used during this intrusion were not destructive and seen as clearly for an intelligence operation. Thus, like Moonlight Maze and Agent.btz before it, these compromises were "very concerning" but still viewed as traditional nation-state espionage. This factor limited the options for response.[72] Interviewees also indicated that the concerns over potential escalation constrained decisionmaking. They said the United States does not have experience with "what escalation looks like in cyberspace . . . what things trigger what kind of responses."[73] Interviewees observed that if the United States publicly acknowledges that a nation state was responsible for the intrusion, it would "be under pressure to take action."

Our interviewees also noted that, in this case, the suspected adversary fought attempts to eject it from the compromised networks. The adversary did not disappear from the networks but maintained access and "did it aggressively," as one interviewee put it.[74] This was a change in behavior from previous intrusions. Another difference from Moonlight Maze and Agent.btz was that two U.S. government agencies were countering a cyber intrusion by the same actor almost simultaneously. These incidents led one interviewee to conclude that the United States "needed to get most federal agencies out of the business of trying to do their own cybersecurity." The interviewee concluded from this case that "we needed to do with cybersecurity what we've done with other government services . . . centralize cybersecurity services across the government."[75] This conclusion echoed the sentiment interviewees expressed about Agent.btz that protecting the U.S. cyberspace is inherently a government responsibility.

Russia was quiet during this incident. One Russian media source reported in three short paragraphs that the White House officially confirmed that hackers accessed its unclassified computer system.[76] The article further noted that a representative of the White House admitted in fall 2014 that "unknown entities" hacked into its computer network and that U.S. media had reported that the hackers were associated with Russia's government. The Russian Federation did not issue an official response to this incident. Further investigations and action may also have been overcome by the discovery of the compromise of the OPM records (more on this incident in Chapter Four).

The infiltration of White House and State Department networks was a significant concern for the Obama administration but did not lead to any significant response actions beyond economic sanctions on individual actors. The United States tried to eject the adversary, who

Significant Malicious Cyber-Enabled Activities, Washington, D.C.: White House, Office of the Press Secretary, April 1, 2015.

72 Interview with former senior government official, 2021.

73 Interview with former senior government official, 2021.

74 Interview with former senior government official, 2021.

75 Interview with former senior official, 2021.

76 "Beliy Dom Priznal Vzlom Komp'uternoy Seti Osen'u 2014 Goda [The White House Admitted Its Computer System Was Hacked in the Fall of 2014]," *Real'noye Vremya* [*Real Time*], May 4, 2015.

fought back against these efforts in a new evolution of adversary behavior. There were not any overt responses to Russian activity, and this lack of response does not appear to have had any impact on Russian behavior.

U.S. Government Policy Response Considerations

The Russia case studies showed that the U.S. government did not have a standing, overarching policy response to cyber espionage during the two decades in which the incidents in question occurred. Instead, following each incident, the government constructed an ad-hoc response that depended on the scope of the intrusion, the sensitivity of the targets involved, and the variety of missions of the government agencies that may have had a role in responding to such an incident; however, the response did not appear to account for the history of adversary activity predating each incident. Yet each response essentially encompassed similar actions. Each incident also revisited the debate over who should oversee protecting government networks and who was in charge of responding to the incident. For example, some people thought that the FBI should not have anything to do with cyber espionage cases, that this was an intelligence mission and not a law enforcement mission.[77] Our interviewees, however, concluded that both intelligence and law enforcement agencies should have their missions focus on coordinating and responding to these events.

Senior officials were also concerned that certain responses might be viewed as disproportionate or escalatory, yet they had no idea about, and could not agree on, what a proportionate response should be. The United States' use of cyber operations to conduct espionage was a common reason cited for the hesitation to respond. Thus, U.S. policies in cyberspace created a situation in which "[the United States doesn't] have the standing to take countermeasure against countries that engage in espionage against [it]."[78] Yet when pressed to consider whether other options, such as counterintelligence operations, should be considered, the interviewees conceded that a lack of robust and consistent response also encourages future adversary operations.

Impacts on Russian Behavior

If Russia or Russian government–backed actors were responsible for all three intrusions, then U.S. and Russian experiences with these incidents do not appear to have had any deterrent effect on the attackers. Instead, the attack vectors became progressively more creative and brazen. The attackers also chose riskier targets (e.g., classified military systems and presidential communications) that could have produced bigger rewards. As one interviewee noted,

[77] Interview with former senior official, 2021.

[78] Interview with former senior official, 2021.

"If we compare Russian activity today to back then, it's 100 times more. They're still doing it, doing it effectively, and indiscriminately through the supply chain."[79]

These and subsequent incidents also showed that past responses did not deter future Russian cyber espionage attempts. In the Moonlight Maze intrusion, the United States directly asked Russia for help. Russia denied any wrongdoing but noted that the websites from which the attacks originated were inactive. Following Agent.btz, the United States did not publicly acknowledge or attribute the intrusion, yet Russia publicly and strongly denounced the allegation that it was the culprit of the attack and blamed the United States for not doing more to support international legal standards in this area in the first place. Finally, after the 2014 intrusion incidents, both the United States and Russia avoided making public statements. President Obama issued sanctions against "certain persons engaging in significant malicious cyber-enabled activities,"[80] but these actions do not appear to have altered Russian behavior.

