CSS CYBER DEFENSE PROJECT

Trend Analysis

The Evolution of US Defense Strategy in Cyberspace (1988 – 2019)

Zürich, August 2019

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Stefan Soesanto

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css.info@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Stefan Soesanto (2019): Trend Analysis: The Evolution of US deterrence strategy in Cyberspace (1988-2019), August 2019, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1 Introduction

This trend analysis provides a historical overview of the evolutionary path US defense strategy has taken in cyberspace since 1988. To a large extent, the analysis utilizes a deterrence-focused approach, rather than one driven by the intelligence community, legal sentiments, or private sector concerns. As such, it primarily looks at cyber-related events relevant to strategic developments within the US Department of Defense (DoD).

Section one explains the DoD's evolution in cyberspace between 1988 and 2008, which was almost exclusively focused on experimentation and adaptation after every incident that hit DoD networks. Section two dives into the policy discrepancies and emerging internal conflicts during the Obama administration on offensive capabilities and cyber deterrence mechanisms. Section three then explores the changes during the first three years of the Trump administration and the introduction of persistent engagement. Section four highlights issues that currently remain unresolved, and section five provides a summary conclusion and several lessons learned.

Disclaimer: This paper does not seek to provide a complete and detailed historical account of US defense strategy pertaining to cyberspace, nor will it contrast the DoD's posture in cyberspace with the department's strategies elsewhere. At its core the paper seeks to answer only one overarching question: How did the DoD's strategy end up in the here and now?

2 In the Beginning (1988-2009)

2.1 AFCERT

Long before the first 'National Strategy to Secure Cyberspace' was released by the Bush administration in 2003, the US Air Force profoundly shaped US thinking on defending, fighting, and winning in cyberspace. As often, the reasons for the Air Force's prominence are multiple. Some point to the Air Force's creation of the Semi-Automatic Ground Environment (SAGE) system in 1954 – the world's first computer network used to "receive data from multiple radars and perform real-time processing to produce targeting information for intercepting aircraft and missiles" (MIT, n.d.). Others will highlight the 1995 document written by the Secretary of the Air Force Widnall and Gen. Fogleman titled 'Cornerstones of Information Warfare' - which for the first time laid out a doctrinal framework for cyberspace by famously recognizing that "before the Wright brothers, air, while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical" (Fogleman & Widnall, 1995).

While both conversion points represent unique events in history, they were not concocted amidst the Wild West days of the Internet. During the 1980s, the DoD like many other government agencies had a hard time protecting its systems against network outages, hacking incidents, and malware infections. At the time, the Pentagon's security thinking was still to large degree locked in an analog age, and thus focused on physical security over network security aspects. As such, the DoD failed to implement basic cybersecurity standards as well as train its system administrators in rudimental computer security practices. Testifying before the Senate Subcommittee on Government Information and Regulation in November 1991, then General Accounting Office (GAO) Director Jack L. Brock noted that, "[DoD] system administration duties are generally part-time duties and that administrators frequently have little computer security background or training. At one site, for example, the system administrator had little knowledge of computers and system administrator responsibilities" (Brock Jr., 1991, p. 4). Brock went on to warn that, "failure to maintain or periodically review audit trails was a key reason why most system administrators were unable to detect the intrusions or determine how long their system had been compromised" (Brock Jr., 1991, p. 4).

In reaction to the Morris worm in 1988[1] a handful of young and bright officers at San Antonio's Lackland Air Force Base (AFB) were finally tasked with writing the next generation cybersecurity policy for the Air Force. None of them knew where to start nor possessed any reliable data to build a comprehensive evidence-based policy document. Roughly 15 years later, Bill Burr at the National Institute of Standards and Technology (NIST) would face a similar conundrum when he had to write the government's guideline on password policy without any empirical data at hand (McMillan, 2017).

At Lackland, the team quickly converged on the notion that "you need to detect when prevention failed, and you need to be able to respond to that in real time" (Lawrence, 2017). In other words, they invented what we now call network security monitoring, e.g. preparing for compromise, not preventing compromise. This operational thinking is inherently anathema to cyber deterrence but deeply ingrained in the field of digital forensics.

From the onset, this new approach faced immense bureaucratic hurdles because system administrators would immediately shut down a system that was under attack, rather than letting an attacker freely rummage through the network to attain forensic data. Thanks to two curious system administrators at Kirkland AFB, the team's persistence and improvisation – some would call it bending the truth - got them the unique chance to monitor a live intrusion when hackers penetrated numerous systems across 34 DoD sites. This first live data collection event of an ongoing hack helped the Airmen figure out what hackers were actually doing in the network, how they were doing it, and what they were after. As one of the team member explained, "we actually – literally and technically – had no authority to do this. No one had really authority to do this" (Lawrence, 2017). The intrusions were eventually traced back to four members of a Dutch hacking group in Geldrop, the Netherlands, but no arrests occurred because the Dutch at the time had no laws barring unauthorized computer access (Markoff, 1991; Lawrence, 2017).

