Disconnected:
Accessing The Obscured Legacy of The U.S. Intelligence Community's Cyber Operations

Caitlin St. John Mulvihill
Undergraduate Senior Thesis
Department of History
Columbia University
5 April 2023

Seminar Leader: Natasha Lightfoot
Second Reader: Anders Stephanson

Table of Contents

Acknowledgments

This thesis is the product of the unbelievable level of support I have been surrounded by over the past year. Firstly, this project would not have been possible without the encouragement of my seminar instructor Professor Natasha Lightfoot, whose brilliant insight and seemingly limitless ability to believe I could pull my myriad of cyber anecdotes into something compelling allowed me to believe it as well. I also am indebted to my second reader Professor Anders Stephanson for helping me to straighten out a narrative thread. The research for this project began in Professor Stephanson's international history seminar last spring, and I feel incredibly lucky to have gone through this process with guidance (and news links) from a scholar whom I admire so much. I must also extend my gratitude to Professor Matthew L. Jones, whose seminar on surveillance and advice during this project's earliest stages were foundational to this work. In my first semester at Columbia, I took a course taught by Professor Mamadou Diouf and Karim Malak. This class would prove to be a crash course in how to research and write history, and I am very grateful to them both for putting me on the path that led to this thesis.

To all my friends who have listened to me ramble on about cyberwar and watched me fill chalkboards with scrawled ideas, thank you for your patience and for being proud of me, no matter how unhinged I got. To my peer review group, thank you for your excellent feedback and your much-needed solidarity. I would also be remiss not to thank the entire Columbia Women's Basketball program for supporting me throughout this endeavor. Even though writing a history thesis from a hotel lobby in Kansas during the crunch of the final work week is perhaps a bit untraditional, there is truly nowhere I would have rather been, and no group of people I would have rather had cheering me on. Thank you for being my family.

Finally, thank you to my parents, whose lifelong support of my academic pursuits has led me to this point. Dad, thank you for instilling me with a love of history and being my perennial sounding board. Your advice and insight from the beginning through the eleventh hour of this thesis has meant the world to me. Mom, thank you for always encouraging me to pursue my interests. Thank you even more for believing in me through them all.

Glossary of Terms

This thesis makes extensive use of terms and acronyms that may be foreign to readers not familiar with the cyber field or U.S. intelligence operations. The inclusion of this glossary is intended to make the information contained herein as accessible as possible. Page numbers reference the first time the term is mentioned.

12333/Executive Order 12333: President Ronald Reagan signed this Executive order framing the U.S. intelligence effort in the Executive Branch in 1981 (p.17)

ARPANET: An early computer network; Department of Defense project beginning in 1966 (p.16)

Black hat hacker: A term for a hacker with criminal or malicious intent (p.27)

CNA: Computer Network Attack (p.19)

CNE: Computer Network Exploitation (p.20)

Cyber Command: U.S. unified combatant command for the cyberspace domain within the Department of Defense (p.47)

DoD: Department of Defense (p.8)

DEF CON: An annual convention in Las Vegas for the hacking community (p.26)

Equation group: A highly advanced and sophisticated cyber attack group identified by the Kaspersky group in 2015, thought to have been operational since as early as 1996; likely associated with the U.S. National Security Agency (p.45)

Exploit: Used in cybersecurity terms as a noun, a cyber tool that takes advantage of a system's vulnerability (p.13)

Fifth Domain: Term for the cyber domain of warfare (p.5)

FISC: Foreign Intelligence Surveillance Court (p.22)

IC: U.S. Intelligence Community (p.10)

IO: Information Operations (p.19)

IW: Information Warfare (p.19)

Malware: Portmanteau of 'malicious software,' software used by an attacker to infect a target system (p.6)

Metadata: Data regarding other data, often used for identification purposes (p. 22)

Moonlight Maze: A cyber attack levied on U.S. Department of Defense computer system in the late 1990s (p.40)

NSA: National Security Agency (p.7)

PPD-20: 2012 Obama-era Presidential Directive concerning U.S. Cyber Operations Policy (p.21)

SCADA System: Acronym for Supervisory Control and Data Acquisition Systems, a widely used industrial control system reliant on computers (p.5)

SIGINT: Short for 'Signals Intelligence,' or intelligence gathered from the interception of electronic signals or systems (p.10)

Stuxnet: Name of computer malware that was used in an attack on the Iranian Natanz Nuclear Facility discovered in 2010 (p.6)

USA PATRIOT Act/PATRIOT Act: Broad 2001 legislation that expanded U.S. intelligence methods, acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (p.42)

VEP: Vulnerabilities Equities Process, the governing U.S. policy on determining disclosure of a vulnerability (p.32)

Vulnerability: A flaw in a software's code (p.24)

White hat hacker: A term for an ethical hacker who acts with the intention of identifying security flaws (p.25)

Zero-day vulnerability: A vulnerability in a software completely unknown to its developer (p.25)

Introduction

On July 1st 2010, *The Economist* published a briefing titled "War in the Fifth Domain: Are the mouse and keyboard the new weapons of conflict?"[1] It imagined a future in which cyber attacks break down their targets with consequences as cataclysmic as a nuclear attack, but without the safeguard of mutually assured destruction and with the potential to be wielded by terrorists as easily as by nation states. The editors referenced one target in particular as the source of increasing security concerns: the computer systems that keep industrial plants running, or, more technically, supervisory control and data acquisition systems (SCADA systems). *The Economist* had an unnamed senior American military source who told the editors that "if any country were to be found planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis."[2]

Such a 'logic bomb' was not just a part of some future vision. It was already being dropped. At the same time that the article was being published, an attack on a control system was indeed being carried out at the Natanz Nuclear Facility in Iran. Early in 2010, Sergey Ulasen, a young anti-virus programmer at the small Belarussian computer security firm VirusBlokAda, was assigned a case where an Iranian customer had been experiencing random reboots and error screens on his computer. Instead of the basic software misconfiguration Ulasen expected, he found a web of connected software infections coded at a level beyond anything he had seen before. In hopes of sourcing explanations, VirusBlokAda published its findings on the Internet.[3]

---

[1] "War in the Fifth Domain," *The Economist*, July 1, 2010. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain, (accessed 12/14/22).

[2] *Economist*, "War in the Fifth Domain."

[3] Eugene Kaspersky, "The Man Who Found Stuxnet - Sergey Ulasen in the Spotlight," Nota Bene: Notes Comment and Buzz from Eugene Kaspersky (blog), Kaspersky, November 2, 2011, https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/, (accessed 3/22/22).

14 days after the publication of the *Economist* article, wildersecurity.com user "frank_boldewin" posted some of the code he had decrypted on the site's forum and made a startling observation: "this points me to the Siemens WinCC SCADA system. looks like this malware was made for espionage."[4]

The Natanz Nuclear Facility in Iran had been experiencing inexplicable breakdowns in its uranium enrichment centrifuges since 2008, with up to 10 percent being destroyed between November 2009 and January 2010.[5] The facility was reliant on the very same Siemens SCADA system that the code posted by VirusBlokAda was targeting. It became apparent that the very same malware (a portmanteau of 'malicious software'[6]) troubling Ulasen's Iranian client was also the cause of the shutdowns at the nuclear plant.[7] The client's computer system had simply been a stop on the virus' way toward its true target. The malware was dubbed "Stuxnet," and the news that a cyberattack of such magnitude had been carried out struck fear and confusion into the international political community. The Senate Committee on Homeland Security and Governmental Affairs held an investigative hearing in November of 2010 regarding "Securing Critical Infrastructure in the Age of Stuxnet," during which Maine Senator Susan Collins, a

---

[4] frank_boldewin, post to "Rootkit.TmpHider," malware problems & news, Wilder Security Forums, July 13, 2010. https://www.wilderssecurity.com/threads/rootkit-tmphider.276994/#post-1712134, (accessed 3/22/22).

[5] David Albright, Paul Brannan, and Chrstina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," Institute for Science and International Security, December 22, 2010. https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/, (accessed 3/29/22).

[6] *Computer Security Resource Center Glossary*, "malware", National Institute of Standards and Technology, U.S. Department of Commerce, accessed April 29, 2022, https://csrc.nist.gov/glossary/term/malware, (accessed 3/22/22).

[7] Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (The Langner Group, November 2013), https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

woman vocal about her belief in the necessity of strong tactics against Iranian nuclear proliferation,[8] gave an opening statement expressing her fear of the devastating potential of Stuxnet. She proclaimed to the Committee that the malware was evidently "the work of a well-financed team of experts with extensive knowledge of the targeting systems."[9] What neither she, nor the editing desk at *The Economist,* nor potentially even the publication's military source knew, was that the team of experts behind the attack were Americans, acting under the jurisdiction of the National Security Agency (NSA).

The United States government has never admitted to its role in the Stuxnet attack, but the evidence is nothing short of damning.[10] This operation is the subject of other academic and journalistic work and, while there is not the space here to chart the exposé, it prompts questioning the very nature of the tactical capabilities created by cyberspace. A country had planted a cyberattack on a SCADA grid, but no Cuban missile crisis equivalent occurred. The government responsible has not even discussed its own operation with members of Congress. Who is making the rules in this new space? Is it even most productively considered as an independent domain of war, or is it simply an added level of technological complexity to the pre-existing domains? And is that debate valuable to have in the first place?

---

[8] "Senator Collins Announces Position on Iran Nuclear Agreement," U.S. Senator Susan Collins Official Webpage, September 9, 2015, https://www.collins.senate.gov/newsroom/senator-collins-announces-position-iran-nuclear-agreement, (accessed 4/6/22).

[9] *Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century & Securing Critical Infrastructure in the Age of Stuxnet, before the Senate Committee on Homeland Security and Governmental Affairs*, 111th Cong., 2nd Sess., 40 (2010) (Statement of Ranking Member Senator Susan M Collins)

[10] Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israel experts, officials say," *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, (accessed 12/14/22).

This thesis will examine the paradoxes of American engagement with offensive cyber tactics by critically interacting with the existing scholarship and pressing further into primary sources. National Security Directives, policy language, Congressional hearings, and materials from private cybersecurity companies will all play a role in creating an understanding of how the U.S. government has interacted with cyberspace in an offensive capacity. Interrogating the specific rhetoric used while centering it in a wider political context will shed light on how cyberspace as a unique hybrid of military and intelligence undertakings has been shaped by the American Intelligence Community. Much of the existing historiography focuses on how the United States engages in cyber tactics and offers commentary on how its tactics can be shaped by the nature of cyber. However, as underscored by the debate of whether or not cyber can truly constitute a Fifth Domain of warfare, the field itself is a malleable, conceptual one. By critically analyzing American policy language not simply as products of the contemporary cyber world, but as shapers of it, this paper demonstrates that the U.S. has progressively tailored the world of cyber operations to its economic and geopolitical advantage and unpacks the paradoxes that have come to the surface as a result of this activity.

One year after *The Economist's* declaration of cyberspace as the Fifth Domain of warfare, the United States Government officially followed suit. In its July 2011 "Strategy for Operating in Cyberspace," the Department of Defense (DoD) stated that "Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions."[11] The four traditional domains of war (land, sea, air, and space) now included a fifth

---

[11] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: Department of Defense, July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

entry—cyber. One of these things is not like the others. The DoD conceptualized this Fifth Domain as entirely global, not bound by a physical environment in the way that the other four domains are, but instead by what it calls the "information environment."[12] The 'man-made' nature of cyberspace is understood by the U.S. government, but despite the difficulty in nailing down an exact set of boundaries, the DoD strategizes within it just as they would in the land, sea, air, and space domains.

The Fifth Domain is a contested one; some scholars argue that adding it to the list of warfare domains neglects to take into account the fact that cyber is a fundamentally different arena that permeates everything, rather than a clearly delineated physical space. The U.S. federal standard definition of cyberspace is an "interdependent network of informational technology infrastructures," with official language often listing the Internet, computer systems, and telecommunications networks, or electronic communications, as examples of what the domain contains.[13] The difference between this and the four physical environments of the other domains is quite clear. For example, it would be possible to conduct an operation on land without integrating the space domain, but no operations in the space domain would be possible without those information systems that make up cyberspace. Career Air Force officer and security scholar Michael P. Kreuzer argues that there really is no such thing as cyberspace, but rather "a metaphor to help humans understand the near instantaneous sharing of information across

---

[12] Catherine A. Theohary, *Defense Primer: Cyberspace Operations,* CRS Report No. IF10537 (Washington, DC: Congressional Research Service, Updated December 9, 2022), https://sgp.fas.org/crs/natsec/IF10537.pdf.