On the other hand, being quiet and stealthy used to be the defining characteristics of Russia as a cyber actor. Our interviewees recalled that Russia endeavored to avoid attribution: "It appeared to be important to Russia to be quiet and not get caught."[81] At some point, this priority changed. Some of Russia's activity got noisier and more aggressive as one interviewee described Agent.btz, to the point that Russia may deny responsibility more for show than because a denial will convince others.

Implications for Future Responses

The U.S. experience with Russian cyber espionage incidents has revealed several challenges that have implications for future policy responses:

- U.S. intelligence collection operations in cyberspace made the United States reluctant to respond to similar adversary activities. Strengthening U.S. cyber defenses was seen as the only practical response, yet it clearly has not prevented compromises from recurring. Reducing U.S. cyber intelligence collection might be considered to establish an international norm against large-scale cyber espionage, but this approach comes with the risk of reducing U.S. insights into adversary activity with no guarantee that the other side will reciprocate.
- Classification barriers between the intelligence community and the rest of the government hindered response, particularly in earlier cases, although the relationship and operating mechanisms across government have improved in recent years. Understanding the intent behind the intrusions was important to operators and law enforcement entities to be able to craft an appropriate response.

[79] Interview with former senior official, 2021.

[80] Obama, 2015.

[81] Interview with former senior official, 2021.

- Lack of a centralized view of government networks precluded better defense and quicker response. As the SolarWinds incident demonstrated, however, centralization carries its own risks and can lead to broader effects across multiple organizations when vulnerabilities are discovered and exploited.

The lack of clear guidelines for which activities are acceptable in cyberspace and which are not created confusion over what the appropriate response should be. Following Agent.btz, President Obama publicly stated that all nations conduct espionage operations.[82] Our interviewees echoed this theme: "Certain things are acceptable between adversarial states." Many of our interviewees also agreed that the best response is to have clear guidelines for which activities are acceptable in cyberspace and which are not. Clear definitions for *intelligence collection operations* must underpin these guidelines: "If it's not an intelligence collection operation, then you shouldn't be doing it." But when it is, policy options and their impact on future incidents have been limited and inconsistent. All these years later, these incidents show that the risks of not thinking through and planning for responding consistently to foreign cyber espionage operations in U.S. government systems are significant, and "we're not ready as a nation."[83]

[82] "Hollande, Obama Discuss Latest US Spying Allegations," France24, October 22, 2013.

[83] Interview with former senior official, 2021.

CHAPTER FOUR

China Case Studies

Titan Rain

Chinese cyber-enabled espionage in the early 2000s gained prominence with the Titan Rain series of cyber incidents, which began in the early 2000s.[1] Cybersecurity researcher Thomas Rid, drawing on leaked NSA documents, affiliated parts of Titan Rain to China's People's Liberation Army (PLA) Unit 61398, the subject of a notable report by cybersecurity firm Mandiant in 2012.[2] Chinese actors accessed unclassified information across many organizations, including DoD, Department of State, NASA, DHS, Department of Energy, Department of Commerce, Army Information Engineering Command, Defense Information Systems Agency, U.S. Army Space and Strategic Command, Army Aviation and Missile Command, and defense contractors, as well as the United Kingdom's Ministry of Defence, Foreign Office, and House of Commons.[3]

At that time, U.S. government officials considered the Titan Rain incidents "to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced."[4] The full scale of Titan Rain has not been publicly disclosed. However, in 2006, Air Force Maj Gen William Lord acknowledged that 10 to 20 terabytes of data were stolen from DoD's Nonclassified Internet Protocol Router Network (NIPRNet).[5] In addition to such technical information as aviation mission planning software and schematics for aerospace pro-

[1] Sean Bodmer, Max Kilger, Gregory Carpenter, and Jade Jones, "State of the Advanced Cyber Threat," in *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, New York: McGraw Hill, 2012.

[2] Council on Foreign Relations, "PLA Unit 61398," webpage, undated-c. See also Thomas Rid [@RidT], "Very impressive NSA attribution of TITAN RAIN to China, 3PLA, in 2007 -- required advanced nation-state capabilities," Twitter post, October 25, 2015; however, in 2005, Shawn Carpenter, a network security analyst at Sandia National Laboratory, traced Titan Rain infiltrations back to Guandong province, which is more than 1,200 kilometers from where Unit 61398's headquarters in Shanghai had been pinpointed. See Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005.

[3] Council on Foreign Relations, "Titan Rain," webpage, undated-d; Gary Adkins, "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism," *Journal of Strategic Security*, Vol. 6, No. 3, Fall 2013.

[4] Thornburgh, 2005.

[5] Adkins, 2013.

pulsion systems, the actors appeared to be interested in learning more about U.S. military strategy and doctrine.[6]

The Titan Rain incidents were the first publicly known Chinese state–sponsored cyber espionage events against the United States, although U.S. government officials were reluctant to publicly attribute it to China, while privately noting the significant breadth and scope of the Titan Rain incidents.[7] China publicly denied responsibility, calling the private accusations "totally groundless, irresponsible and unworthy of refute."[8] The lack of an explicit attribution to the Chinese government (and the strong denial by the Chinese government) constrained the development of response options. One interviewee characterized the government response to the early stages of the incident as confused and panicked.[9] Absent any damage beyond loss of data, policymakers felt that strong responses, including military action, would not be proportionate, nor did they seriously consider hacking back or hunt operations.[10] However, Titan Rain like Moonlight Maze signaled that foreign governments were beginning to develop sophisticated cyber-related capabilities that could pose a danger to U.S. systems.[11] This factor translated into a growing recognition for the role that cyber plays in national security issues and the need for heightened awareness in the cyber domain.