On October 1, 1992, the team was officially designated the Air Force Computer Emergency Response Team (AFCERT) – the first ever military CERT (Bejtlich, 2007). As Col. Brad Pyburn, commander of the 67th Cyberspace Wing at Lackland stressed, "this needed to be done – this idea that we have to have an organization dedicated to cybersecurity and cyber incident response" (Lawrence, 2017). In 1993, AFCERT was incorporated into the newly formed Air Force Information Warfare Center (AFIWC) and its responsibilities grew in lockstep. According to Richard Bejtlich, AFCERT's former chief for real time intrusion detection, the Air Force had well over 100 internet points-of-presence of which AFCERT was monitoring 26 installations by 1995, 55 by 1996, and all of them by 1997 (Bejtlich, 2007). The Navy built up its own CERT on October 1, 1995, by standing up the Fleet Information Warfare Center (FIWC) at Little Creek Amphibious Base in Virginia, and the Army launched its Computer Emergency Response Team (ACERT) when it created the Land Information Warfare Activity (LIWA) on May 8, 1995 (FAS, 2004; Sizer, 1997; Department of the Army, 1997).

In the mid-1990s, few senior government officials in Washington paid serious attention to information warfare in specific and cybersecurity in general. Thus, while a military CERT was certainly good to have for detecting, monitoring, and mitigating intrusions, the DoD was still lacking an overall strategy to respond to and deter incidents from occurring in the first place. 1600 miles away from Lackland AFB, Lt. Gen. Kenneth Minihan set out to change all that when he became Director of the NSA in 1996. As a former commander of Air Force Intelligence Command and director of the Joint Command and Control Warfare Center, Minihan was aptly aware of the existing vulnerabilities and security shortfalls in DoD systems.

2.2 Eligible Receiver 97

Minihan's plan was relatively simple; four NSA teams consisting of 10 people each – with one team deployed aboard a ship in the Pacific - would try to breach the unclassified networks of, among others, US Pacific Command, the National Military Command Center, and the Joint Staff's Intelligence Directorate (NSA, 2017; Kaplan, 2016, pp. 68-69). Using only commercially available equipment and software, the red team's goal was to gain supervisory-level access that would allow them to "interrupt communications, intercept and sent false emails, exfiltrate and delete files, disrupt phone services," and ultimately wreak chaos within DoD's command-and-control systems (Graham, 1998). To make the exercise as realistic as possible the wargame was hidden behind a physical threat scenario consisting of a joint Iranian/North Korean terrorist campaign that included "a real-world hijacking-at-sea of the sea vessel MV National Pride by participant's roleplaying as North Korean Special Operations Forces" (Martelle, 2018).

Minihan's decision to push for the NSA's first ever information operation exercise to test the DoD's cyber defenses did not fall out of the sky. In July 1996, President Clinton had already signed Executive Order (EO) 13010, which recognized that (a) "certain national infrastructures are so vital that their incapacity or

[1] The Morris worm took down ~10% of the internet at the time. It was the first major worm attack, the first distributed denial of service attack, and one of the first dictionary attacks. For a detailed account see: Lee, 2013

destruction [by physical or cyber threats] would have a debilitating impact on the defense or economic security of the United States." and that (b) "many of these critical infrastructures are owned and operated by the private sector" (Federal Register, 1996). To tackle this problem, the EO established the President's Commission on Critical Infrastructure Protection which was tasked to, "assess the scope and nature of the vulnerabilities of, and threats to, [US] critical infrastructures," and develop a working strategy that would define acceptable measures for protection and assured continued cooperation between the government and the private sector (Federal Register, 1996). The findings of the Presidential Commission would ultimately lead to the signing of Presidential Directive 63 (PD-63) in May 1998, which set out - as a national goal - the ability to protect US critical infrastructure from intentional physical and cyberattacks by the year 2003 (The White House, 1998).

It took Minihan more than a year to gain all the bureaucratic sign offs and legal clearances for the Joint Chiefs of Staff (JCS) to authorize a two-week no-notice information warfare campaign within the annually held 'Eligible Receiver' JCS exercise. Meaning, only the red teams, the NSA's lawyers, and the most senior DoD officials knew the cyber component was occurring. Overall, Eligible Receiver 97 (ER97) was specifically designed to exercise four crucial elements: Crisis Action Planning Procedures, Command and Control Relationships, Communications Connectivity, and the DoD's relationships with other Federal Agencies (NSA, 2017). The latter element being especially relevant for the de-confliction of jurisdictional limits and the necessity for intra-agency cooperation in tackling cyber incidents.