[13] "cyberspace," Computer Security Resource Center Glossary, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/glossary/term/malware, (accessed 4/29/22).

widespread computer networks."[14] However, regardless of a pinpointed definition, what is at the heart of any attempt to define the cyber realm is information.

Information has always been foundational to geopolitics. But even while it declares a Fifth Domain, the Department of Defense still frames cyber operations in such a way that obscures the fact that this seemingly theoretical theater is actually quite tangible. In a mission statement posted to NSA's website, it establishes a two-pronged purpose encompassing both "signals intelligence (SIGINT) insights and cybersecurity products and services."[15] The first prong, SIGINT, which refers to intelligence gathered from intercepting electronic signals or systems,[16] conjures the popular image of an intelligence agent with clunky headphones intercepting an enemy conversation, fervently compiling information to send off and use in an operation to prevent catastrophe. The second, cybersecurity, is instinctually associated with protecting American cybersystems from outside attacks, given its root of 'security.' Both of these endeavors equate to a defensive strategy, keeping the nation safe from any adversarial foreign actors. However, this takeaway from the NSA statement is missing an important truth—the 18 federal organizations that conduct intelligence and counterintelligence, collectively making up the U.S. Intelligence Community[17] (IC) are just as deeply involved in offensive cyber operations as defensive ones. What is advertised as 'information' is weaponized, both with and without the catalyst of kinetic operations. The Stuxnet operation, for example, was a cyber operation that

---

[14] Michael P. Kreuzer, "Cyberspace Is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age," The Strategy Bridge, July 8, 2021. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (accessed 12/20/22).

[15] "About NSA/CSS," National Security Agency/Central Security Service, https://www.nsa.gov/about/, (accessed 12/2/22).

[16] "Signals Intelligence (SIGINT) Overview," National Security Agency/Central Security Service, https://www.nsa.gov/Signals-Intelligence/Overview/, (accessed 12/2/22).

[17] "Members of the IC," Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/members-of-the-ic, (accessed 12/2/22).

caused real harm to its target, without the goal of collecting SIGINT or building protection around an existing American system. Despite the definitional fluidity, or perhaps more aptly, opacity, of cyber as a distinct Fifth Domain, it is nonetheless an arena with tangible consequences that can destabilize nations and international affairs.

Even if cyberspace is simply a metaphor, it is one that has been constructed by those operating within it. This paper is interested in understanding how the United States government has shaped the meaning and capacity of cyberspace, acting both offensively and clandestinely within it, while maintaining an image of pure defense. Leveraging frameworks of security and traditional espionage, the U.S. is entrenched in a deeply paradoxical arena. In one instance, an international order predicated on the Westphalian paradigm of state actors is infiltrated by unattached and anonymous hacking collectives. In another, the overclassification and stockpiling of offensive capabilities directly undercuts itself by leaving open weaknesses for adversaries to exploit.

The scholarship surrounding cyber warfare is actively trying to historicize and contextualize a concept that has been intentionally obfuscated by the intelligence community. The literature spans multiple fields; but given cyber's very recent emergence, rapidly changing nature, and high level of classification, a great deal of investigative revelations are coming from journalists. David E. Sanger, a journalist for *The New York Times* whose 2012 book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*[18] led to a federal investigation to determine his sources,[19] uncovered Operation Olympic Games, the codename

---

[18] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012).
[19] Josh Gerstein, "Court unseals details on Stuxnet leak probe," *Politico*, January 12, 2018, https://www.politico.com/blogs/under-the-radar/2018/01/12/stuxnet-leak-probe-court-unseals-details-337912, (accessed 4/29/22).

for the operation that launched the Stuxnet worm against the Natanz nuclear facility in Iran, and identified it as a joint undertaking between the United States and Israel. Another *Times* reporter, Nicole Perlroth, authored the commercially successful 2021 book *This is How They Tell Me the World Ends*, which traces the development of the cyber arms market.[20] Both Sanger and Perlroth's books are both important endeavors in expanding knowledge about cyberspace operations, but their journalistic nature situates them in a space more akin to primary sources than historical analyses. Because this field is dealing not only with quite recent events but also with ones that remain overwhelmingly classified, these writers are telling stories that are unavailable in government records, instead utilizing relationships they have built with sources inside tight-lipped groups, like NSA[21] and the hacking community. Critical historical analysis tends to be left largely to the reader, or to the writers' sources, whose quotations often provide a slant that journalists tend to shy away from in their own writing for the sake of integrity.

Apart from journalistic endeavors, there are more theoretical policy and legal approaches found throughout the literature as well. Sanger's work has touched on key themes that academics writing on the world of cyber warfare frequently grapple with, including the difficulties of determining how to defend potential targets when so many are privately-owned civilian infrastructures, the potential of cyber weapon capabilities juxtaposed with the track record of their use, and the comparison between the historical trajectories of nuclear and cyber capabilities. The merits of this last theme are frequently debated within the historiography, engaging with the applicability of deterrence (the strategy of discouraging enemy attack through a credible

---

[20] Nicole Perlroth, *This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race*, (New York: Bloomsbury Publishing, 2021).

[21] 'NSA' is used throughout this paper, rather than 'the NSA'; this serves as best practice in cyber scholarship and the lack of definite article is congruent with the language used by government officials.

retaliatory threat),[22] the role of public debate in an informed democratic process to balance federal powers, and the viability of international cooperation. This paper will engage less with the nuclear comparison, but rather a different comparison, one which this intervention argues is clearly favored by the U.S. government for largely strategic reasons—the comparison to espionage activities. Political scientist Thomas Rid is a major proponent of this comparison, arguing that conceptualizing cyber offensives as warfare is misguided, and they are indeed analogous to espionage.[23] In 2013, he published a book titled *Cyber War Will Not Take Place*, in which he argues that no cyber attack ever has or ever will constitute an act of war on its own, and instead should be considered within the accepted tradition of state espionage and sabotage.[24] Part of this paper's goal is to critically examine the foundation for this comparison within U.S. official rhetoric. Offensive cyber capabilities and engagement have also been examined through an economic lens. Academics and economists are producing work grappling with the value and legality of so-called 'cyber goods,' such as codes that could be used as tools in hacking a system. Works like Rainer Böhme's *The Economics of Information Security and Privacy*[25] and Mailyn Fidler and Jennifer Granick's "Changes to Export Control Arrangement Apply to Computer Exploits and More"[26] attempt to reconcile the nebulous cyberspace within the current market.

---

[22] Manuel Fischer, "The Concept of Deterrence and Its Applicability in the Cyber Domain," *Connections* 18, no. 1/2 (2019): 69–92. https://www.jstor.org/stable/26948850.
[23] Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* 92, no. 6 (2013): 77–87. http://www.jstor.org/stable/23527014.
[24] Thomas Rid, *Cyber War Will Not Take Place,* (Oxford: Oxford University Press, 2013).
[25] Rainer Böhme, *The Economics of Information Security and Privacy* (Heidelberg: Springer Berlin, 2013).
[26] Jenniver Stisa Granick and Mailyn Fidler, "Changes to Export Control Arrangement Apply to Computer Exploits and More," *Just Security*, January 15, 2014. https://www.justsecurity.org/5703/export-control-arrangement-apply-computer-exploits/, (accessed 11/20/22).

Understanding how the U.S. government has worked to do the same is a central part of this paper.

The first chapter will look at how the language and laws of war have (or often more aptly, have not) been applied to offensive cyber tactics. Particularly interested in the United States' demonstrated desire to treat its cyber operations as analogous to espionage, this chapter considers the arc of the Intelligence Community's official internal language as it pertains to cyber in relation to the nation's history of utilizing the language of defensive security to champion its military undertakings.

The next section will consider how the U.S. has engaged with the 'weapons' of the Fifth Domain. Drawing on Nicole Perlroth's work, visualizing what the existence of a cyber arms market truly entails reveals a dynamic between the U.S. government and the hacking and security research community that is largely dictated by the former. The rhetoric that the public-private dynamic in the field of cyber rests squarely on the government's intent to keep American networks fully secure is belied by the Intelligence Community's acquisition of tools for offensive cyber operations from private researches and third-party brokers.

Finally, the third chapter will explore the major inconsistencies that became apparent throughout the policy making conversation as a result of the narrative of cyberdefense. While the usage of defensive-oriented language as a way to circumvent involvement in offensive operations is not novel in U.S. history, as the first chapter discusses, cyber is a unique case in how extremely opaque it has become. The accessibility of hacking to both nation states and individual actors convolutes the story that the U.S. has typically told—that it is America and its allies versus an ideological 'Big Bad,' whether that be communism or Islamic extremism. Leveraging that same state-actor narrative in the context of the Fifth Domain keeps both the

public and the lawmaking conversation focused on defense, while the overclassification within the IC undermines the security it purports to prioritize.

Offensive cyber undertakings are becoming increasingly more critical in a world where technology has created an almost unimaginable level of interconnectivity. This thesis seeks to contribute to the scholarly discussion of this "Fifth Domain" by understanding the arc of the United States' contradictory engagement with cyber. By shaping this man-made war front in the image of offense, the ability to actually achieve that security is undercut.

Chapter 1: The Misnomer

"In the long history of the world, only a few generations have been granted the role of defending freedom in its hour of maximum danger." [27] This was how John F. Kennedy framed his responsibility as President in his Inaugural Address on January 20, 1961. Since the turn of the 20th Century, the United States has seen itself as bearing the cross of the global defense of freedom even in its interventions unprovoked by any direct military offense. Just a few months after his inauguration, Kennedy greenlit and launched the notoriously disastrous Bay of Pigs invasion in Cuba. Even after the operation failed, the president told the American people that the fiasco was further proof that "the forces of communism are not to be underestimated."[28] The enemy was still at large, and every move the U.S. made was in defense of freedom. As technology marched forward and cyber capabilities took shape, this ethos became fundamental to the process. In this chapter, I will explore the development of the U.S. Intelligence Community's definition of its cyber operations both internally and to the public. Ultimately, the chapter demonstrates the fallacy of the U.S. Government's claim that cyber exploitation equates purely to espionage, which does not hold up to scrutiny and ultimately places the IC's approach to the Fifth Domain in a historical arc of defensive justification.

The technical foundation for the Internet was itself an American military project: the Department of Defense's ARPANET, designed by their Advanced Research Projects Agency. The project began in 1966, designed to allow computers to share information between one

---

[27] John F. Kennedy, "Inaugural Address" (speech, Washington, DC, January 20 1961), JFK Presidential Library and Museum, https://www.jfklibrary.org/learn/about-jfk/historic-speeches/inaugural-address

[28] John F. Kennedy, "Address Before the American Society of Newspaper Editors" (speech, Washington, DC, April 20, 1961), JFK Presidential Library and Museum, https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-society-of-newspaper-editors-19610420

another from remote locations. This was not a physical network, but instead developed technology based on telecommunications to allow for remote communication.[29] ARPANET was a great success, albeit limited in scope. The next step in the development of the technological capabilities that support operations in the Fifth Domain was not far behind. In 1971, Bob Thomas, a software engineer with DoD-partnered research company BBN Technologies, developed a demo code to jump across different systems connected to the ARPANET. Considered the first computer "worm," a self-replicating and spreading malware, it did not intend to shut down systems or steal data, activities associated with most worms today, but just forced the machine it was running in to print the words "I'M THE CREEPER. CATCH ME IF YOU CAN."[30] Another BBN programmer, Ray Tomlinson, amended his colleague's code to create the "Reaper," which replicated itself to move through the ARPANET in order to find and log out instances of the Creeper program.[31] The Creeper and Reaper together constitute the first computer virus and the first antivirus program, cracking open the door for a novel way of operating within cyberspace.

Ten years after the Creeper and Reaper first wormed their way across the ARPANET, President Ronald Reagan signed Executive Order 12333, framing the United States' intelligence effort in the Executive Branch. Colloquially known as "twelve triple-three," the 1981 order delineated the National Security Agency's responsibilities, assigning them the mission of

---

[29] "ARPANET," Defense Advanced Research Projects Agency, https://www.darpa.mil/about-us/timeline/arpanet, (accessed 3/13/22).
[30]Jeffrey D. Pierdomenico, "Applied Feature Extraction for Novel Malicious Software Identification Using Convolutional Neural Networks," *American Intelligence Journal* 37, no. 2 (2020): 55–58, https://www.jstor.org/stable/27087722.
[31] Ray Tomlinson, interview by Jordan Spencer Cunningham, OSNews, April 6, 2016, https://www.osnews.com/story/29157/interview-with-ray-tomlinson-on-creeperreaper/, (accessed 3/13/22).