Titan Rain itself appears to have resulted in little direct response, although it is unclear from public records what actions FBI and Army intelligence investigations into the incidents may have prompted.[12] Policymakers noted that the roles, responsibilities, and authorities for response were unclear. There were not established precedents for which authorities could and should be used for response.[13] Additionally, the capacity and capability for response at that time resided primarily in the intelligence agencies (e.g., NSA), but were not available for military response in cyberspace and the authorities to do so were unclear even if policymakers had wanted to respond using traditional military activity. Domestically, the George W. Bush administration established the Comprehensive National Cybersecurity Initiative in 2008 to better strengthen cyber security across government systems, including through developing systems across government departments and agencies to detect and prevent intrusions.[14] The initiative included efforts to expand cybersecurity education, identify critical technologies,

6 Interview with senior official, 2021; Thornburgh, 2005.

7 Council on Foreign Relations, undated-d; Thornburgh, 2005.

8 Thornburgh, 2005.

9 Interview with former senior official, 2021.

10 Interview with former senior official, 2021.

11 Interview with former senior official, 2021.

12 Thornburgh, 2005.

13 Interview with former senior official, 2021.

14 Joshua E. Duke, "Cyber World War: The People's Republic Of China, Anti-American Espionage, and the Global Cyber Arms Race," *Global Security Review*, October 7, 2020.

and coordinate research and development efforts.[15] There is little indication that the United States took any response measures intended to influence the Chinese government's behavior, and Chinese cyber activity grew in scope and scale in subsequent years.

Office of Personnel Management

In March 2014, DHS's United States Computer Emergency Response Team detected a third-party actor actively exfiltrating information from OPM's network.[16] A second actor in May 2014, previously undetected, had also entered OPM's network and begun exfiltrating information later that year. The second actor was only identified in April 2015, at which point the full scale of the incident started to become evident.[17]

Malicious actors exfiltrated 4.2 million current and former government employee personnel files, 21.5 million records on security clearance background investigation information, and 5.6 million fingerprint records. These data included information on individuals outside government, such as children and family members. More than 2,000 pieces of malware were found to have infected 10,250 OPM devices. The magnitude of this breach shocked many across the intelligence, defense, and policymaking communities. A former NSA official said, "What is done is done and it will take decades to fix," and former CIA Director Michael Hayden said the exfiltrated OPM data remain "a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[18] Hayden also added, "I don't blame the Chinese for this at all. If I [as head of the NSA] could have done it, I would have done it in a heartbeat. And I would have not been required to call downtown, either [to seek White House permission]." Former National Intelligence Director James Clapper "expressed grudging admiration for the OPM hack, saying U.S. spy agencies would do the same against other governments."[19]

Government officials quickly attributed the compromise to Chinese actors by matching the tactics, techniques, and procedures used in the OPM incident with those used in previous Chinese cyber operations.[20] The majority of effort was spent trying to understand the implications and fallout from this data breach.[21] There was also a broad consensus across the

[15] White House, "The Comprehensive National Cybersecurity Initiative," webpage, undated.

[16] Jason Chaffetz, Mark Meadows, and Will Hurd, *The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation*, Washington, D.C.: U.S. House of Representatives, Committee on Oversight and Government Reform, September 7, 2016.

[17] Chaffetz, Meadows, and Hurd, 2016.

[18] Chaffetz, Meadows, and Hurd, 2016.

[19] Ellen Nakashima, "U.S. Decides Against Publicly Blaming China for Data Hack," *Washington Post*, July 21, 2015.

[20] Interview with former senior official, 2021.

[21] Interview with former senior official, 2021.

intelligence community and policymakers that this incident was an intelligence and espionage operation rather than an offensive attack by a foreign country. The United States did not publicly attribute the attack to China, in part because it likely would have required revealing some of its own cyber and intelligence capabilities.[22] China showed no apparent intent to modify data or permanently damage systems, nor were there any kinetic or physical consequences, which also contributed to the conclusion that the compromise was for espionage purposes, though of a massive scale.[23]

The categorization of the incident as an intelligence operation quickly reduced the number of policy responses available, although a wide variety of diplomatic, economic, and operational options were considered.[24] Within the U.S. government there was uncertainty whether there should be any type of response because the incident fell within the bounds of a traditional intelligence operation. Policymakers were concerned that a strong response would set a precedent for how foreign states respond to cases when the U.S. conducts its own cyber operations, especially when U.S. intelligence agencies would have executed the same operation against foreign governments if the opportunity presented itself.[25]

The OPM incident came at a critical point in U.S.-China relations when the two countries were preparing for a summit meeting between Presidents Barack Obama and Xi Jinping. Although the U.S. government did not make public its conclusion that China was responsible for the OPM incident, multiple senior government officials made it clear in private meetings with their Chinese counterparts their belief that China was responsible. The Chinese government denied responsibility, but when U.S. officials said that the United States was contemplating imposing sanctions on China for widespread espionage (including industrial espionage), China quickly dispatched a high-level delegation to Washington, D.C., to hammer out a deal.[26] This put the White House in a position to extract key concessions from China on cyber issues which laid the groundwork for the broader Obama-Xi agreement on a variety of topics.[27] On cyber specifically the statement noted agreement in the following areas:

- The two countries agreed to timely response to requests for information on malicious cyber activities and to cooperate on investigating cybercrimes.
- Neither country's government will participate in cyber-enabled theft of intellectual property with the intention to gain a commercial advantage.
- Both agreed to a commitment to work toward identifying and promoting norms of behavior in cyberspace.