On June 9, 1997, the scenario commenced and abruptly ended only four days later with the NSA having penetrated all their targets ahead of time. According to a redacted declassified 10-minute After Action Review video released in August 2018, ER97 Red Team Chief Targeting Officer Keith Abernethy noted that the red team had "the blue team on the run by the third day of the actual exercise. So the need to play all our capabilities was not there. We only played about 30% of what we could have. The message there is it could have been a lot worse" (NSA, 2017). One of the most important lessons learned from ER97 was that the detection of suspicious activity within the DoD's network actually worked quite well - which goes back to the success of AFCERT -, but that DoD's networks had little to no operational security in place and the incident reporting mechanisms were overwhelmed with analytical data coming in even weeks after the exercise had already ended. Abernethy aptly described it as, "they now know the horse is out of the barn after it burned down and the ashes are cold" (NSA, 2017). Similarly, a senior government official quoted in the Washington Post explained that, "coordination within the executive branch was fraught with confusion. We found that within the Defense Department, we lacked the ability to integrate the picture well, and the rest of the government was not prepared at all to handle this. It was a fairly wrenching experience for us" (Graham, 1998).

According to author Frank Kaplan, Air Force brigadier general John Campbell put together a postmortem briefing on ER97, which showed that the DoD was "completely unprepared and defenseless for a cyberattack. The NSA Red Team had penetrated its entire network. Only a few officers had grasped that an attack was going on, and they didn't know what to do about it; no guidelines had ever been issues, no chain of command drawn up" (Kaplan, 2016) To visually get the point across, US Navy Captain Michael Sare, the head of the NSA Red Team in ER97, also "brought along records of intrusions – photos of password lists retrieved from dumpsters, tape recordings of phone calls in which officers blithely recited their password to strangers, and much more" (Kaplan, 2016).

While within the Pentagon the severe vulnerabilities of DoD networks laid bare by the exercise were undeniable, US military planners faced fundamental difficulties in communicating the threat to the wider public due to ER97's classified nature. Writing for the Crypt Newsletter in December 1997, Joseph K for instance argued that, "Eligible Receiver, like the phrase 'electronic Pearl Harbor,' has become a good touchstone for uncritical, unsophisticated journalism on the potential for cyberterrorism to lay low the nation. Although never substantiated with solid proof by Pentagon leadership, it has become an article of faith in the mainstream news media and still appears regularly as prima facie evidence of what hackers could do to plunge the empire into chaos" (Crypt Newsletter, 1999).

While much of ER97 still remains highly classified even 22 years later, three real world events subsequently shaped the political discussion on information security in 1998 (Martelle, 2018).

2.3 Operation Solar Sunrise 1998

In January 1998, tensions between the US and the Iraqi government escalated as Baghdad sought to curtail the work of the United Nations Special Commission inspection teams, which were tasked to verify the destruction of Iraq's biological, chemical, and nuclear weapons programs. On January 13, Iraq went so far as to block an inspection team and accuse the team leader of spying for the US, which in turn prompted the Pentagon to prepare for a sustained series of air- and missile strikes against Iraqi targets within the next few weeks (BBC, 1998; CNN, 1998).

Amidst this political crisis, the Air Force Information Warfare Center (AFIWC) reported an attempted break-in on February 3 into computers at Andrews Air Force Base. Similar intrusions were

subsequently detected on several other DoD systems across the country – pointing toward a coordinated campaign. Talking to the Washington Post, Col. James C. Massaro, then Commander of AFIWC, explained that, "we were seeing things we hadn't seen before. Normally there wouldn't be any correlations right away, but these connections seemed to be going to the same places and using the same techniques" (Graham, 1998). In a 18-minute training video published by the FBI and the National Counterintelligence Center in 1999, Commander of the Air Force Office of Special Investigations (AFOSI) Brigadier General Francis X. Taylor noted that, "it certainly was, given its timing, in concert with our military actions against Iraq, a wake-up call for many of our leaders, both in uniform and otherwise, that this is potentially a very major threat to our ability to execute our missions" (NCC & FBI, 1999). Adding to these concerns, Major General John Campbell clarified that the DoD does "an awful lot of work by email and through unclassified transmission of deployment information. If you take one part of that machine and disable it, you got a real problem trying to make deployment operations take place" (NCC & FBI, 2008). While the DoD was still unsure where the attacks originated from, what their purpose was, and how many hackers they were dealing with, then Deputy Defense Secretary John Hamre informed President Clinton that "the intrusions might be the first shots of a genuine cyber war, perhaps by Iraq as it faced a renewed threat of US airstrikes" (Graham, 1998).