'signals intelligence' (SIGINT).[32] In a leaked briefing presentation for NSA agents from the 2010s, the agency writes that the mission assigned to it by E.O. 12333 includes "COMINT [communications intelligence] and in turn CNE," or "Computer Network Exploitation."[33] What exactly NSA means by Computer Network Exploitation is a question that this chapter will examine more in depth, but it is key to note here that nowhere in Reagan's executive order is computer exploitation mentioned. Even though the U.S. was already aware of the potential for hacking beyond the simple purpose of information gathering, the NSA was historically only granted the task of collecting, processing, and disseminating signals intelligence and communications security. How, then, has NSA effectively granted itself the ability to undertake offensive cyber operations intended to damage an adversary's systems under the guise of intelligence gathering for national security?

In a 2017 piece for *Limn* titled "The Spy Who Pwned Me," science and technology historian Matthew L. Jones traces the U.S. official language surrounding cyber tactics since the 1990s. He concludes that the government's claim that cyber exploitation should merely be thought of as espionage, a legitimate NSA responsibility under 12333, when considering questions of legality and policymaking, is a brittle one.[34] He points to a 1992 Department of Defense Directive as the first known definition of 'information warfare' provided by the U.S., which rendered it as "the competition of opposing information systems to include the

---

[32] Ronald Reagan, "Executive Order 12333: United States Intelligence Activities," December 4th, 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html.
[33] NSA Office of General Council, "CNO Legal Authorities," slide deck, n.d., https://www.aclu.org/sites/default/files/field_document/general_counsel_brief_on_sigint_law_and_information_assurance_law.pdf.
[34] Matthew L. Jones, "The Spy Who Pwned Me," *Limn* 8 (February 2017), https://limn.it/articles/the-spy-who-pwned-me/..

exploitation, corruption, or destruction of an adversary's information system."[35] Exploitation could arguably be considered here as encapsulating espionage, with a system being exploited for the transference of information. However, corrupting or destroying a system takes an operation a step (or perhaps many steps) beyond intelligence gathering. Some lines in the Directive remain redacted, but the section titled "Responsibilities" has been fully declassified, mentioning NSA only insofar that the Agency's director is to be kept informed of any information warfare technology developments.

In 1996, the Department of Defense issued another directive, overriding the 1992 document, and providing three new key definitions.

> Computer Network Attack (CNA): "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer and networks themselves."
>
> Information Operations (IO): "Actions taken to affect adversary information and information systems while defending one's own information, and information systems."
>
> Information Warfare (IW): "IO conducted during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[36]

Here, there is a new provision for information warfare—a time of conflict or crisis. However, by adding the term 'information operations,' the DoD provides the language for potential operations of the exact same nature to occur outside the scope of wartime. Beyond the conflict requirement

---

[35] U.S. Department of Defense, *Information Warfare (U),* DOD Directive TS 3600.1 (Washington, DC: Department of Defense, December 21, 1992) https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up.

[36] U.S. Department of Defense, *Information Operations (IO) (U),* DOD Directive TS 3600.1 (Washington, DC: Department of Defense, December 9, 1996) https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up.

of IW, the only other marked difference between IO and IW is the mention of defense in the former. Additionally, although the directive distinguishes separate terms for CNA and IO, the phrase “actions taken to affect" systems is immensely broad, with what is defined as CNA potentially falling within the category of IO. The “Responsibilities” section of this revision is also markedly different. The responsibilities of the NSA Director now involve inter-agency cooperation in supporting IO in incredibly vague terms. Unlike in the 1992 iteration, the Director’s responsibilities are partially redacted. Through these definitions, the U.S opened up doors to legitimize a wide range of cyber activities. IO became a legitimate peacetime undertaking that put offensive cyber operations hand-in-hand with defense, dulling the impact of the implications of an offensive maneuver.

NSA is an agency with very little transparency, meaning the available archive of relevant documents is likely incomplete. However, the DoD’s definition of CNA has evidently remained virtually the same since 1996,[37] meaning the recently leaked slide deck reveals that NSA treats directly offensive cyber operations as part of its inherent responsibilities designated in 1981. Referencing E.O. 12333 alone, the agency’s mission seems defense oriented, gathering intelligence for the strengthening of national security. However, comparing notes on how obscure policy has rerendered the agency’s operational capacity now reveals an offensive tilt.

In “The Spy Who Pwned Me,” Jones references a 1999 CIA document that appears to be a departure from the policy language described above.[38] The directive defined a slightly different acronym, CNE, short for ‘Computer Network Exploitation,’ as “an intelligence collection

---

[37] “computer network attack (CNA),” Computer Security Resource Center Glossary, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/glossary/term/computer_network_attack, (accessed 10/12/22).

[38] Jones, “The Spy Who Pwned Me.”

activity" not central to DoD IO doctrine, but "IO-related."[39] However, the acceptably espionage-oriented activity of CNE is deceptively bound by very loose guidelines. Crucially, Jones' article points to a leaked 2012 Presidential Directive from the Obama administration (PPD-20) that further degrades the espionage analogy. PPD-20 provides for "cyber collection," which, at face value, appears to be a clear path for the development of SIGINT into the computer age, just as the aforementioned NSA briefing slide purports. However, at the very end of the definition, which classifies cyber collection as cyber programs for "the primary purpose of collecting intelligence…by or on behalf of the United States Government,"[40] there is a clause that allows for something other than intelligence gathering. The activities of cyber collection include those "essential and inherent to enabling cyber collection…*even if they create cyber effects*."[41] Even further than Jones discusses, the document's definition of cyber effects is nearly identical to the 1996 DoD definition of Computer Network Attack, leaving the Intelligence Community legitimized room to tack on an element to a SIGINT collection operation that compromises the computer system being targeted. The definition of cyber effect in PPD-20 notably leaves out any mention of intentionality, and even the banality of the word 'effect' itself as compared to 'attack' is telling. This circumvents the necessity of acknowledging that cyber effects created during a primarily information-collecting operation are nonetheless separate from the category of espionage being used to cover American cyber operations.

---

[39] Central Intelligence Agency, *(U) INformation Operations and Intelligence Community Related Activities,* Director of Central Intelligence Directive 7/1 (Langley, Virginia: Central Intelligence Agency, July 1 1999), https://www.archives.gov/files/declassification/iscap/pdf/2008-049-doc18.pdf

[40] White House, *Presidential Policy Directive 20 (PPD-20)*, Presidential Policy Directive, (Washington, DC: The White House, 2012), pg. 2. https://irp.fas.org/offdocs/ppd/ppd-20.pdf.

[41] The White House, *Presidential Policy Directive 20*, pg. 3, emphasis added.

Another leaked document from 2012, NSA's 2012-2016 SIGINT Strategy, contains multiple points with a top-secret classification, one of which is to "Integrate the SIGINT System into a national network of sensors which interactively sense, respond, and alert one another at machine speed."[42] Once again, the U.S. casts an incredibly large web with its official language; an integrated and automated system as vast as is described here creates such a high level of interconnection that it becomes difficult to maintain separations of purpose and corresponding concerns of legality and authorization. This is evident in a 2009 decision of the Foreign Intelligence Surveillance Court (FISC), which operates in secret to grant warrants for foreign intelligence gathering projects. In 2006, the Court had authorized an NSA alert list process that served to prioritize "its review of the telephony metadata it received" through analysis of a reasonable articulable suspicion (RAS) standard.[43] However, in the time after that authorization, the agency integrated that system with other SIGINT collection processes, including Business Record metadata, updating the approved alert list with these outside telephone identifiers. As a result, the RAS standard was no longer the controlling factor in NSA's alert list, and not only was the agency collecting a wide array of information that the Court had not authorized, but it also reported to the FISC that "there was no singular person who had a complete technical understanding of the … system architecture."[44] NSA itself did not even have a full grasp of the amount of information it was collecting. In this way, cyber operations are also distinct from historical cases of espionage, wherein the capability for mass data acquisition that exists in the cyber realm did not exist. Sneaking behind enemy lines to gather physical intelligence from a

---

[42] National Security Agency, Central Security Service, *(U) SIGINT Strategy 2012-2016* (Washington, DC: National Security Agency, February 23, 2012), https://ia600906.us.archive.org/12/items/NSA-SIGINT-Strategy/2012-2016-sigint-strategy-23-feb-12.pdf.
[43] *In Re Production of Tangible Things From [REDACTED]*, BR 08-13, (FISC 2009).
[44] *In Re Production of Tangible Things From [REDACTED]*, BR 08-13, (FISC 2009).

locked office is hugely different in scale from information systems surveillance, and it is unreasonable to expect that they should be treated analogously. Even within a strict interpretation of its ordained E.O. 12333 mission of SIGINT collection, NSA lacks a track record of internal accountability, leaving Americans subject to unwarranted surveillance not commensurate with a well-defined mission of national defense.

The United States Intelligence Community has allowed itself the space to develop cyber operations far beyond the intelligence gathering mission of espionage, while promoting the idea that the two are analogous. Its utilization of the cyber domain proves to be congruent with the IC's history of covert operations, with this language of operational necessity in the name of national security a tried and true method of justification. Official documents reveal a high level of ambiguity in definition, as well as a rather opaque divide between war and peace. This has allowed for the espionage comparison to go relatively undisputed, but has left the backdoors open for 'effects' outside the scope of tailored intelligence gathering for national security. The tools the IC has used to create those effects and the consequences of their acquisition are the focus of the next chapter.

Chapter 2: The Marketplace

When Mark Zuckerberg was first building Facebook into a global leviathan, he preached a gospel that would characterize the mentality of Silicon Valley for the foreseeable future: "Move fast and break things."[45] This ethos has pushed technology forward at an exponential rate, but it is often not just the status quo being broken in the process, but the very technology itself. The more interconnected our systems become, the harder they are to keep secure. Each flaw in a code, known as a vulnerability or a bug, allows space for threat actors to take advantage of that weak point and utilize an exploit, hacking the system.[46] With the seemingly incessant desire to expand the scale at which everything in our daily lives, from smart homes[47] to pacemakers,[48] connects across a network, a concept known as the 'internet of things,' or IoT, comes a greater potential ripple effect from a single vulnerability.[49] Vulnerabilities in a code come in various stages of severity, but the most concerning type, and thus the most valuable for a developer to

---

[45] Samantha Murphy, "Facebook Changes Its 'Move Fast and Break Things' Motto," *Mashable,* April 30, 2014. https://mashable.com/archive/facebooks-new-mantra-move-fast-with-stability#I7FF2Du4IPq6, (accessed 10/21/22).

[46] "vulnerability," Computer Security Resource Center Glossary, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/glossary/term/vulnerability, (accessed 4/22/22).

[47] "The Smart Homes Market is Expected to Reach $205 Billion by 2026, Driven by the Growing Adoption of Smart Devices as per the Business Research Company's Smart Homes Global Market Report 2022," The Business Research Company, August 18, 2022, https://www.globenewswire.com/news-release/2022/8/18/2501085/0/en/The-Smart-Homes-Market-Is-Expected-To-Reach-205-Billion-By-2026-Driven-By-The-Growing-Adoption-Of-Smart-Devices-As-Per-The-Business-Research-Company-s-Smart-Homes-Global-Market-Rep.html, (accessed 10/30/22).

[48] Daniel Clery, "Could a Wireless Pacemaker Let Hackers Take Control of Your Heart?" *Science*, February 9, 2015. https://www.science.org/content/article/could-wireless-pacemaker-let-hackers-take-control-your-heart, (accessed 10/30/22).

[49] Alexander S. Gillis, "What Is the Internet of Things (IoT)?" IoT Agenda, TechTarget, March 4, 2022. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT, (accessed 10/30/22).

find, is known as a "zero-day." This is a vulnerability about which the software developer or company is completely unaware, and has therefore had *zero days* to develop a fix, or patch, for the code.[50] However, it is not only the developer who sees value in a zero-day. These vulnerabilities have become key assets to the U.S. Government. This chapter will chart the Intelligence Community's role in building a cyber weapons market around computer exploits and consider how the ideals of American exceptionalism have granted it legitimacy. Understanding this development sheds light on how the U.S. Government undermines cybersecurity for the sake of cyber offense[51] development under the guise of securing a strong national cyber defense.

Discovering vulnerabilities and the exploits that take advantage of them has long been a source of pride amongst ethical hackers, known as white hats.[52] For a long time, the ethos of the white hat hacking community was one in which the bragging rights of being the person to outsmart a developer was the only motivation a security researcher needed. They often traded and sold amongst themselves, but generally followed responsible best practices when it came to disclosure, voluntarily informing the vendor of the vulnerability they had discovered in their program.[53] Hackers could not resist poking fun at corporations with holes in their code, but still

---

[50] Clare Stouffer, "What is a zero-day exploit?," Emerging Threats, Norton, September 3, 2021, https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html#, (accessed 4/20/22).