---

[22] Nakashima, 2015.

[23] Interview with former senior official, 2021.

[24] Interview with former senior official, 2021.

[25] Interview with former senior official, 2021.

[26] Interviews with former U.S. government officials, 2021.

[27] Interview with former U.S. government official, 2021.

- Both support establishing a high-level joint dialogue mechanism for fighting cybercrime related issues.[28]

The agreement did not extend to cyber-enabled espionage targeting government systems, but the agreement on intellectual property theft represented a considerable Chinese concession.

After the summit, the U.S. government lacked any clear enforcement mechanism or method to measure changes in Chinese behavior. The Chinese government initially responded positively to requests for assistance in investigating cybercrime cases, but that cooperation quickly dissipated. Cyber-enabled economic espionage decreased markedly in the months following the agreement, particularly from groups targeting the United States and other Western partners.[29] To monitor Chinese compliance with the agreement, the U.S. government relied on assessments from the private sector (usually in regular roundtable discussions) and the intelligence community.[30] Since 2016, however, Chinese cyber activity has increased.[31] Some sources suggest that the exposure of Chinese cyber operations generated by the United States and its partners forced China to reduce its active cyber operations and to reassess how its wide variety of government and military organizations were conducting them. It is also possible, as some interviewees noted, that the Chinese leadership recognized that some of its cyber units were engaging in wanton and potentially counterproductive behavior, which warranted bringing them under tighter control. Ultimately, this effort led to a centralization of cyber operations highlighted by the creation of the Strategic Support Forces that combined China's military cyber units with its space, electronic warfare, and psychological operations capabilities.[32] The benefits of cyber-enabled espionage and growing Chinese confidence appear to have overridden the benefits that China perceived it derived from the Obama-Xi agreement.

U.S. Government Policy Response Considerations

Chinese actors have actively pursued access to U.S. government systems since at least the early 2000s, if not before. Both incidents examined here are similar in that they involved exfiltration of sensitive but usually unclassified information from government systems. Neither incident involved the compromise of classified systems, but the information collected had the potential for grave effects to U.S. national security. Despite both incidents being cases of cyber espionage, evaluating the scale and magnitude of these cyber incidents provides

[28] White House, Office of the Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States," press release, Washington, D.C., September 25, 2015a.

[29] FireEye iSight Intelligence, *Red Line Drawn: China Recalculates Its Use of Cyber Espionage*, Milpitas, Calif., June 2016.

[30] Interview with former senior official, 2021.

[31] CISA, "China Cyber Threat Overview and Advisories," webpage, undated.

[32] FireEye iSight Intelligence, 2016.

one approach to characterizing each incident, establishing response options, and delineating between each incident. In comparing the Titan Rain and OPM incidents, the scale and magnitude of the former took the form of tens of terabytes of unclassified technical data. In the OPM case, however, the damage could have been far greater given the potential ways the Chinese could use the information, including information to exert influence on individuals in sensitive positions in government. The OPM case also affected millions of Americans who were not directly in the employ of the U.S. government, such as family and friends of government employees.

This difference in scale and magnitude was the primary driver in why the White House at the time pressed their Chinese counterparts significantly and threatened enacting sanctions, while in the case of Titan Rain no high-level pressure was applied to the Chinese government to extract changes in behavior.

Effects on Chinese Behavior

The unique circumstances and timing surrounding the OPM incident and the meeting between President Obama and President Xi are unlikely to reappear in the future, but important insights can be gained. First, in responding to cyber incidents the nature of the actor needs to be considered. In the OPM case, at the time President Xi was particularly sensitive to the perception of China's global image and reputation. Knowing this, the U.S. government was able to compel China to change its behavior on several issues, albeit some of these changes in behavior were temporary and unenforceable. The lack of any concerted response to the Titan Rain compromise did not diminish Chinese cyber operations and may have even emboldened China to expand its operations.

Implications for Response in the Future

Several interviewees indicated that they considered the Obama-Xi agreement a unique occurrence given the nature of U.S.-Chinese relations at the time and the motivations driving Chinese desire for a successful summit. Interviewees speculated that circumstances today would be much different, and China would be less likely to concede to U.S. demands. The OPM breach prompted significant debate on the potential damage to U.S. national security stemming from the breach, and a simultaneous shrugging of shoulders and grudging admiration of the sheer scale of the Chinese operation. Titan Rain served as something of a wake-up call to policymakers who at the time in 2005 likely saw China as a relatively unsophisticated cyber actor.

Yet the OPM case demonstrates that diplomatic efforts can yield at least short-term benefits, if the circumstances allow, and the United States takes full advantage of them. A lack of response in the Titan Rain incident also appears to have given China additional motivation to continue and expand its espionage activities, including the broader theft of intellectual property from the U.S. private sector. Therefore, no response is a response in itself.