According to the FBI, the attackers were targeting the Sun Solaris 2.4 and 2.6 operating systems by exploiting a known vulnerability common to all UNIX systems, whose patch was made available in December 1997 (NCC & FBI, 1999). The FBI's training video throws a bit of shade onto the DoD by sarcastically noting that, "Pentagon experts haven't focused on the potential backdoor into their systems. Obviously, hackers have" (NCC & FBI, 1999). Under the codename Solar Sunrise, a joint task force was assembled consisting of the FBI, various military services, and the intelligence community. On February 6, investigators uncovered that the intrusions were routed through a number of foreign Internet Service Providers (ISPs) and proxied through US university sites with lax security. Two proxy sites stood out: EMIRNET in the United Arab Emirates – one of the few electronic gateways into Iraq - and SONICNET a commercial ISP in California. According to the FBI, EMIRNET was beyond the reach of US law enforcement but it showed repeated links to a site that was not: Maroon.com - a webpage hosting service in Texas. With the permission of Maroon.com, agents began to monitor all traffic in and out of the network, which revealed unauthorized access from Israel, multiple connections to military sites, and hacking activities similar to the Solar Sunrise intrusions. At SONICNET, agents followed the same procedure after they uncovered numerous passwords and files stolen from Andrews Air Force Base stashed on the network. In an unexpected break, the joint task force was informed that during the initial intrusions into the DoD, SONICNET also received complaints from Harvard and MIT that attacks were launched against their network. SONICNET identified the attackers as two high school kids in California, screen named Makaveli (Mac) and TooShort (Stimpy). Together with the information gained from SONICNET, the joint task force was able to reconstruct several IRC logs between Makaveli, TooShort, and a third person with the screen name Analyzer who was teaching them how to hack. Investigators eventually traced Analyzer back to an ISP in Israel with a possible connection to Maroon.com. On February 25, the media got scent of the story and investigators were forced to raid the home of Makaveli to secure all digital evidence. Talking to AntiOnline.com reporter John Vranesevich, Makaveli described the FBI raid as, "they came into my house, took me in the living room, and starting taking all of the computer equipment from my room. They didn't even leave the phone line leading from the wall to the modem. They took all of my cd's, music cd's, data cd's, my printer, speakers, everything..." (Warner, 2008). Makiaveli and TooShort were subsequently sentenced to three years of probation and 100 hours of community service.

In a sign of defiance, Analyzer went public and gave interviews to numerous reporters. Gadi Shimshon, news editor at Israeli Internet site Walla, met Analyzer face-to-face at a McDonalds in Tel Aviv (Abrams, 1999). In the interview, Analyzer noted that the youngsters in California never really performed any hacking and that the training he provided was rudimental at best. The overall aim, according to Analyzer, was not to spy or destroy, but to use the Pentagon's systems for DDoS attacks against racist and pedophile sites. In an online interview with John Vranesevich, Analyzer was a lot more aggressive, taking about how he hated big organizations, how chaos was a nice idea, and even provided a live demonstration by breaking into a military site during the interview (Warner, 2008). Armed with the electronic evidence that connected Analyzer to the DoD intrusions, the joint task force approached Israeli law enforcement. On March 18, 1998, 18-year old Ehud Tenenbaum aka. Analyzer was arrested in Israel. In 2001, he was sentenced to a mere six months of community service, one year of probation, and a two-year suspended prison sentence (Poulsen, 2001).[2] Writing

[2] Seven years later, Tenenbaum was again arrested, this time in Montreal on six counts of credit card fraud that stole a combined $1.5 million from Canadian banks. In 2009, he was extradited to the US on one count of credit card fraud and computer hacking that scored $10 million from US banks. In 2012, Tenenbaum accepted a plea bargain and was sentenced to time served awaiting judgment. In 2013, Tenenbaum was again arrested. This time in Israel for setting up a large-scale money-laundering scam.

for Securityfocus, Kevin Poulson pointedly summarized the ruling as, "Thursday's sentencing puts a banal capstone on a case that once commanded headlines" (Poulsen, 2001).