[51] The term cyberwar is not used in this paper, excepting cases where it is reflecting the language used by a source, so as to not make implications regarding the nature of war. This paper is not focused on the point at which a cyber operation becomes an act of war. There is a wide array of scholarship debating this question. Instead, the terms 'cyber offense' and 'offensive cyber operation' are used to refer to those operations which are not solely protecting one's own systems, but are targeting another.

[52] "White Hat Hackers: The Good, the Bad, or the Ugly?" Kaspersky Resource Center, March 30, 2022. https://www.kaspersky.com/resource-center/definitions/white-hat-hackers, (accessed 10/20/22).

[53] Charlie Miller, "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales," (Independent Security Evaluators, May 6, 2007)

had the best interests of public security at heart. However, in the early 2000s, a new market began to take shape around white hat hacking,[54] commercializing the zero-days that could decimate information systems and security apparatuses and injecting a new ethos of capitalism into the white hat community.

To understand exactly how the Intelligence Community's intervention contoured the zero-days market, we need to trace its development. White hats had been gleefully exposing software developers with a chip on their shoulder through the 90s, but at the turn of the millennium, the winds of free exchange were starting to wane. Tech vendors, tired of being exposed on stage at hacking conventions by attendees sharing their security research, were beginning to threaten lawsuits.[55] In 2001, Russian programmer Dmitry Sklyarov was arrested at DEF CON, an annual hackers convention in Las Vegas, for his presentation of an Adobe Acrobat eBook Reader exploit.[56] Sklyarov was charged under the 1998 Digital Millennium Copyright Act given that his program circumvented protections of copyrighted material[57] rather than anything inherent to the presentation of an exploit, but the atmosphere of the hacking community became increasingly sullen.[58] The spirit of blithe transparency and anti-establishment attitude began to feel like a liability rather than an asset and the legal tides were shifting. The legislation being furiously drawn up in the fallout of September 11th, 2001 terror attacks, including a

---

[54] Perlroth, *This is How They Tell Me the World Ends*
[55] Perlroth, *This is How They Tell Me the World Ends*, 45.
[56] "Russian computer programmer arrested at hacker conference," CBC News, July 19, 2001, https://www.cbc.ca/news/science/russian-computer-programmer-arrested-at-hacker-conference-1.27667, (accessed 11/3/22).
[57] United States v. ElcomSoft and Dmitry Sklyarov, 203 F Supp 2d 1111 (N.D. Cal., 2002).
[58] Kim Zetter, "Shock! Maturity rules at hack fest," DC10 Articles, DEF CON, last modified August 13, 2002, https://defcon.org/html/defcon-10/dc-10-articles/dc-10-smh-shocked.html (accessed 12/15/22).

proposal for a law that would give a life sentence to anyone convicted of a computer crime resulting in a death,[59] cast a shadow over the cyber world. A recap of the 2002 DEF CON highlighted annual speaker Richard Thieme's statement to the crowd that "the stakes are different."[60]

In her book *This is How They Tell Me the World Ends*, journalist Nicole Perlroth pins the birth of the zero-days market within the context of this uncertain moment of change on Texan investor John P. Watters' purchase of the bankrupt and crumbling cyber security company iDefense for $10 in 2002.[61] At the same time Watters shelled out pocket change for iDefense, its competitor, SecurityFocus, was bought by security software giant Symantec for $75 million. SecurityFocus' main service was something called BugTraq, a forum mailed out to clients where unaffiliated white-hat hackers, for no compensation, posted bugs they had found on their own time. Posters on the forum engaged for the sake of greater network security and personal clout within the hacking community; the only hackers really turning a profit from disclosing vulnerabilities during this time were criminals with malicious intent, or 'black hats.' The international intelligence community was aware of the threat posed by black hat hacking as early as 1986 when three German hackers hacked into and stole data from Western military, research, industrial and commercial computer systems, including U.S. systems, later selling that data to the Soviet KGB intelligence service.[62] Watters and his research team at iDefense, led by 20-somethings David Endler and Sunil James, realized that there was an opportunity to capitalize on the wariness of hackers to freely share their findings and trailblaze a new, legitimate market.

---

[59] Zetter, "Shock!"
[60] Zetter, "Shock!"
[61] Perlroth, *This is How They Tell Me the World Ends*, 40-42.
[62] Robert J. McCartney, "Computer Hackers Face Spy Charges," *Washington Post,* August 17, 1989, https://www.washingtonpost.com/archive/politics/1989/08/17/computer-hackers-face-spy-charges/cad42e6b-73db-48d4-814f-86eb1574ae68/, (accessed 3/31/23).

In 2003, the company began paying hackers for zero-day vulnerabilities through their new Vulnerability Contributor Program (VCP). They were willing to lay down their pro-transparency and public interest attitudes and join in. As Perlroth puts it, "getting paid was a lot more enticing than getting sued."[63] At first, iDefense's clients, who paid a subscription fee to be sent the bugs relevant to their software, were dismissive. However, when New Zealand hacker Greg McManus, who had become the provider of half of iDefense's bug collection as an independent hacker and was subsequently offered a job, began sending clients examples of how the vulnerabilities being gathered could be used, or proof-of-concept exploits,[64] to prove their value, iDefense began raking in profit.[65] In a 2003 interview with Help Net Security, Sunil James touted the company's VCP as "reaching a balance between remaining true to our clients and being responsible to vendors and the Internet community at large."[66] The responsibility to this broader 'Internet community' had always been a part of the hacking community's modus operandi, but the legal pushback against publicly airing out vulnerabilities opened the door for that responsibility to be financially compensated and exponentially less visible.

In a paper for the RAND Corporation titled "The Defender's Dilemma: Charting a Course Toward Cybersecurity," scholars Martin C. Libicki, Lillian Ablon, and Tim Webb delineate three different levels of the vulnerability market as it has developed over the last few

---

[63]Perlroth, *This is How They Tell Me the World Ends*, 28.
[64] Contributor, "Proof of Concept (PoC) Exploit," Security, TechTarget, May 22, 2019. https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit#:~:text=A%20proof%20of%20concept%20(PoC,and%20protect%20itself%20against%20attacks, (accessed 1/12/23).
[65]Perlroth, *This is How They Tell Me the World Ends*, 48.
[66] Sunil James, "Interview with Sunil James, Manager of IDEFENSE's Vulnerability Contributor Program," interview by Mirko Zorz, Help Net Security, June 1, 2020, https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/, (accessed 1/3/23).

decades.[67] There is a 'white-market,' in which vulnerabilities are sold directly to the vendor, a 'black-market,' where vulnerabilities are sold to cybercriminals, and a much blurrier category, the 'gray-market.' RAND defines this market as one in which the buyers are government and intelligence agencies.[68] Watters' iDefense was an independent provider, acting as an intermediary between security researchers and software vendors, with an ethos akin to the 'white-market.' iDefense's website in the early 2000s outlined their vulnerability reporting process, declaring that their mission was only to formally publicly release security advisories for the sake of corrective action, and that the company would notify vendors "as soon as reasonably possible after it has discovered and verified a problem with their product or service."[69] The idea of a bug bounty program, where companies offer payoffs in exchange for identification of vulnerabilities needing to be patched, dates back to Netscape's 1995 cash bounty for non-employees who found bugs in their Netscape Navigator 2.0 Beta program.[70] But iDefense set the stage for relatively above-ground vulnerability deals brokered by a public third party. The gap between gray-market independent brokers who dealt only in the shadows and the widely advertised rewards of the white-market was beginning to close, paving the way for the IC's influence on the acquisition and sale of vulnerabilities to further permeate the world of security research.

In the years after the VCP took off, brokers who publicly advertised their role in the gray-market started to pop up; American infosec company Zerodium proudly states in their

---

[67] Martin C. Libicki et al., "The Defender's Dilemma: Charting a Course Toward Cybersecurity," (Santa Monica, CA: RAND Corporation, 2015) https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf.
[68] Libicki, et. al, "The Defender's Dilemma."
[69] "iDEFENSE Security Vulnerability Reporting Policy," About Us, iDefense Last Modified Jan 11, 2005, Accessed via Wayback Machine, https://web.archive.org/web/20020802020542/http://www.idefense.com/disclosure.html, (accessed 10/15/22).
[70] Esben Friis-Jensen, "The History of Bug Bounty Programs," Cobalt, April 11, 2014, https://www.cobalt.io/blog/the-history-of-bug-bounty-programs, (accessed 11/14/22).

website's FAQ that their buyers are government institutions, "mainly from Europe and North America."[71] It might seem intuitive to conceptualize the rise of these types of brokers as a natural evolution of the iDefense model, a new avenue of the market with the hacking ethos of responsible disclosure still intact. However, while iDefense might have influenced the legitimacy of these firms, a much murkier underbelly of the vulnerability market contributed to their success. One of the minds behind the VCP, David Endler, went to work for another security startup, TippingPoint, after his time at iDefense. In developing their Zero Day Initiative program, which also paid researchers for vulnerabilities and then disclosed them to their respective vendors,[72] Endler had proposed a questionable idea akin to an auction, selling a vulnerability to the highest bidder regardless of their affiliation with the software vendor in question, but still requiring disclosure to that vendor. In 2007, Endler reflected that the auction venture never moved forward, as the concept "seemed to touch a strong nerve with the few security people I approached with the idea."[73] However, these kinds of auctions had already been taking place for at least a decade, not just as black market deals, but as gray-market, state-sponsored ones.[74]

In researching for *This is How They Tell Me the World Ends*, Nicole Perlroth secured a meeting with a former government contractor, whom she writes about using the pseudonym Jimmy Sabien. Sabien told her that he and his team had been discovering exploits and selling them to different entities within the U.S. government since the mid-1990s, and were purchasing zero-days later in the decade at the behest of U.S. intelligence agencies. These transactions

---

[71] "Frequently Asked Questions," *Zerodium*, https://zerodium.com/faq.html.
[72] "Program Benefits," Zero Day Initiative, n.d., https://www.zerodayinitiative.com/about/benefits/#process, (accessed 11/15/22).
[73] Endler, "Remembering."
[74] Lillian Ablon and Andy Bogart, " Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

occurred entirely in the shadows, with the majority of the hacking community still thumbing their noses at the proverbial Man and freely exposing vulnerabilities in the name of public responsibility. One of the most popular activities at the DEF CON annual conference was a game of Spot The Fed, with a free t-shirt for attendees able to identify undercover federal agents in attendance (and one for the exposed agent as well).[75] Hackers were unwilling to openly cooperate with the IC. In fact, in 2003, Sabien had gone to John Watters as a mysterious, anonymous buyer and tried to coax him into forgoing iDefense's disclosure model and selling the zero-days directly to him for a staggeringly higher price. Watters did not bite, but the U.S. government's willingness to shell out massive sums of money to obtain zero-days effectively undermined Watters' business model of responsible disclosure.[76] Security researchers had already been given good reason to start seeking compensation for their findings when the fear of legal retaliation struck the community. If the hackers were already selling, poaching them from companies like iDefense was not much of a stretch for the deep pockets of the nation's intelligence apparatus. David Endler's scrapped auctioneering blueprint had actually already been built and bankrolled by the government. The model his peers had bristled at now lured the best security researchers with the bait of an exponentially higher payoff.

The three-letter American agencies paying for the zero-days have done so in the name of national security. Having framed cyber espionage as a continuation of existing SIGINT operations,[77] the Intelligence Community easily passes off their collection of zero-days as necessary components of classified defense operations. This prioritization of national strategy over information and software security only truly serves the offensive side of American cyber

---

[75] Alex Wellen, "DEF CON's sport: Spot the fed," ZDNET, July 5, 1999, https://www.zdnet.com/article/def-cons-sport-spot-the-fed/, (accessed 10/10/22).
[76] Perlroth, *This is How They Tell Me the World Ends*, Chapter 4.
[77] NSA Office of General Council, "CNO Legal Authorities."

operations. In 2010, the U.S. government first instituted a heavily redacted 'Vulnerabilities Equities Process', or 'VEP,' which has since been overridden by an unclassified 2017 Trump-era iteration, *Vulnerabilities Equities Policy and Process for the United States Government*.[78] The VEP regulates disclosure of vulnerabilities that fall into the hands of the government before the targeted company is made aware of their existence. The process requires a vote to be taken by representatives across a few federal agencies within a tight timeframe as to whether a vulnerability should be restricted or disclosed. "Operational Value and Operational Impact Considerations" is cited as a major factor the voters consider in making their determination.[79] Procedurally, the VEP is developed with a meaningful sense of urgency and keeps some apparent nuance in mind, clarifying that the evaluation process is not always a binary between total restriction and complete dissemination. However, while the process is designed to incorporate discourse across more than one agency, it is confined to exclusively executive powers, and can still leave vendors (and those that use their software) out to dry. While NSA might be armed with an arsenal of potential cyber network exploits and attacks to be carried out, there are gaping holes in the software left open for threat actors. The gray-market allows the United States to gamble on the fact that an adversary will not get to an exploit before the IC has a chance to use it against them and subsequently secure its own assets.