CHAPTER FIVE

Conclusion and Recommendations

Clearly the benefits of cyber-enabled espionage continue to outweigh any perceived repercussions for such countries as Russia and China. The response options that U.S. policymakers consider for cyber espionage cases do not appear to have changed much over the past two decades—and, in some respects, they may be even more constrained today. Alternatively, simply shrugging the shoulders and concluding that cyber espionage is something the United States has to accept as a normal course of business and "because we do it too" is too fatalistic.

The SolarWinds incident prompted a great deal of activity in the U.S. government to plug the holes in its cybersecurity defenses. The Biden administration, like other administrations after prior cyber incidents, issued an Executive Order on U.S. cybersecurity priorities. It has directed federal departments and agencies to develop plans for migrating to a zero-trust architecture approach for operating and defending their networks.[1] Some interviewees felt that these priorities were misplaced and that most government agencies should "get out of the business of defending themselves" and instead outsource their cybersecurity entirely.[2] Clearly improving the cybersecurity posture of U.S. government systems is needed, but doing so is also insufficient to prevent future incidents. The United States must also consider additional measures, which we turn to now.

Increasing Diplomatic Efforts and Promoting Norms of Responsible State Behavior in Cyberspace

U.S. policies in cyberspace have created a situation in which the United States is reluctant to consider certain responses "because we do it [cyber espionage] too," and, therefore, the United States would likely lose more from reducing its cyber intelligence collection than it would gain from an agreement with China and Russia, if such an agreement could even be made and enforced. However, to build a better foundation for U.S. responses to cyber espionage, the international community can create clear guidelines for which activities are acceptable in cyberspace and which are not. This would not require the United States or its allies to abandon cyber espionage as a legitimate tool of statecraft, but it could put guardrails around what is considered targeted and focused intelligence-gathering as opposed to indiscriminate action.

---

1 Aaron Boyd, "Biden Administration Releases Draft Zero-Trust Guidance," *NextGov*, September 7, 2021.

2 Interviews with former senior government officials, 2021.

Notwithstanding the potential for conflating terms and concepts between cyber-enabled espionage and cyber attack, establishing norms is also beneficial in calling out indiscriminate or reckless use of cyber capabilities that affect organizations other than those the adversary seeks to target. A zero-day vulnerability that becomes known often leads to a spike in exploitation for that vulnerability before it can be mitigated, a circumstance seen clearly with the publicizing of the Microsoft Exchange Server vulnerabilities in March 2021.[3]

International norms of behavior in cyberspace have garnered a great deal of attention over the years, but the fragile consensus from the United Nations deliberations collapsed quickly, and it is not clear that countries, such as Russia and China, would necessarily live up to those norms absent some costs for noncompliance, especially costs imposed on a multilateral basis. It is instructive to examine the coordinated statements issued by the United States, the United Kingdom, the European Commission, and NATO calling out Chinese malicious cyber behavior exploiting the Microsoft Exchange Server vulnerabilities and its reliance on contract hackers in July 2021.[4] The Chinese Ministry of Foreign Affairs denied the allegations and pointed its finger back at the United States. Although this response may seem to undercut the value of a coordinated, multilateral diplomatic response to such incidents, it represents an important first step in taking a firmer stand against such activities.[5]

The United States demonstrated that it could work effectively with allies and partners to present a united front and call out more-concerning cyber operations that can have far-reaching and indiscriminate effects. Coordinated diplomatic efforts to call attention to this action should continue to be pursued, if nothing else than to force Russia and China to account for their actions and to emphasize that it is not just the United States that is concerned.

Actively Pursue Adversaries on U.S Government Networks and with Partners

The current circumstances in which the adversary has extended, persistent access to U.S. government networks and can exploit partner systems as infrastructure to support this access is a continuing concern. Whether the means of network access is sophisticated or rudimentary, failure to detect the adversary quickly means that the adversary has time to move through

---

[3] Sean Hollister, "Microsoft Was Warned Months Ago—Now, the Hafnium Hack Has Grown to Gigantic Proportions," *The Verge*, March 8, 2021.

[4] White House, Office of the Press Secretary, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," press release, Washington, D.C., July 19, 2021; Council of the European Union, "China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action Against Malicious Cyber Activities Undertaken from its Territory," press release, Brussels, Belgium, July 19, 2021; and North Atlantic Council, "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise," press release, Brussels, Belgium, July 19, 2021.

[5] Adam Janofsky, "China Accuses US of Launching Cyberattacks, Denies Microsoft Exchange Hack," *The Record*, July 20, 2021.

systems, identify critical information it wishes to exfiltrate, and can often cover up its tracks as it goes. Improving the cybersecurity posture of U.S. government systems and networks remains a priority and an enduring challenge. Better passive defenses are unlikely to prove sufficient against a determined adversary. The United States should expand and deploy its cyber hunt teams more broadly—a process that has slowly begun with new authorities that Congress bestowed on CISA.[6] This type of activity can also help our partners and allies, as Cyber Command apparently did in 2019 at the request of the government of Montenegro.[7] Some partners may not wish to have U.S. military or intelligence teams conduct such operations but may be more amenable to support from a civilian agency, such as CISA, or through commercial vendors that provide these services.

Employ Counterintelligence Techniques More Widely to Decrease the Benefits of Cyber Espionage

Several of the former government officials we interviewed pointed to the need for better, more-calibrated responses to these types of incidents but tellingly had few detailed, concrete recommendations. The role of more-active forms of counterintelligence, however, seems undervalued. These active forms could include employing deception techniques, such as honeypots, to attract the adversary to false information and support hunt operations as noted above. Deterrence by denial is an important and obvious area of focus and has been repeatedly emphasized after each incident. One way to decrease the value of cyber espionage to the adversary is to poison the well—creating false information and data that appear legitimate so that the adversary either is coming to the wrong conclusions based on the analysis or is confused as to what is real and what is fake.