With no Iraqi info-warriors to be found, the lessons learned for US defense strategy in cyberspace were few and far in between. Then Deputy Secretary of Defense John Hamre highlighted that, "everything we learned in Eligible Receiver, we learned in Solar Sunrise. In big organizations, you learn things slowly. But there is nothing like a real-world experience to bring the lessons home" (Graham, 1998). Similarly, John A. Serabian, then Junior Information Operations Issue Manager at the CIA, explained before the Joint Economic Committee on Cyber Threats and the US Economy that, "this incident galvanized agencies with foreign and domestic missions alike to coordinate their efforts. […] The U.S. response to this incident required a massive, cooperative effort by the Federal Bureau of Investigation, the Justice Department's Computer Crimes Section, the Air Force Office of Special Investigations, the National Aeronautics and Space Administration, the Defense Information Systems Agency, the National Security Agency, the CIA, and various computer emergency response teams from the military services and government agencies" (Serabian Jr., 2000). In contrast, Michael Warner, Command Historian of US Cyber Command, soberly noted that, "the diplomatic net result of Solar Sunrise was nothing. Calmer heads prevailed, and the United States did not strike Iraq over the misattributed intrusion. What Solar Sunrise proves about crisis instability and escalation is anyone's guess" (Warner, 2017, p. 26).

The one lesson Solar Sunrise did contribute to was to shine a light on the immense knowledge gap between the picket fence scenery of technological progress on the surface and the hacker culture ranging underneath. On May 19, 1998, seven members of the then 6-year-old US hacker think tank – called L0pht Heavy Industries – were invited to testify before the US Senate Committee on Governmental Affairs. This now iconic Senate hearing with Brian Oblivion, Kingpin, Mudge, Space Rogue, Stefan von Neumann, Tan, and Weld Pond, was "a landmark moment for hackers, shunned, derided and loathed by the technology industry" (Fitzgerald, 2017). The highlight of the whole hearing occurred when Senator Fred Thompson (R-Tenn.) asked, "I'm informed that, you think that within 30 minutes the seven of you could make the internet unusable for the entire nation, is that correct?" To which Peiter Zatko (Mudge) answered, "That's correct. Actually one of us with just a few packets. We have told a few agencies about this, [a Border Gateway Protocol (BGP) flaw that would cause a cascading effect through most routers at the time]. We think that this is something the various government agencies should be actively going after. We know the Department of Defense just did a very large investigation into what is known as Denial of Service attacks. […] We contributed a large portion of the information to that actual investigation. Much to our chagrin the learnings from it were instantly classified – which we were giving them largely public information" (CSPAN, 1998).

20 years later Luta Security founder Katie Moussouris gathered four L0pht veterans back in D.C., who all agreed that cybersecurity now is considerably stronger than it was back in 1998 when Mudge warned that "if you're looking for computer security, then the Internet is not the place to be" (Pegoraro, 2018). Reminiscing about the old days, Chris Thomas (Space Rouge) noted in an interview with Business Insider that "the internet was very fragile. It still pretty much is very fragile. And there's probably more than one way to cause similar issues today as it was then" (Szoldra, 2016).

Coincidentally, on the day after L0pht testified in 1998, a Panamsat Galaxy 4 communications satellite malfunctioned and tumbled out of control more than 22,000 miles above the state of Kansas. Testifying before the House Military Procurement and Military Research & Development Subcommittees on June 11, then Deputy Secretary of Defense John Hamre explained that the malfunction "disrupted the satellite's ability to communicate with its customers and set off a cascade of communications failures of a magnitude never seen before. […] By conservative estimates, more than 35 million people lost the use of their pagers, including everyone from school children and repairmen to doctors, nurses, and other emergency personnel. Transplant recipients could not be notified when organs became available. Members of a bomb squad in New Jersey could not be paged to respond to an emergency call. Motorists nationwide could not use their credit cards to pay for gas at the pump. Television and radio broadcasts were broken off. Several Fortune 500 companies and news wires had their business operations impaired" (Hamre, 1998). Laurence Zuckerman at the New York Times put the impact in perspective by writing that "as in a major electricity blackout or the disruption of telephone service, users suddenly realize how much they have taken technology for granted" (Zuckerman, 1998).

2.4 Playing defense: JTF-CND & DISA

Combined with the three events mentioned above, ER97 prompted several changes within the DoD. The most prominent move resulted in the creation of the Joint Task Force Computer Network Defense (JTF-CND) under its designated leader, Air Force brigadier general John Campbell. Writing for CTOvision.com in 2010, Robert Gourley, JTF-CND's first Director of Intelligence, explained the task force's creation by stating that, "[DoD] services had defensive organizations, law enforcement had investigative and

forensic experts, the intelligence community had growing insights, […] but no one had an ability to pull all the info together and coordinate a defense. And more importantly, no organization had command authority with an ability to direct action across DoD" (Gourley, 2010)