The Intelligence Community creates weaknesses in its own armor by hoarding vulnerabilities, but because federal agencies are willing to pay so much more than either intermediate bounty programs like the VCP or the software vendors themselves, they effectively corner the market, making themselves and the brokers that sell to them the most appealing option

---

[78] White House, *Vulnerabilities Equities Policy and Process for the United States Government*, Unclassified Charter (Washington, DC: November 15, 2017) https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[79] The White House, *Vulnerabilities Equities Policy*, 14.

for the most accomplished researchers. The old ethos of the hacking community, one where waving around a vulnerability discovery made researchers lunchroom heroes, was replaced by an arms market. In a piece titled "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales," former NSA employee and renowned hacker Charlie Miller recalls helping an acquaintance sell a Microsoft Powerpoint XP vulnerability he had discovered. Because these deals are incredibly opaque, selecting a buyer requires researchers to make a somewhat arbitrary judgment call on what a fair price to accept is without a full picture of the market. In the search for a buyer, Miller imagined a $1,000 - $3,000 payout from iDefense or Tipping Point, a $20,000 evaluation directly from the company affected, and a $50,000 bounty from the government.[80]Any researcher looking at selling their discovery would have to make both a financial and a moral decision. While the moral element might take into account the security of the software's users, it is also heavily weighted by the omnipresent pressure of U.S. messaging promoting patriotism and loyalty. Particularly given that the market grew most markedly in the wake of 9/11, the sale of an exploit is pulled into the category of "seeing something and saying something."[81] As to the financial aspect of the seller's decision, the complete lack of pricing transparency in the zero-days vulnerability marketplace means that researchers have no tangible idea as to the market price of their work, and the government has built a reputation for offering a high price point.[82] Scholars and economists have proposed potential solutions to combat this opacity, such as Rainer Böhme's idea for an exploit derivative market, where contracts could be bought and sold as investments, paying out in the case of a

[80] Charlie Miller, "The Legitimate Vulnerability Market."
[81] Joshua Reeves, *Citizen Spy: The Long Rise of America's Surveillance Society* (New York: NYU Press, 2017), Chapter 5.
[82] Miller, "The Legitimate Vulnerability Market"

specified software either experiencing a security event or remaining secure.[83] However, the government is unlikely to bring any of this above-board, given the IC's tendency toward overclassification in the name of national security.

The opacity of the gray-market forces security researchers and hackers to deal in shadowy, word-of-mouth contexts, and leaves government-acquired vulnerabilities subject to a disclosure policy that is incredibly insular and political. Even the distinction between the black and gray markets is effectively a geopolitical one. A study on the vulnerability market titled "Bugs in the System" from the left-leaning think tank New America reports that deals brokered with "countries whose governments are much less likely to respect human rights…could be considered part of the black market."[84] The delineation of the gray-market as a concept, then, rests on the assumption that the United States and its allies are inherently good actors, and thus their exploit purchasing warrants a distinction from what is otherwise a black market arms trade. Not only does the image of America as an international defender of freedom legitimize the IC's vulnerabilities dealings, but its lack of transparency in order to protect offensive assets effectively undermines cyber defense. Intelligence agencies want to move fast and break things, and they have the funds to drag independent security researchers along for the ride. The nature of the zero-days market and its goods exacerbates vulnerabilities, leaving information and technology systems, as well as those who research them, open to further exploitation. As the next chapter continues to reveal, the exacerbation of vulnerabilities due to the obfuscation of U.S.

---

[83] Rainer Böhme, "A Comparison of Market Approaches to Software Vulnerability Disclosure," in *International Conference on Emerging Trends in Information and Communication Security*, (Berlin, Heidelberg: Springer-Verlag, June 6, 2006), https://dl.acm.org/doi/10.1007/11766155_21.

[84] Andi Wilson, Ross Schulman, Kevin Bankston and Trey Herr, *BUGS IN THE SYSTEM: A Primer on the Software Vulnerability Ecosystem and Its Policy Implications,* (Washington, DC: New America, July 2016), https://nsarchive.gwu.edu/sites/default/files/documents/3525982/Document-07-Andi-Wilson-Ross-Schulman-Kevin.pdf.

cyber operations is a central issue in understanding how the Fifth Domain has been shaped by the IC.

Chapter 3: The Misdirect

On a Saturday in early June, 1983, in a cozy, wood paneled room of Camp David, President Ronald Reagan and First Lady Nancy sat back for a movie night with a group of White House staffers. The MGM lion roared across the screen, and the group was transported to the missile launch control room at the NORAD Combat Operations Center. Over the course of the next two hours, the President watched as a teenager accidentally hacked into a government supercomputer and nearly launched a nuclear war.[85] As the credits rolled, a sobering hush took over the room. Finally the First Lady turned to the group: "Could that really happen?"[86]

Watching that movie, John Badham's *WarGames*, inspired Reagan to precipitate a national security conversation that would culminate in the first National Security Decision Directive addressing information security.[87] This chapter will examine that policy and more, understanding that the Intelligence Community has obscured so much of its own action and intention that both lawmakers and the public that elects them are having a conversation about cyber that has not kept up with the actual undertakings of the IC and does not account for the full reality. By keeping the focus on defense, a historically successful angle for getting the public on the side of the American government, and consistently underscoring the presence of a familiar looming threat, such as Russia or Islamic terrorism, U.S. involvement in offensive cyber operations is obscured. As a result of this opacity, the cybersecurity that remains the center of an

---

[85] *WarGames*, directed by John Badham (1983; Santa Monica, CA: MGM Home Entertainment, 2008), DVD.
[86] Mark D. Weinberg, *Movie Nights with the Reagans: A Memoir* (New York, NY: Simon & Schuster, 2018).
[87] White House, *National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive 145 (Washington, DC: The White House, September 1984)
https://nsarchive.gwu.edu/document/21567-document-01-ronald-reagan-national-security

outdated public discussion is actually undermined, leaving American systems and individual privacy at serious risk.

National Security Decision Directive Number 145 (NSDD-145), published confidentially in September 1984, recognized the significance of the threat that the exploitation of electronic information systems posed. The directive outlines a leadership framework for its oversight that ultimately never came to pass as subsequent legislation moved forward, but it remains a vital touchpoint for understanding the attitudes surrounding the issue of cyber within the White House. As a document that started policymaking conversations, NSDD-145 hinges on the promotion of "a coherent and coordinated defense against the hostile intelligence threat" to the telecommunications and automated information systems developing with unprecedented speed. Its only reference to E.O. 12333, the order Reagan signed three years earlier that would later be used by NSA to justify Computer Network Exploitation activities, is in identifying the Secretary of Defense as the Executive Agent in this systems security undertaking. NSDD-145 was considered a positive step in addressing the expanding cyber frontier, although the aforementioned deserted leadership specifics raised concerns of ambiguity and organizational overlap.[88] The capacity that the developing systems technology created for offensive attacks was beginning to take shape during this period in the mid-80s and, as evidenced by this policy response, the White House was increasingly aware. However, from this beginning moment, the focus of elected officials was on keeping American cyber systems secure from these attacks, rather than how to capitalize off of this new world.

---

[88] *The Potential Impact of National Security Decision Directive (NSDD) 145 on Civil Agencies before the Subcommittee on Transportation, Aviation and Materials Committee on Science and Technology, House of Representatives,* 99th Cong. (1985) (statement of Warren G. Reed, Director of Information Management and Technology Division) https://www.gao.gov/assets/127279.pdf.

This stretch of policymaking was focused on security, but it would be naive to assume that this was the only conversation happening inside the Intelligence Community. Certainly, if there are those concerned about defending from a novel offensive capability, there are those thinking about how the U.S. itself can take advantage of that offense. The NSA's Top Secret periodical *Cryptolog*, published only for employees of the agency, ran an article in 1994 titled "Information Warfare: A New Business Line for NSA."[89] The article remains partially redacted, but the title alone is summary enough; NSA was actively scoping how it could engage in the offensive measures that the lawmaking conversation was so focused on defending against. As the NSA author writes, "the vulnerabilities that require protection in our own systems are also exploitable weaknesses in an adversary's system."[90] This disconnect meant that the legislation of the time was laying the groundwork for justifying offensive tactics. Because there was no explicit policy reconciliation with the likelihood that NSA and the wide Intelligence Community would engage in offensive cyber operations, legislative gaps were left wide open, allowing for practices like NSA's application of E.O. 12333 to Computer Network Exploitation as discussed in Chapter 1.

The mid-90s saw a spike in attention paid to the threat of Information Warfare. The Joint Chiefs of Staff published an over 500-page document titled "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance" in 1996.[91] Multiple Congressional hearings took place the same year addressing the vulnerability of American cyber

[89] National Security Agency, "Information Warfare: A New Business Line for NSA," *Cryptolog Vol. 20, No.2*, July 1994, https://nsarchive.gwu.edu/document/27449-national-security-agency-cryptolog-vol-20-no-2-information-warfare-new-business-line.
[90] National Security Agency, "Information Warfare: A New Business Line for NSA," p. 9.
[91] Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition* (Washington, DC, DoD: July 4, 1996), https://nsarchive.gwu.edu/document/19024-national-security-archive-joint-chiefs-staff.

networks.[92] However, as established in the previous chapter, the IC was already engaged in purchasing exploits from private contractors,[93] and it is not apparent that any of this discourse accounted for that type of operation. One minority staff statement from the U.S. Senate Permanent Subcommittee Committee on Investigations prepared for a June 5, 1996 Hearing on Security in Cyberspace mentions in passing that NSA "hopes to create a 'thousand person' information warfare center that would include both a defensive and offensive infowar focus," but the implications of that are not addressed any further. In fact, the subcommittee only includes this to underscore that their investigation revealed that no agencies had been able to provide a comprehensive threat assessment beyond anecdotal information.[94] It is unclear exactly how this potential center ultimately manifested, which itself is another marker of policymakers' focus on defending against external cyber threats leaving NSA's offensive undertakings essentially unaddressed.

Despite this deficiency, this era of cyber discussion did take note of some valuable and legitimate concerns that arose with the development of Information Warfare capabilities, such as the ever-increasing ease of utilizing hacking tools[95] and the difficulty of operating in a sphere that lacks traditional nation-state boundaries and provides attackers with a previously unseen level of anonymity.[96] While the policy surrounding defending U.S. cyber systems from attacks

---

[92] See list of Congressional Hearings in 1996 published by the Federation of American Scientists' Intelligence Resource Program, https://irp.fas.org/congress/1996_hr/index.html.
[93] Perlroth, *This is How They Tell Me the World Ends*, Chapter 4.
[94] *Security in Cyberspace before the Senate Committee on Government Affairs Permanent Subcommittee on Investigations*, 104th Cong. 27 (1996) (statement of Minority Staff: Dan Gelber, Chief Counsel (Minority) and Jim Christy, Investigator (Minority), Senate Permanent Subcommittee on Investigations), https://irp.fas.org/congress/1996_hr/s9606053.htm.
[95] Minority Staff, testimony on *Security in Cyberspace.*
[96] Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition*, 4-2.

became an increasingly larger part of the national security discussion as technology advanced, the question of just who those attackers were became a part of public discussion as well. Archived in an FBI file, a 1999 *Newsweek* magazine article titled "We're In the Middle of a Cyberwar" covered an intrusion on DoD computer systems. The suspects, according to the piece, were "crack cyberspooks from the Russian Academy of Sciences, a government-supported organization that interacts with Russia's top military labs."[97] The attack, known as 'Moonlight Maze,' was ultimately tied by FBI and DoD investigators to Russia,[98] but that investigation was classified, and remains largely so to this day. With little response from U.S. officials, the *Newsweek* article reveals a dramatic response toward perceived international state-actor threats. Crying 'cyberwar' and terming the attackers 'crack cyberspooks' reflects a looming Russian threat that Americans had been warned of for decades. Tapping into those residual fears was immediately salient on the heels of the Cold War. Of course, the threat of international cyber aggression was (and remains) a very real one. Moonlight Maze was indeed a multi-million dollar loss and significant security breach for the United States.[99] However, lawmakers immediately grasped onto the threat posed by nation-states, a trend that would continue to overwhelm the conversation.