Deception campaigns are complex to plan and implement well. The information and systems have to look real to the adversary and provide a lucrative, but not obvious, target. The lure cannot be too good to be true. For better or worse, however, the scale of information that the United States has left vulnerable likely lessens this challenge. The United States has made a significant amount of valuable information too readily exploitable. The first risk in pursuing deception campaigns is to ensure that we do not fool ourselves. The information has to be carefully crafted and seeded in our systems, but in a way that legitimate users do not accidently use it or make decisions based on it that could be detrimental. The second risk is that the information and data we want the adversary to steal should not lead to the kind of miscalculation or decisionmaking that would prove more dangerous to the security dynamic.

[6] Section 1720 of the fiscal year 2021 National Defense Authorization Act tasked DoD with developing a "framework for cyber hunt forward operations . . . to enhance the consistency, execution, and effectiveness of cyber hunt forward operations," and Section 1705 gave CISA authority to actively identify vulnerabilities on U.S. government networks, including through "no-notice" hunt operations (see Public Law 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, January 1, 2021).

[7] Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020.

Finally, operational security is critical to effective deception. The more people in on the trick, the greater the risk of inadvertent exposure. Given these considerations, the United States is more likely to benefit from judicious employment of deception campaigns when the calculus of benefit to risk is advantageous. This might include such areas as military technology in which U.S. adversaries have a great interest, and the United States could cause adversaries to either copy technology that is not quite correct or to make assessments of U.S. capabilities that the United States desires them to have.

Will any of these actions stop cyber espionage against the United States? It is highly unlikely that they will, but there is potential for constraining and limiting what is considered legitimate espionage and actively thwarting future incidents through action to limit their effectiveness and benefits.

Abbreviations

APT	Advanced Persistent Threat
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DoD	U.S. Department of Defense
FBI	Federal Bureau of Investigation
FSB	*Federalnaia Sluzbha Bizopastnoci* (Federal Security Service, Russian Federation)
IP	internet protocol
IT	information technology
JWICS	Joint Worldwide Intelligence Communication System
NASA	National Aeronautics and Space Administration
NIPRNet	Nonclassified Internet Protocol Router Network
NNSA	National Nuclear Security Administration
NSA	National Security Agency
OPM	Office of Personnel Management
PLA	People's Liberation Army (China)
SIPRNet	Secret Internet Protocol Router Network
UCG	Unified Coordination Group

References

Adkins, Gary, "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism," *Journal of Strategic Security*, Vol. 6, No. 3, Fall 2013, pp. 1–9.

Barnes, Julian, "Pentagon Computer Networks Attacked; The Cyber-Strike on Key Sites Is Thought to Be from Inside Russia," *Los Angeles Times*, November 28, 2008.

Batvinis, Raymond J., *The Origins of FBI Counterintelligence*, Lawrence, Kan.: University Press of Kansas, 2007.

Baumgartner, Kurt, and Costin Raiu, "The CozyDuke APT," *Securelist by Kaspersky*, April 21, 2015.

"Beliy Dom Priznal Vzlom Komp'uternoy Seti Osen'u 2014 Goda [The White House Admitted Its Computer System Was Hacked in the Fall of 2014]," *Real'noye Vremya* [*Real Time*], May 4, 2015.

Biden, Joseph R., Jr., *Executive Order Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation*, Washington, D.C.: White House, April 15, 2021a.

———, *Executive Order on Improving the Nation's Cybersecurity*, Washington, D.C.: White House, May 12, 2021b.

Bodmer, Sean, Max Kilger, Gregory Carpenter, and Jade Jones, "State of the Advanced Cyber Threat," in *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, New York: McGraw Hill, 2012, pp. 1–22.

Boyd, Aaron, "Biden Administration Releases Draft Zero-Trust Guidance," *NextGov*, September 7, 2021.

Brewster, Thomas, "Russians Hacked White House via State Department, Claims Report," *Forbes*, April 8, 2015.

Bridis, Ted, "E-Espionage Rekindles Cold-War Tensions—U.S. Tries to Identify Hackers; Millions of Documents Are Stolen," *Wall Street Journal*, June 2001.

Chaffetz, Jason, Mark Meadows, and Will Hurd, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, Washington, D.C.: U.S. House of Representatives, Committee on Oversight and Government Reform, September 7, 2016.

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Council of the European Union, "China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action Against Malicious Cyber Activities Undertaken from its Territory," press release, Brussels, Belgium, July 19, 2021.

Council on Foreign Relations, "Cyber Operations Tracker: Operations by Country," webpage, undated-a. As of March 10, 2021:
http://www.cfr.org/cyber-operations/

———, "Hellsing," webpage, undated-b. As of December 7, 2021:
https://www.cfr.org/cyber-operations/hellsing

———, "PLA Unit 61398," webpage, undated-c. As of September 2, 2021:
https://www.cfr.org/cyber-operations/pla-unit-61398

———, "Titan Rain," webpage, undated-d. As of September 2, 2021: https://www.cfr.org/cyber-operations/titan-rain

Cybersecurity and Infrastructure Security Agency, "China Cyber Threat Overview and Advisories," webpage, undated. As of October 26, 2021: https://us-cert.cisa.gov/china

Defense Science Board, *DSB Task Force Report on Cyber Defense Management*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2016.