Following an extensive review and exchange between the military services, the Pentagon finally decided that the JTF-CND would not be assigned to any unified command but instead be located in Washington D.C. – the home of its supporting agency, the Defense Information System Agency (DISA).[3] According to Lt. Col. Robert J. Lamb, then DISA liaison officer to the JTF-CND, this move allowed "the JTF-CND to be collocated with DISA's Global Operations and Security Center (GOSC) and to leverage DISA's existing global presence with the unified commands, its established liaisons with the law enforcement community, and its network operational view, intrusion analysis, and core technical capabilities" (Lamb, 98/99, p. 3). Tasked with coordinating and directing the defense of DoD computer systems and computer networks, the JTF-CND achieved initial operational capability on December 30, 1998 (DISA, n.d.). With a mere 10 initial staff the JTF-CND was essentially a high-level fusion cell that was supported by DISA but primarily leveraged existing capabilities elsewhere - such as within the National Communications System's National Coordinating Center for Telecommunications (NCS-NCC), the National Military Command Center (NMCC), the NSA, and others - to fulfill its defensive mission (Lamb, 98/99, p. 4; Caton, 2015).[4]

Apart from coordinating the DoD's own defensive mission, the JTF-CND was also tasked to coordinate with the FBI's newly established National Infrastructure Protection Center (NIPC) – which, based on the success of the Solar Sunrise joint task force, was created by PD-63 on May 22, 1998. PD-63 put in place many of the elements future administrations will later expand upon, such as (a) designating federal government liaison officials that will work with the private sector, (b) appointing a national and several functional coordinators to de-conflict interagency cooperation, and (c) creating the National Infrastructure Assurance Council - which will continuously advise the White House. It also set in motion the creation of procedures that would allow every federal agency to conduct vulnerability assessments on their own government computer and physical systems, and tasked the intelligence community with "elevat[ing] and formaliz[ing] the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure" (The White House, 1998).

On the law enforcement side, PD-63 directed the Department of Justice and the Department of the Treasury to "compare state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles." It additionally authorized the FBI "to expand its current organization to a full scale National Infrastructure Protection Center (NIPC)," which "depending on the nature and level of a foreign threat/attack, […] may be placed in a direct support role to either DOD or the Intelligence Community" (The White House, 1998).

The DoD received little attention within PD-63, as critical infrastructure protection was primarily seen as a civilian task, and thus outside the military's purview.[5] It would take another 20 years for this mindset to change. Under PD-63, the Department of Defense was merely directed to (a) "assist federal agencies in the implementation of best practices for information assurance within their individual agencies," (b) work with the Department of Commerce "to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards," and (c) consult the Department of Transportation on "a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System" (The White House, 1998).

With the JTF-CND becoming fully operational in June 1999, and after realizing that the task force was lacking crucial connections to the military services and regional warfighting commanders, the JTF-CND was placed under the auspices of US Space Command to fulfill its DoD-wide mission of stopping and mitigating computer network attacks (CNA) and computer network exploitation (CNE) (Caton, 2015, p. 3). In April 2001, US Space Command was additionally saddled with the DoD's offensive mission of conducting computer network attacks, which subsequently forced the JTF-CND to be renamed into the Joint Task Force – Computer Network Operations (JTF-CNO). While little to nothing is known about the JTF-CNO's offensive cyber operations, Maj. Gen. James D. Bryan, founding Commander of JTF-CNO, noted in a speech in 2012 that, "shortly [after 9/11] the nation was at war […] and that really changed the dynamics for us. We were about a 70/30 split between defense and offense […] We'd actually treated cyber offensive missions as a kinetic effect generating thing in terms of progress. [But] it still made us think: whether or not we achieve the desired effect on the offensive side, the nation was not at risk. If we fail on the

[3] DISA is a combat support agency of the DoD. The agency provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations.

[4] JTF-CNO was designated to have 24 staff when fully operational, but increased to more than 150 during the height of post-9/11 conflict.

[5] The DoD did create a voluntary program for Defense Industrial Base companies to cooperate directly with the Pentagon.

defensive side, the nation would be at risk" (Healey, 2015, p. 60)

The DoD's offensive mission eventually moved away from US Space Command around 2003, when President Bush signed the Change-2 plan to the 2002 Unified Command Plan, which among other items merged US Space Command into the existing US Strategic Command (USSTRATCOM).[6] In April 2004, the JTF-CNO was again transformed and renamed into the Joint Task Force – Global Network Operations (JTF-GNO), in line with a new concept of operations for network organizations (NetOps) to protect the DoD's global information grid. On June 18, 2004, then Secretary of Defense Donald Rumsfeld, designated the director of DISA to become the commander of the JTF-GNO, cementing the task force's focus on defensive support. According to Air Force General Kevin P. Chilton, throughout its existence the JTF-GNO "ensured support to operation Iraqi Freedom, Operation Enduring Freedom in Afghanistan, Operation Noble Eagle [Homeland security support after 9/11], and the overall global war on terror" (Carden, 2010).