In a Senate Committee hearing on March 2, 2000 entitled "Cyber Attack: Is the Government Safe?" Senator Daniel Akaka gave an opening statement in which he affirmed that

---

[97] Gregory Vistica, "We're in the Middle of a Cyberwar," *Newsweek,* September 20, 1999, 52, scan from Federal Bureau of Investigation, Cyber Vault Library, National Security Archive, The George Washington University, Washington, DC, https://nsarchive.gwu.edu/document/19293-national-security-archive-federal-bureau.

[98] Juan Andres Guerrero-Saade, et al., *Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage,* (Kaspersky Lab, April 3, 2017), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

[99] *Hearing before Committee on Governmental Affairs,* United States Senate (March 2, 2000) (Statement of James Adams, Chief Executive Officer Infrastructure Defense, Inc) https://irp.fas.org/congress/2000_hr/030200_adams.htm.

"hacking is a crime, but it has also become an act of international aggression," with "more than 20,000 cyber attacks" on DoD networks the previous year. Akaka's numbers were accurate – the Defense Department detected a total of 22,144 attacks on its networks in 1999. However, all but 1,000 of those had been attributed to recreational hackers, despite the implications Akaka's delivery made regarding the extreme severity of the nation-state cyber threat.[100] In the same hearing, Kevin Mitnick, the FBI's once most-wanted hacker released less than two months earlier from a five-year prison sentence,[101] told the Committee that his youthful exploits in hacking had been encouraged in the 1970s. "Now," he told them, "it is taboo."[102] Hacking was becoming a dirty word, and it was being attached to the major rhetorical enemies of the U.S. in the associations of the public.

This development of the popular understanding of the cyber domain in the 80s and 90s laid the groundwork for the IC's ability to undertake offensive cyber operations with extremely murky oversight. At the turn of the 21st century, the capabilities and operations of the intelligence community were primed to evolve with few checks from elected officials as the Russian Hacker and the Jihadist Facebook Recruiter became the mascots of cyber attacks. The attack on the World Trade Center on September 11, 2001 served to cement this. In the immediate wake of 9/11, American patriotism surged.[103] A month after the attacks, a Gallup poll found that

---

[100] "Pentagon Still Under Assault from Hackers," CNN, August 9, 2000, http://www.cnn.com/2000/TECH/computing/08/09/cybersecurity.reut/index.html, (accessed 4/1/23).

[101] "Mitnick Released from Prison," *New York Times,* January 21, 2000, https://www.nytimes.com/2000/01/21/technology/mitnick-released-from-prison.html#:~:text=Mitnick%20Released%20From%20Prison%20THE,for%20the%20next%20three%20years (accessed 4/1/23).

[102] Adams, testimony to the Senate Committee on Governmental Affairs.

[103] "Two Decades Later, the Enduring Legacy of 9/11," War and International Conflict, Pew Research Center, September 2, 2021 https://www.pewresearch.org/politics/2021/09/02/two-decades-later-the-enduring-legacy-of-9-11/#:~:text=Patriotic%20sentiment%20surged%20in%20the,of%20the%209%2F11%20attacks, (accessed 3/30/23).

60% of Americans reported trust in their government "to do what is right just about always/most of the time," the highest percentage in 30 years, nearly doubling from the 31% rate reported by a CBS/NYT poll nine months before the attack.[104] Policymakers threw themselves into high gear on defense, and the combination of public trust and patriotism meant that elected officials were under pressure to do absolutely everything in their power to let the DoD do its job. Mention of the terrorist threat was enough for policymakers to sign on to legislation they may not have had a full understanding of—the USA PATRIOT Act passed the Senate on October 25, 2001, only two days after its introduction, with only a singular vote against it.[105]

The narrowing focus in the cyber conversation on an international threat faced by the U.S. was now coupled with a high level of leeway being given to the Intelligence Community. On February 6, 2002, an annual open Senate hearing before the Committee on Armed Services regarding "Current and Projected National Security Threats to the United States" unsurprisingly centered around the threat of terrorism, and the limited discussion of cyber operations was therefore concerned with what the growth of cyber capabilities could mean for terrorists. Dale L. Watson, the FBI's Executive Assistant Director of Counterterrorism and Counter Intelligence at the time, was asked by Senator John Edwards' to give his assessment on how serious the cyber threat really was. Watson answered that the main concern was cyber communications between terrorists and, more importantly, cyber threats on infrastructure, but made sure to use his brief time to point to the defensive element. Watson called terrorist cyber capabilities a "tremendous

---

[104] "Public Trust in Government: 1958-2022," Trust in Government, Pew Research Center, June 6, 2022, https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/ (accessed 3/30/23).

[105] "USA PATRIOT Act of 2001 (H.R. 3162): Rollcall Vote No. 313, Leg.," *Congressional Record* 98:1 (October 25, 2001), Available from: ProQuest Congressional, https://www.senate.gov/legislative/LIS/roll_call_votes/vote1071/vote_107_1_00313.htm, (accessed 3/29/23).

threat," telling the Committee that "We need the capability to be able to understand that and be able to counter that threat."[106] To drive this home, he gave them a statistic they would find sobering, noting that over 55% of threat cases the National Infrastructure Protection Center reported the previous year "had ISPs [Internet Service Providers] involved outside the United States."[107] The broad ask for 'capability to understand and counter' provides for essentially any type of operation if properly couched, as became very clear in the breadth of operations coming out of the PATRIOT Act revealed by NSA whistleblower Edward Snowden.[108] The defensively oriented conversation that had begun in the 80s, while bringing up valid concerns, did not change with the times, instead setting a circular discussion that drudged on in the chambers of Congress while those at NSA's Fort Meade compiled a trove of zero-days and built a search engine for agents to parse through networks of global exploitable systems.[109]

As the years went on following 9/11, polls showed American public trust in the federal government crashing.[110] However, the conversation surrounding cyber operations being held by the public and government officials not privy to closed-door, highly classified IC undertakings continued to focus on the defense element. The trajectory of defense as a conversation-ending

---

[106] *Current and Projected National Security Threats to the United States before the Select Committee on Intelligence of the United States Senate*, 107th Cong. (2002) (Testimony of Dale L. Watson, Executive Assistant Director, Counterterrorism and COunterintelligence, FBI), https://www.govinfo.gov/content/pkg/CHRG-107shrg82338/html/CHRG-107shrg82338.htm.

[107] Watson, testimony on *Current and Projected National Security Threats to the United States*.

[108] For further review of the revelations brought to light by the documents leaked by Edward Snowden, visit *The Intercept's* "Snowden Archive," in which they compile stories published using the documents provided to them by the NSA whistleblower. https://theintercept.com/collections/snowden-archive/.

[109] Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee, "XKEYSCORE: NSA's Google for the World's Private Communications," *The Intercept*, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/, (accessed 4/13/22).

[110] Pew Research Center, "Public Trust in Government: 1958-2022."

justification being an ingrained part of the American intelligence conversation extends beyond 9/11, ensuring its longevity even after the sharp boost in public trust waned. Senator Susan Collins, who had indicated her fear of whichever malignant figure had perpetuated the Stuxnet attack on the Natanz Nuclear Facility in the 2010 Senate Committee investigative hearing "Securing Critical Infrastructure in the Age of Stuxnet," also brought attention in that hearing to how she believed the event should be addressed. Pointing to bipartisan legislation intended to "strengthen our cyber defenses across both the federal government and the private sector" she had introduced alongside two other Senators, she called this the development of "a comprehensive approach to this national threat."[111] While Collins' seems to have had no inkling of U.S. involvement in perpetrating the Stuxnet attack, it is unclear as to whether she had been privy to the Top Secret Bush-era National Security Presidential Directive/NSPD–54, also known as Homeland Security Presidential Directive/HSPD–23 published on January 8, 2008. Released with redactions seven years later under a heavily contested FOIA request,[112] NSPD–54/HSPD–23 contains the first mention of American application of cyber capabilities explicitly referred to as "offensive" in a document released publicly by the government. Paragraph (49) provided that a core group of officials would submit a "joint plan for the coordination and application of offensive capabilities to defend U.S. information systems."[113] While the language here still ultimately lands on an intent to 'defend,' David Sanger's reporting for *The New York Times* indicates that this policy was issued just as the IC was conceptualizing a

---

[111] Collins, Statement on *Protecting Cyberspace as a National Asset.*
[112] "Presidential Directives on Cybersecurity," Cybersecurity, Electronic Privacy Information Center, https://epic.org/issues/cybersecurity/presidential-directives/ (accessed 3/31/23).
[113] White House, *Cybersecurity Policy*, National Security Presidential Directive/NSPD–54; Homeland Security Presidential Directive/HSPD–23 (Washington, DC: The White House, January, 8, 2008), 14, https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

cyberweapon attack on Natanz.[114] Calling the Stuxnet attack a defense of U.S. information systems is a rhetorical stretch, but to an elected official like Collins without knowledge of the malware's true perpetrator, NSPD–54/HSPD–23's language of a defensive mission was sound. The response the Senator from Maine brought to the 2010 hearing promoting the strengthening of defenses was likely well-intentioned, but effectively served to also promote the strengthening of operational power for the agency that had launched the attack.

Because the IC, particularly NSA, keeps its offensive capacity so close to its chest, the public discourse is unable to properly reflect the scope of policy implications. The nature of cyber, as officials had recognized for decades, was such that an increase in operational capacity for one actor could easily become an increase for any actor.[115] If a security researcher painstakingly developed a hacking tool utilizing a high level of resources, but shared that tool publicly, someone with far fewer skills and resources could utilize the same capability. The liability that this creates was on full display in 2016, when a faceless group calling themselves the Shadow Brokers began leaking to the internet an array of cyber tools they attributed to an entity known as the Equation group.[116] A year before the leaks began, Moscow-based and UK-operated cybersecurity company Kaspersky Labs published a report titled *Equation Group: Questions and Answers*, in which it identified and gave a name to a group that it called "the most advanced threat actor we have seen," operating definitively since 2001, but perhaps since as

---

[114] David E. Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site," *New York Times*, January 10, 2009, https://www.nytimes.com/2009/01/11/washington/11iran.html?scp=1&sq=january%202009%20sanger%20bush%20natanz&st=cse, (accessed 4/22/22).

[115] See: Joint Chiefs of Staff, *Information Warfare.*

[116] Bruce Schneier, "Who Are the Shadow Brokers?" *The Atlantic*, May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/, (accessed 4/29/22).

early as 1996.[117] This initial report made no specific claims tying the Equation group to any particular government, but it did find indicators in its malware that indicated Equation "and the Stuxnet developers are either the same or working closely together."[118] Further technical elements of the code cross-referenced with Snowden-leaked NSA materials establishes a strong case that the Equation group is part of the Agency. After the Shadow Brokers leaks, one of the zero-day exploits included in the Equation toolkit was used in two highly publicized cyber attack in 2017, one attributed by the U.S. to the North Korean state[119] and the other to Russian military intelligence.[120] The former attack, known as WannaCry, infected corporate victims' systems globally with ransomware, or malware that blocks the user from accessing their files unless a ransom is paid.[121] The latter, NotPetya, completely wiped victims' files, also attacking with a global reach, although 80% of infections occurred in Ukraine, according to Slovak antivirus vendor ESET.[122] Both attacks caused significant harm to the global economy and the public trust. However, American discourse on cyber operations had hinged so strongly on what the IC was

---

[117] "Equation Group: Questions and Answers," Kaspersky Lab, February 2015, pg 3. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf.

[118] Kaspersky Lab, "Equation Group: Questions and Answers," 13.

[119] Department of Justice, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Department of Justice Press Release, Sept. 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[120] Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Department of Justice Press Release, Oct. 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[121] "What is WannaCry Ransomware?" Resource Center, Kaspersky, https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry, (accessed 1/5/23).

[122] Jane Wakefield, "Tax software blamed for cyber-attack spread," BBC News, June 28, 2017, https://www.bbc.com/news/technology-40428967, (accessed 1/5/23).

doing to keep U.S. systems secure, and these attacks were attributable to two of the nation's most antagonized state-actors, so NSA's role in gathering and refining the zero-day exploits used in these attacks easily became a secondary issue to the active external threat. The consequences of the Shadow Brokers leak is a prime case in which the unique paradoxy of developing weapons in the cyber domain is on full display. The Equation group's toolkit was unknown to the public before the leaks, but could have been rhetorically categorized as the type of offensive capability meant to defend U.S. systems that NSPD–54/HSPD–23 called for. An offensive cyber arsenal can become a liability overnight if other actors become aware of it in a way that a kinetic weapons arsenal does not, yet the decades of cyber discourse leading up to the 2016 leak had not aggressively pursued any solution to this issue, remaining wrapped up in a narrative of building U.S. information systems defenses to shield from the threats of nation-states and major terrorist organizations.