Doman, Chris, "The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History," blog post, July 7, 2016. As of March 26, 2021: https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7

Drogin, Bob, "Yearlong Hacker Attack Nets Sensitive U.S. Data," *Los Angeles Times*, October 7, 1999.

Duke, Joshua E., "Cyber World War: The People's Republic of China, Anti-American Espionage, and the Global Cyber Arms Race," *Global Security Review*, October 7, 2020.

Duvenage, P. C., V. J. Jaquire, and S. H. von Solms, "Toward a Literature Review on Cyber Counterintelligence," *Journal of Information Warfare*, Vol. 17, No. 4, Fall 2018.

———, "A Cyber Counterintelligence Matrix for Outsmarting Your Adversaries," *Journal of Information Warfare*, Vol. 19, No. 1, March 2020.

FireEye iSight Intelligence, *Red Line Drawn: China Recalculates Its Use of Cyber Espionage*, Milpitas, Calif., June 2016.

Grant, Rebecca, "The Cyber Menace," *Air Force Magazine*, March 1, 2009.

Greenberg, Andy, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York: Anchor Books, 2020.

Guerrero-Saade, Juan Andres, Costin Raiu, Daniel Moore, and Thomas Rid, *Penquins Moonlit Maze: The Dawn of Nation-State Digital Espionage*, London: Kaspersky Lab, King's College London, 2017.

"Hack May Have Exposed Deep U.S. Secrets; Damage Yet Known," Associated Press, December 15, 2020.

"Hollande, Obama Discuss Latest US Spying Allegations," France24, October 22, 2013.

Hollister, Sean, "Microsoft Was Warned Months Ago—Now, the Hafnium Hack Has Grown to Gigantic Proportions," *The Verge*, March 8, 2021.

Jackson, David, and William M. Welch, "CNN: Russians Hacked White House Computers," *USA Today*, April 7, 2015.

Janofsky, Adam, "China Accuses U.S. of Launching Cyberattacks, Denies Microsoft Exchange Hack," *The Record*, July 20, 2021.

Joyner, Christopher C., and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law*, Vol. 12, No. 5, 2001, pp. 825–865.

Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster, 2016.

King, Angus, and Mike Gallagher, *United States of America Cyberspace Solarium Commission: Final Report*, Arlington, Va., March 2020.

Loeb, Vernon, "NSA Adviser Says Cyber-Assaults on Pentagon Persist with Few Clues," *Washington Post*, May 7, 2001.

Mandia, Kevin, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," *FireEye Stories*, blog post, December 8, 2020a. As of October 14, 2021: https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

———, "Global Intrusion Campaign Leverages Software Supply Chain Compromise," *FireEye Stories*, blog post, December 13, 2020b. As of October 14, 2021: https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

Maneki, Sharon A., *Learning from the Enemy: The GUNMAN Project*, 2nd ed., Fort George G. Meade, Md.: Center for Cryptologic History, National Security Agency, 2018.

Mazzetti, Mark, and Michael S. Schmidt, "Two Russian Compounds, Caught Up in History's Echoes," *New York Times*, December 29, 2016.

Miller, Maggie, "Lawmakers Ask Whether Massive Hack Amounted to Act of War," *The Hill*, December 18, 2020.

Ministry of Foreign Affairs of the Russian Federation, "Kommentarii Departamenta Informatsii I Pechati MID Rossii v Sviazi s Soobsheniyami SMI o Kiberatakakh na Komp'uterniye Seti Pentagona [Russian MFA Information and Press Department Commentary Regarding Media Reports about Cyber Attacks on Pentagon Computer Networks]," Moscow: Press-sluzhba [Press Department], December 4, 2008.

Mutisi, Tapiwa Matthew, "Microsoft President Brad Smith Calls SolarWinds Hack 'Act of Recklessness,'" *Innovation Village*, blog post, December 20, 2020. As of October 20, 2021: https://innovation-village.com/microsoft-president-brad-smith-calls-solarwinds-hack-act-of-recklessness/

Nakashima, Ellen, "Cyber-Intruder Sparks Response, Debate," *Washington Post*, December 8, 2011.

———, "U.S. Decides Against Publicly Blaming China for Data Hack," *Washington Post*, July 21, 2015.

Nakasone, Paul M., and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020.

National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America, 2020–2022*, Washington, D.C.: Office of the Director of National Intelligence, February 2020.

North Atlantic Council, "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise," press release, Brussels, Belgium, July 19, 2021.

National Security Council [@WHNSC45], "(1/3) Pursuant to Presidential Policy Directive-41 (26 July 2016) and its Annex, a Cyber Unified Coordination Group (UCG) has been established to ensure continued unity of effort across the United States Government in response to a significant cyber incident," Twitter post, December 15, 2020. As of February 7, 2022: https://twitter.com/WHNSC45/status/1338863139278913537

Obama, Barack, *Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, Washington, D.C.: White House, Office of the Press Secretary, April 1, 2015. As of April 26, 2021:
https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

Office of the Director of National Intelligence, *Annual Threat Assessment of the United States Intelligence Community*, Washington, D.C., April 9, 2021.