2.5 Playing offense: JFCC-NW & NSA

While open sources are clear on what the DoD did to strengthen its glasshouse, little is known as to what lessons learned the NSA took away from ER97 in terms of hurling bigger stones. PD-63 for example merely directed the NSA on the defensive end to "provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations" (The White House, 1998). What we do know is that post-9/11, the Bush administration published several documents and passed a number of legislations that shaped US policies in cyberspace. Most notably (1) the Patriot Act, which expanded the NSA's surveillance reach to fight terrorism at home and abroad, (2) the Homeland Security Act, which established the Department of Homeland Security (DHS) in March 2003, and (3) the publication of the National Strategy to Secure Cyberspace, which among other items tasked defense and security agencies to (a) strengthen their counterintelligence efforts, (b) improve their attribution capabilities, (c) deconflict interagency coordination, and (d) announced that the US "reserves the right to respond in an appropriate manner" to nation state, terrorist groups, and other adversarial cyberattacks (US Congress, 2001; DHS, 2015; The White House, 2003).

While these policies fundamentally altered the US posture in cyberspace, it is unclear whether the affected agencies were actually getting a bigger hammer, or merely gained the legal capacity to build parts of the hammer without ever assembling it. GAO for instance designated the creation of DHS as high risk because the government had to "transform 22 agencies—several with major management challenges—into one department. Failure to effectively address the management and program challenges that arose from this effort could have serious consequences for U.S. national security" (GAO, n.d.). On the US declaratory policy end Alex Wilner, Assistant Professor of International Affairs at Carleton University, recently argued that, "while these pronouncements may have been obligatory, for the purposes of coercion they are also inherently weak" (Wilner, 2019, p. 14). Unsurprisingly, the growing role of the NSA under the Bush administration also negatively affected the DoD. Around 2003, the DoD's offensive cyber mission was transferred from the JTF-CNO to a Network Attack Support Staff that was controlled by STRATCOM but housed at the NSA headquarter at Fort Meade, Maryland (Healey, 2013, p. 65). By January 2005, the Support Staff consolidated into the Joint Functional Component Command – Network Warfare (JFCC-NW) and was commanded by the Director of the NSA (STRATCOM, 2018). Thus, while on the DoD's defensive end, the Director of DISA served as dual head for the JTF-GNO, the Director of the NSA operated on the DoD's offensive end as the dual head of the JFCC-NW.

On paper, the DoD's cyber portfolio was neatly split and clearly organized, but in terms of operational outcomes it produced a history of mix results. On the one hand, the JTF-CNO performed well against the multitude of viruses and worms that hammered networks worldwide during the early 2000s. According to Maj. Gen. James D. Bryan, the Code Red worm - which is believed to have started in 2001 at a university in Guangdong, China, and infected more than 975.000 servers worldwide – "was really an eye opener. It had a huge effect. But we were able to contain it in a couple of hours in terms of its impact on the DoD" (Rhodes, 2001, p. 12; Healey, 2013, p. 59). On the other hand, a series of coordinated computer intrusions in 2003 into the unclassified systems of DISA, the Army Space and Strategic Defense Command, several DoD contractors, the State Department, Sandia National Laboratory, and numerous other government systems, went undetected for months. Shawn Carpenter, former network security analyst at Sandia National Laboratories - who independently investigated the network breach and was subsequently wrongfully terminated by Sandia for sharing his findings with federal law enforcement - traced the attackers back to three Chinese routers in

[6] For more information on the Change-2 and 2002 Unified Command Plan see: Drea et al. 2013. History of the Unified Command Plan 1946-2012. Joint History Office, Office of the Chairman of the Joints Chiefs of Staff

Guangdong (Vijayan, 2007; Thornburgh, 2005). According to Carpenter, "most hackers, if they actually get into a government network, get excited and make mistakes. Not these guys. They never hit a wrong key" (Thornburgh, 2005).