The "Us versus Them" conversation cultivated in the halls of the Capitol and popular sentiment has allowed the Intelligence Community a very long leash throughout history. From Kennedy's Bay of Pigs failure to the exceptionalism of the 'gray' vulnerability market, propagating the fear of what damage an ideological enemy could do allows for "defense" to cast an incredibly broad net. In a public 2016 Senate Committee on Armed Services hearing on cybersecurity, Senator Jack Reed asked Marcell Lettre, the Under Secretary of Defense for Intelligence, and Admiral Michael Rogers, Commander of the United States Cyber Command and NSA Director, if it is a fair assessment that the cyber threat is "a race not just against another nation-state"[123] but really against widespread and relatively inexpensive technology. Admiral

---

[123] *Cybersecurity, Encryption and United States National Security Matters, Hearing before the Committee on Armed Services*, 114th Cong., 2nd Session, 54, (2016), https://www.govinfo.gov/content/pkg/CHRG-114shrg26536/pdf/CHRG-114shrg26536.pdf.

Rogers replied “Yes, sir. I often use the phrase, “Cyber is the great equalizer.”[124] Senator Reed further inquired as to what innovations have taken place to defend from this new threat, with Mr. Lettre answering with broad buzzwords and Admiral Rogers answering with more. The Admiral told the committee that he asks NSA and Cyber Command to look less at individual targets and consider cyber “more as an ecosystem,” but that he “can’t get onto specifics in an open forum.”[125] This characteristically loose language reinforces the idea that policy makers are setting terms for uses of technology that they do not fully understand, while the ecosystem comparison plays into a framework in which it is the major powers of nation-states that should take precedence in assessing the cyber threat. It is the biggest predators that rule their ecosystems. The actual scope of offensive cyber operations pursued by the U.S. is obscured from the public by a heavy blanket of classification, and the policymaking conversation constantly redirects itself to address defense from the threats posed by major rhetorical threat actors. As a result, cybersecurity is undercut and weakened and the IC is given vague and malleable boundaries in its offensive undertakings.

---

[124] Testimony of Admiral Michael Rogers, Commander of the United States Cyber Command and National Security Agency Director, on *Cybersecurity, Encryption and United States National Security Matters,* 54.

[125] Testimony of Marcell Lettre, the Under Secretary of Defense for Intelligence, on *Cybersecurity, Encryption and United States National Security Matters,* 55.

Conclusion

On a warm and sunny February morning, President Barack Obama addressed the crowd in Stanford University's Memorial Auditorium at the 2015 Cybersecurity and Consumer Protection Summit. "The cyber world is sort of the wild, wild West," he told them. "And to some degree, we're asked to be the sheriff."[126] What his remarks failed to address was the other role the United States has played in the cyber domain: the gun-toting cowboy. Beyond the American government's public shaping of a defensive-minded front for conducting operations lies the U.S. Intelligence Community's involvement in cyber offenses.

This paper has intended to give an accessible, overarching perspective on the U.S. tailoring of the cyber world as it developed across the 80s, 90s, and 00s through the 2017 publication of an unclassified Vulnerabilities Equities Process. The internal language of the National Security Agency and the broader Intelligence Community showcases a leveraging of an American tradition of offensive operations justified by the rhetoric of espionage for the sake of security. As the IC honed its rhetoric, it also engaged in developing a cyber arms market out of the reach of the public eye and at the fringes of legality. The United States' part in delineating a gray-market for purchasing zero-days vulnerabilities is predicated on a similar justification of American exceptionalism, allowing it to dictate dynamics in the hacking community and keep knowledge of vulnerabilities from those who would be able to patch them for the sake of classified defense operations. Alongside these internal workings was a developing conversation among policymakers and the public. That discussion has remained focused on the defensive language of the IC, with the rhetorical emphasis on a powerful ideological cyber-adversary

---

[126] Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," (Transcription, The White House Office of the Press Secretary, Stanford University, Stanford, California, February 13, 2015). https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

keeping the stakes of that focus so high as to not deviate from it. The fear of finding the nation vulnerable to a cyber attack has allowed for legislators who acquiesce to intelligence agencies without fully understanding or addressing the specifics.

The cyber domain and the legislation that governs it is a rapidly evolving field. The Biden-Harris Administration released a new National Cybersecurity Strategy as recently as March 21 2023,[127] and the nature of technology is always marching forward. However, as these shifts continue, it is imperative that we continue to look through a historical lens. Understanding that the use of defensive language to obscure offensive fronts is not an isolated incident in the history of the United States should lend itself to a more critical appraisal of what goes on in the Fifth Domain. Misunderstanding and obscuring cyber operations ultimately undermines security, not just on a national infrastructure level, but on all scales, personal to global, by leaving a myriad of loose ends.

In trying to drive home defensive language, the American Intelligence Community has created a myriad of unaddressed paradoxes that have only led to further opacity and debates that fail to address crucial parts of the issue. In an August 2011 issue brief for Atlantic Council titled "Pursuing Cyber Statecraft," cyber researcher Jason Healy, who had just established the Council's Cyber Statecraft Initiative, pointed to the necessary cooperation of technical cyber practitioners and national security professionals for success in creating a "foreign policy for the Internet" – a cooperation between the "geeks" and the "wonks."[128] This type of broader, interdisciplinary conversation is what is needed to properly address the nuances that arise in the

---

[127] White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 1, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[128] Jason Healey, "Pursuing Cyber Statecraft," Atlantic Council, 2011. http://www.jstor.org/stable/resrep03355.

cyber domain, and the productivity of that conversation requires a fuller picture to be understood by the public and its elected representatives.

Part of that nuance, of course, is the legitimate national security interest in covert operations. Ensuring confidentiality from threat actors during a time of conflict is important to an honest defensive effort. However, the treatment of cyber as the perennial wild West treads into territory that threatens democratic principles. This is where the comparison between nuclear power and cyber weapons becomes salient regardless of exact kinetic effects. The U.S. is the first (and only) nation to have used a nuclear weapon, and has necessarily taken public responsibility for it. There was no question as to who dropped Little Boy and Fat Man on Hiroshima and Nagasaki. The public and policymaking conversation surrounding the future of nuclear power was fully informed of this, knowing not only the tangible consequences of its utilization but also that the U.S. was in active possession of these weapons. There is certainly a clear difference between a bomb and a line of code—it is a matter of simple counting when comparing the nuclear power of nation-states, whereas cyber weapons are much more nebulous. There is also the matter of the ease of the latter's accessibility to individual actors and less-resourced nations. However, the U.S. may also have been the first nation to launch a cyber weapon directly at the critical infrastructure of an enemy when it sent the Stuxnet worm into the Natanz Nuclear Plant, but the lack of acknowledgment has meant there has been no discussion parallel to that which occurred regarding nuclear weapons.

The U.S. government's treatment of cyber weapons over the past few decades is more akin to the Manhattan Project, yet those weapons are already being implemented. Like the atomic bomb, the development of offensive cyber capabilities has taken place under cloak and dagger, but in the case of cyber, its actual usage is still withheld from the public under the guise

of national security. Nuclear responsibility has been a long lasting and serious public discussion ever since the weapons were used. The restriction of the general perception of the cyber domain to its need for defensive strategy has stifled a democratic handling of offensive cyber capabilities.

While this thesis has intended to showcase an overarching trend in the way that the IC's offensive cyber operations have defined American engagement in the Fifth Domain, there are innumerable other projects to be undertaken on a more concentrated level regarding any singular component discussed herein. The goal of this paper has been to increase the accessibility of understanding the U.S. engagement in cyberspace to reveal the serious gap in political discussion regarding offensive cyber operations, and to provide for a longer historical arc regarding the rhetorical use of defense as justification.

The stakes remain incredibly high for the need to properly understand cyberspace and hold public officials accountable to fully comprehending the technology they are legislating. This call for more accuracy in assessing the use of cyber weapons can and must translate across all types of operations in the Fifth Domain. The RESTRICT Act, just introduced in Congress on March 7, 2023, is the perfect example of how the "Big Bad American Enemy" narrative is leveraged to obscure egregiously broad capabilities being handed to the government's national security apparatus.[129] The list of "foreign adversaries" the bill purports to defend against is topped by actors that have all been mentioned in the course of this paper: China, Cuba, Iran, North Korea, and Russia. The powers the bill would imbue the Secretary of Commerce with are familiarly vague:

> (a) In General.—The Secretary…shall take action to identify, deter, disrupt, prevent, prohibit, investigate, or otherwise mitigate, including by negotiating,

[129] RESTRICT Act, S. 656, 118th Cong. (2023).

> entering into, or imposing, and enforcing **any** mitigation measure to address **any** risk arising from **any** covered transaction by **any** person, or with respect to **any** property, subject to the jurisdiction of the United States…[130]

The Act goes on to give the Secretary essentially unilateral discretion as to what constitutes such a risk. This sequence of invoking a nation-state threat and subsequently delineating a broadly-interpretable legislation to address the threat has plagued the national approach to cyberspace. The RESTRICT Act is introduced into a public that now has some idea of the transgressions on personal liberty that legislative language like this can allow for in the wake of the Snowden revelations regarding the application of the PATRIOT Act. Continuing to push the understanding of how American cyber operations have been legitimized as defense regardless of actual effects is crucial to protecting the democratic process. There is a popular political adage that has been attributed to Thomas Jefferson, albeit inaccurately,[131] that feels quite pertinent here. While there are a few iterations of the soundbite, the message remains the same: *A well-informed electorate is a prerequisite for democracy.* The responsibility to keep the American public informed has been shirked in the Fifth Domain. Democracy requires a change in the handling of cyber operations.

---

[130] RESTRICT Act, emphasis added.

[131] The phrase seems to have originated from paraphrasing a letter written by Thomas Jefferson to Richard Price on January 8, 1789, retained by the Library of Congress, https://www.loc.gov/exhibits/jefferson/60.html.

Bibliography

Ablon, Lillian and Andy Bogart. " Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits." Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

Albright, David, Paul Brannan, and Chrstina Walrond. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment." Institute for Science and International Security. December 22, 2010. https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

Andres Guerrero-Saade, Juan, Costin Raiu, Daniel Moore, Thomas Rid. *Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage.* Kaspersky Lab, April 3, 2017. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

Badham, John, dir. *WarGames*. 1983; Santa Monica, CA: MGM Home Entertainment, 2008. DVD.

Beck, Neil J. "Espionage and the Law of War." *American Intelligence Journal* 29, no. 1 (2011): 126–36. http://www.jstor.org/stable/26201929.

Böhme, Rainer. "A Comparison of Market Approaches to Software Vulnerability Disclosure." In *International Conference on Emerging Trends in Information and Communication Security*. Berlin, Heidelberg: Springer-Verlag, June 6, 2006. https://dl.acm.org/doi/10.1007/11766155_21.

Böhme, Rainer. *The Economics of Information Security and Privacy*. Heidelberg: Springer Berlin, 2013.

Business Research Company. "The Smart Homes Market is Expected to Reach $205 Billion by 2026, Driven by the Growing Adoption of Smart Devices as per the Business Research Company's Smart Homes Global Market Report 2022." August 18, 2022. https://www.globenewswire.com/news-release/2022/8/18/2501085/0/en/The-Smart-Homes-Market-Is-Expected-To-Reach-205-Billion-By-2026-Driven-By-The-Growing-Adoption-Of-Smart-Devices-As-Per-The-Business-Research-Company-s-Smart-Homes-Global-Market-Rep.html.

CBC News."Russian computer programmer arrested at hacker conference." July 19, 2001. https://www.cbc.ca/news/science/russian-computer-programmer-arrested-at-hacker-conference-1.27667.

Central Intelligence Agency. *(U) INformation Operations and Intelligence Community Related Activities,* Director of Central Intelligence Directive 7/1. Langley, Virginia: Central Intelligence Agency, July 1 1999. https://www.archives.gov/files/declassification/iscap/pdf/2008-049-doc18.pdf

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies." Washington, DC: Office of the Director of National Intelligence, December 12, 2013. Pg. 72. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Clery, Daniel. "Could a Wireless Pacemaker Let Hackers Take Control of Your Heart?" *Science*. February 9, 2015. https://www.science.org/content/article/could-wireless-pacemaker-let-hackers-take-control-your-heart.

Computer Security Resource Center Glossary. "malware." National Institute of Standards and Technology, U.S. Department of Commerce. accessed April 29, 2022, https://csrc.nist.gov/glossary/term/malware.

Defense Advanced Research Projects Agency. "ARPANET." Accessed March 13, 2022. https://www.darpa.mil/about-us/timeline/arpanet.