Pankov, Nikolay, "Moonlight Maze: Lessons from History," *Kaspersky Daily*, April 3, 2017.

Perez, Evan, and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House," CNN, April 8, 2015. As of March 30, 2021:
https://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html

Peters, Jay, "Microsoft President Sounds Alarm on 'Ongoing' SolarWinds Hack, Identifies 40 More Precise Targets," *The Verge*, December 17, 2020. As of May 23, 2021:
https://www.theverge.com/2020/12/17/22188060/microsoft-president-solarwinds-orion-hack-breach-brad-smith

Public Law 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, January 1, 2021.

Rid, Thomas [@RidT], "Very impressive NSA attribution of TITAN RAIN to China, 3PLA, in 2007 -- required advanced nation-state capabilities," Twitter post, October 25, 2015. As of October 26, 2021:
https://twitter.com/RidT/status/658222367139876864

Rogin, Josh, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012. As of October 26, 2021:
https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Sanger, David E., "Ignoring Sanctions, Russia Renews Broad Cybersurveillance Operation," *New York Times*, October 25, 2021. As of October 26, 2021:
https://www.nytimes.com/2021/10/25/us/politics/russia-cybersurveillance-biden.html

Schaap, Arie J., "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review*, Vol. 64, pp. 121–174, Winter 2009.

Schmidt, Michael M., and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *New York Times*, April 26, 2015.

Smith, Brad, "A Moment of Reckoning: The Need for a Strong Global Cybersecurity Response," *Microsoft on the Issues*, blog post, December 17, 2020. As of October 20, 2021:
https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Staten, C. L., "Warning; Internet Used by Foreign Intelligence Operatives," *ENN Daily Report*, December 9, 1996.

Stewart, Phil and Jim Wolf, "Agent.btz Worm Won't Die After 2008 Attack on Military," Reuters, June 17, 2011.

Stoll, Clifford, "Stalking the Wily Hacker," *Communications of the ACM*, Vol. 31, No 5, May 1988, pp. 484–500.

———, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, New York: Doubleday, 1989.

Thornburgh, Nathan, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005. As of October 26, 2021:
http://content.time.com/time/magazine/article/0,9171,1098961,00.html

Trump, Donald J., "Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Federal Register*, Vol. 82, No. 93, May 16, 2017, pp. 22391–22397.

———, *National Cyber Strategy of the United States of America*, Washington, D.C.: White House, September 2018.

U.S. Army, National Capital Region Field Office, "History of Army Counterintelligence," webpage, undated. As of October 26, 2021:
https://www.nec.belvoir.army.mil/902dNCRFO/history.asp

U.S. Senate, Select Committee on Intelligence, *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence*, Washington, D.C.: U.S. Government Printing Office, November 1, 1994.

Vistica, Gregory, "'We're in the Middle of a Cyberwar,'" *Newsweek*, Vol. 134, No. 12, September 20, 1999. As of April 5, 2021:
https://search.proquest.com/docview/214301319/5048099894B64A54PQ/8?accountid=25333

Wheeler, Tarah, "The Danger in Calling the SolarWinds Breach an 'Act of War,'" *TechStream*, March 4, 2021.

White House, "The Comprehensive National Cybersecurity Initiative," webpage, undated. As of September 2, 2021:
https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

———, "Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021," transcript, Washington, D.C., February 17, 2021. As of February 7, 2022:
https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/

"White House Computer Network Hacked,'" BBC, October 29, 2014. As of March 30, 2021:
https://www.bbc.com/news/technology-29817644

White House, Office of the Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States," press release, Washington, D.C., September 25, 2015a. As of September 2, 2021:
https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States

———, "Securing Cyberspace—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," press release, Washington, D.C., January 13, 2015b. As of April 26, 2021:
https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

———, "Fact Sheet: Cybersecurity National Action Plan," press release, Washington, D.C., February 9, 2016. As of October 21, 2021:
https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

———, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," press release, Washington, D.C., July 19, 2021. As of November 1, 2021: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

NATIONAL DEFENSE RESEARCH INSTITUTE

Cyber-enabled espionage against the United States has been a challenge for more than 20 years and is likely to remain so in the future. In the aftermath of the 2020 SolarWinds cyber incident that affected U.S. government networks, policymakers, lawmakers, and the public asked: "Why does this keep happening, and what can the United States do to prevent it from reoccurring?" It is these questions that motivate this effort. Specifically, this report summarizes three cases of Russian cyber-enabled espionage and two cases of Chinese cyber-enabled espionage dating back to the compromise of multiple government agencies in the late 1990s up to the 2015 compromise of the Office of Personnel Management. The purpose of this inquiry is to address whether U.S. responses have changed over time, whether they led to changes in adversary behavior, and what the United States can learn from these cases to inform future policymaking. The authors show that policymakers typically consider a narrow set of response options, and they often conclude that not much can be done beyond trying to improve network defenses, because the United States "does it too." The authors suggest that the U.S. government could broaden its policy response options by increasing focus on diplomatic engagement, including working with partners and allies to call out malicious cyber behavior; expanding the use of active defense measures to root out adversaries; and employing more-sophisticated counterintelligence techniques, such as deception, to decrease the benefits that adversaries derive from cyber espionage.

$15.00

ISBN-10 1-9774-0901-6
ISBN-13 978-1-9774-0901-0

51500

9 781977 409010

www.rand.org

RR-A1190-1