Department of Justice. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." Department of Justice Press Release. Sept. 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Department of Justice Press Release. Oct. 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Economist. "War in the Fifth Domain." July 1, 2010. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.https://csrc.nist.gov/glossary/term/malware.

Electronic Privacy Information Center. “Presidential Directives on Cybersecurity.” Cybersecurity. Accessed March 31, 2023. https://epic.org/issues/cybersecurity/presidential-directives/.

Fischer, Manuel. “The Concept of Deterrence and Its Applicability in the Cyber Domain.” *Connections* 18, no. 1/2 (2019): 69–92. https://www.jstor.org/stable/26948850.

Friis-Jensen, Esben. “The History of Bug Bounty Programs.” Cobalt. April 11, 2014. https://www.cobalt.io/blog/the-history-of-bug-bounty-programs.

Gerstein, Josh. “Court unseals details on Stuxnet leak probe.” *Politico*. January 12, 2018. https://www.politico.com/blogs/under-the-radar/2018/01/12/stuxnet-leak-probe-court-unseals-details-337912.

Gillis, Alexander S. “What Is the Internet of Things (IoT)?” IoT Agenda. TechTarget. March 4, 2022. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Granick, Jenniver Stisa and Mailyn Fidler. “Changes to Export Control Arrangement Apply to Computer Exploits and More.” *Just Security*. January 15, 2014. https://www.justsecurity.org/5703/export-control-arrangement-apply-computer-exploits/.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. “The Law of Cyber-Attack.” *California Law Review* 100, no. 4 (2012): 817–85. http://www.jstor.org/stable/23249823.

Healey, Jason. “Pursuing Cyber Statecraft.” Atlantic Council. 2011. http://www.jstor.org/stable/resrep03355.

iDefense. “iDEFENSE Security Vulnerability Reporting Policy.” About Us. iDefense. Last Modified Jan 11, 2005. Accessed via Wayback Machine. https://web.archive.org/web/20020802020542/http://www.idefense.com/disclosure.html.

James, Sunil. “Interview with Sunil James, Manager of IDEFENSE's Vulnerability Contributor Program.” Interview by Mirko Zorz. Help Net Security. June 1, 2020. https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/.

Joint Chiefs of Staff. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition*. Washington, DC, DoD: July 4, 1996. https://nsarchive.gwu.edu/document/19024-national-security-archive-joint-chiefs-staff.

Jones, Matthew L. “The Spy Who Pwned Me.” *Limn* 8 (February 2017). https://limn.it/articles/the-spy-who-pwned-me/.

Kaspersky, Eugene. “The Man Who Found Stuxnet - Sergey Ulasen in the Spotlight.” Nota Bene: Notes, Comment and Buzz from Eugene Kaspersky (blog). Kaspersky. November 2, 2011. https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/.

Kaspersky. “What is WannaCry Ransomware?” Resource Center. Accessed January 5, 2023. https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.

Kaspersky. “White Hat Hackers: The Good, the Bad, or the Ugly?” Kaspersky Resource Center. March 30, 2022. https://www.kaspersky.com/resource-center/definitions/white-hat-hackers.

Kaspersky Lab. “Equation Group: Questions and Answers.” February 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf.

Kennedy John F. “Address Before the American Society of Newspaper Editors,” Speech, Washington, DC, April 20, 1961. JFK Presidential Library and Museum. https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-society-of-newspaper-editors-19610420.

Kennedy John F. “Inaugural Address.” Speech, Washington, DC, January 20 1961. JFK Presidential Library and Museum. https://www.jfklibrary.org/learn/about-jfk/historic-speeches/inaugural-address.

Kreuzer, Michael P. “Cyberspace Is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age.” The Strategy Bridge. July 8, 2021. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

Langner, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve*. The Langner Group, November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Libicki, Martin C., Lillian Ablon, and Tim Webb. “The Defender’s Dilemma: Charting a Course Toward Cybersecurity.” Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf.

Marquis-Boire, Morgan, Glenn Greenwald, and Micah Lee. “XKEYSCORE: NSA’s Google for the World’s Private Communications.” *The Intercept*. July 1, 2015.

https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.

McCartney, Robert J. “Computer Hackers Face Spy Charges.” *Washington Post.* August 17, 1989.
https://www.washingtonpost.com/archive/politics/1989/08/17/computer-hackers-face-spy-charges/cad42e6b-73db-48d4-814f-86eb1574ae68/.

Miller, Charlie. “The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales.” Independent Security Evaluators. May 6, 2007.

Mueller, Robert S. *Report On the Investigation Into Russian Interference in the 2016 Presidential Election*. Vol. 1 (Washington D.C.: U.S. Department of Justice, March 2019). https://www.justice.gov/archives/sco/file/1373816/download.

Murphy, Samantha. “Facebook Changes Its 'Move Fast and Break Things' Motto.” Mashable. April 30, 2014.
https://mashable.com/archive/facebooks-new-mantra-move-fast-with-stability#I7FF2Du4IPq6

Nakashima, Ellen and Joby Warrick. “Stuxnet was work of U.S. and Israel experts, officials say.” *The Washington Post*. June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

National Institute of Standards and Technology, U.S. Department of Commerce. “computer network attack (CNA).” Computer Security Resource Center Glossary. Accessed October 10, 2022. https://csrc.nist.gov/glossary/term/computer_network_attack.

National Institute of Standards and Technology, U.S. Department of Commerce. “cyberspace.” Computer Security Resource Center Glossary. Accessed April 29, 2022. https://csrc.nist.gov/glossary/term/malware.

National Institute of Standards and Technology, U.S. Department of Commerce. “vulnerability.” Computer Security Resource Center Glossary. Accessed April 29, 2022. https://csrc.nist.gov/glossary/term/vulnerability.

National Security Agency/Central Security Service. “About NSA/CSS.” Accessed December 2, 2022. https://www.nsa.gov/about/.

National Security Agency/Central Security Service. “Signals Intelligence (SIGINT) Overview.” Accessed December 2, 2022. https://www.nsa.gov/Signals-Intelligence/Overview/.

National Security Agency/Central Security Service. *(U) SIGINT Strategy 2012-2016*. Washington, DC: National Security Agency, February 23, 2012. https://ia600906.us.archive.org/12/items/NSA-SIGINT-Strategy/2012-2016-sigint-strategy-23-feb-12.pdf.

National Security Agency. "Information Warfare: A New Business Line for NSA," *Cryptolog Vol. 20, No.2*. July 1994.
https://nsarchive.gwu.edu/document/27449-national-security-agency-cryptolog-vol-20-no-2-information-warfare-new-business-line.

New York Times. "Mitnick Released from Prison." January 21, 2000.
https://www.nytimes.com/2000/01/21/technology/mitnick-released-from-prison.html#:~:text=Mitnick%20Released%20From%20Prison%20THE,for%20the%20next%20three%20years.

NSA Office of General Council, "CNO Legal Authorities," slide deck, n.d., https://www.aclu.org/sites/default/files/field_document/general_counsel_brief_on_sigint_law_and_information_assurance_law.pdf.

Obama, Barack. "Remarks by the President at the Cybersecurity and Consumer Protection Summit." Transcription, The White House Office of the Press Secretary. Stanford University, Stanford, California, February 13, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

Office of the Director of National Intelligence. "Members of the IC." Accessed December 1, 2022. https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

Perlroth, Nicole. *This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race*. New York: Bloomsbury Publishing, 2021.

Pew Research Center."Public Trust in Government: 1958-2022." Trust in Government. June 6, 2022. https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/.

Pew Research Center. "Two Decades Later, the Enduring Legacy of 9/11." War and International Conflict. September 2, 2021.
https://www.pewresearch.org/politics/2021/09/02/two-decades-later-the-enduring-legacy-of-9-11/#:~:text=Patriotic%20sentiment%20surged%20in%20the,of%20the%209%2F11%20attacks.

Pierdomenico, Jeffrey D. "Applied Feature Extraction for Novel Malicious Software Identification Using Convolutional Neural Networks." *American Intelligence Journal* 37, no. 2 (2020): 55–58. https://www.jstor.org/stable/27087722.

Reeves, Joshua. *Citizen Spy: The Long Rise of America's Surveillance Society.* New York: NYU Press, 2017.

Reuters. "Pentagon Still Under Assault from Hackers." CNN. August 9, 2000. http://www.cnn.com/2000/TECH/computing/08/09/cybersecurity.reut/index.html.

Rid, Thomas. "Cyberwar and Peace: Hacking Can Reduce Real-World Violence." *Foreign Affairs* 92, no. 6 (2013): 77–87. http://www.jstor.org/stable/23527014.

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

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012.

Sanger, David E. "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site." *New York Times*. January 10, 2009. https://www.nytimes.com/2009/01/11/washington/11iran.html?scp=1&sq=january%202009%20sanger%20bush%20natanz&st=cse.

Schneier, Bruce. "Who Are the Shadow Brokers?" *The Atlantic*. May 23, 2017. https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Stouffer, Clare. "What is a zero-day exploit," Emerging Threats. *Norton*. September 3, 2021. https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html#.

TechTarget. "Proof of Concept (PoC) Exploit." Security. TechTarget. May 22, 2019. https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit#:~:text=A%20proof%20of%20concept%20(PoC,and%20protect%20itself%20against%20attacks.

Theohary, Catherine A. *Defense Primer: Cyberspace Operations.* CRS Report No. IF10537. Washington, DC: Congressional Research Service, Updated December 9, 2022. https://sgp.fas.org/crs/natsec/IF10537.pdf

Tomlinson, Ray. Interview by Jordan Spencer Cunningham. OSNews. April 6, 2016. https://www.osnews.com/story/29157/interview-with-ray-tomlinson-on-creeperreaper/.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

U.S. Department of Defense. *Information Warfare (U)*. DOD Directive TS 3600.1. Washington, DC: Department of Defense, December 21, 1992. https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up.

U.S. Department of Defense. *Information Operations (IO) (U)*. DOD Directive TS 3600.1. Washington, DC: Department of Defense, December 9, 1996. https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up.

U.S. Senator Susan Collins Official Webpage. "Senator Collins Announces Position on Iran Nuclear Agreement." September 9, 2015. https://www.collins.senate.gov/newsroom/senator-collins-announces-position-iran-nuclear-agreement.

Vistica, Gregory. "We're in the Middle of a Cyberwar." *Newsweek.* September 20, 1999. 52. Scan from Federal Bureau of Investigation. Cyber Vault Library. National Security Archive. The George Washington University, Washington, DC. https://nsarchive.gwu.edu/document/19293-national-security-archive-federal-bureau.

Wakefield, Jane. "Tax software blamed for cyber-attack spread." BBC News. June 28, 2017. https://www.bbc.com/news/technology-40428967.

Weinberg, Mark D. *Movie Nights with the Reagans: A Memoir*. New York, NY: Simon & Schuster, 2018.

Wellen, Alex. "DEF CON's sport: Spot the fed." ZDNET. July 5, 1999. https://www.zdnet.com/article/def-cons-sport-spot-the-fed/.

White House. *Cybersecurity Policy*. National Security Presidential Directive/NSPD–54; Homeland Security Presidential Directive/HSPD–23. Washington, DC: The White House, January, 8, 2008. https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

White House. *National Cybersecurity Strategy*. Washington, DC: The White House, March 1, 2023.
https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

White House. *National Policy on Telecommunications and Automated Information Systems Security*. National Security Decision Directive 145. Washington, DC: The White House, September 1984. https://nsarchive.gwu.edu/document/21567-document-01-ronald-reagan-national-security.

White House. *Presidential Policy Directive 20 (PPD-20)*. Presidential Policy Directive. Washington, DC: The White House, 2012. https://irp.fas.org/offdocs/ppd/ppd-20.pdf.

White House. *Vulnerabilities Equities Policy and Process for the United States Government*. Unclassified Charte. Washington, DC: November 15, 2017. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

Wilson, Andi, Ross Schulman, Kevin Bankston and Trey Herr. *BUGS IN THE SYSTEM: A Primer on the Software Vulnerability Ecosystem and Its Policy Implications*. Washington, DC: New America, July 2016. https://nsarchive.gwu.edu/sites/default/files/documents/3525982/Document-07-Andi-Wilson-Ross-Schulman-Kevin.pdf.

Zero Day Initiative."Program Benefits." Accessed November 15, 2022. https://www.zerodayinitiative.com/about/benefits/#process.

Zetter, Kim. "Shock! Maturity rules at hack fest." DC10 Articles. DEF CON. Last modified August 13, 2002. https://defcon.org/html/defcon-10/dc-10-articles/dc-10-smh-shocked.html.