Dubbed operation Titan Rain, the 2003 breaches are widely recognized to be the first instance of Chinese state-sponsored espionage against US government targets (CFR, 2005). However, according to a 2008 State Department cable published by Wikileaks in December 2010, a group called Byzantine Candor, also known as Comment Group, might have actually been the first Chinese state-linked actor to have conducted computer network exploitation against US government targets.[7] According to the Air Force Office of Special Investigation (AFOSI), the group was based in Shanghai, linked to the People's Liberation Army's Third Department, and was targeting US government organizations since late 2002 (Wikileaks, 2008; Riley & Lawrence, 2012). The Cyber Threat Analysis Division (CTAD) within the US State Department's Bureau of Diplomatic Security additionally noted that, "in the U.S., the majority of the systems [Byzantine Candor] have targeted belong to the U.S. Army, but targets also include other DoD services as well as [Department of State], Department of Energy, additional [US government] entities, and commercial systems and networks" (Wikileaks, 2008).

On the offensive end, the JFCC-NW was confronting its own existential problems when in May 2004 videos depicting the execution of American freelance journalist Nicholas Berg popped up on jihadi websites. In an interview with Wired in 2005, ret. US Army Col. Lawrence Dietz, former Deputy Commander of NATO's Information Campaign in Bosnia, explained that, "there are some tremendous questions being raised about this […] On whether they (JFCC-NW) have the legal mandate or the authority to shut these [Islamic] sites down with a defacement or a denial-of-service attack" (Lasker, 2005). It would take another 15 years for the DoD to attain the legal authorities necessary to DDoS commercial servers (Nakashima, 2019).

All this notwithstanding, the DoD published its first cyber strategy in 2006 - called the National Military Strategy for Cyber Operations (NMS-CO) - which expressed the Pentagon's intent to achieve "military strategic superiority in cyberspace" to ensure that "adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace" (JCS, 2006, p. 13). In line with this thinking, the NMC-CO stipulated that the DoD "will deter malicious adversary use of cyberspace, while promoting freedom of action and trust and confidence in U.S. cyberspace operations. Through deterrence, DOD seeks to influence the adversary's decision-making processes by imposing political, economic, or military costs; denying the benefits of their actions; and inducing adversary restraint based on demonstrated U.S. capabilities" (JCS, 2006, p. 13). Asked during his House confirmation hearing in 2010 as to whether the US has ever demonstrated capabilities in cyberspace in a way that would lead to deterrence of potential adversaries, NSA Director and Head of US Cyber Command Gen. Keith Alexander answered, "not in any significant way. We have conducted exercises and war games, and responded to threats, intrusions, and even attacks against us in cyberspace. Law Enforcement and the Counter-Intelligence community have responded to intrusions and insider threats. Even industry and academia have attempted to `police' the Internet. How all of these have deterred criminal actions, terrorists, hostile intelligence entities, and even nation states cannot be systematically measured" (Alexander, 2010). In essence, the DoD's glowing words on paper did not translate into credible action in practice. As far as open source information goes, the DoD did not conducted any offensive operations in cyberspace prior to the discovery of Stuxnet in 2010.

On cross-domain issues the NMS-CO significantly moved the goal post by declaring for the first time that the "DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace. Kinetic actions can be either offensive or defensive and used in conjunction with other mission areas to achieve optimal military effects" (JCS, 2006, p. 15; Lawson, 2011). Put plainly, the DoD will kill enemy cyber operators and will bomb enemy network infrastructure if it helps to achieve US strategic superiority in cyberspace. To some degree the DoD's 2006 Quadrennial Defense Review (QDR) also outlined this approach when reading between the lines. For example, the QDR stated that DoD needs capabilities to (a) "shape and defend cyberspace", (b) "locate, tag and track terrorists in all domains, including cyberspace," and that (c) "any attack on U.S. territory, people, critical infrastructure (including through cyberspace) or forces could result in an overwhelming response" (DoD, 2006, p. 31, 23, 25). In 2015, a US drone strike took out ISIS hacker Junaid Hussain at a petrol station in Raqqa, Syria. The incident marked the first publicly known case of an enemy cyber operator being specifically targeted on the kinetic battlefield (Carlin, 2019).

2.6 Estonia 2007

In May 2007, the DoD realized that it was missing a significant part of the cyber defense puzzle. While its NATO ally Estonia was pummeled for 22-days straight

[7] In 2013, Mandiant identified the Comment Group as the earliest activities by the 2nd Bureau of the PLA's 3rd Department – also known as Unit 61398 – or APT1

with a barrage of politically motivated DDoS attacks for moving a Soviet-era monument from the center of Tallinn to its outskirts, policy analysts within the alliance divided into two groups (Ottis, 2008; Soesanto, 2018). The European side vigorously argued that the DDoS attacks were the beginning of cybermageddon and evidence of Russia's hybrid warfare doctrine (Peters, 2007). On the US end meanwhile, analysts highlighted that the United States was regularly dealing with DDoS attacks of a similar, or greater, magnitude than the ones that hit Estonia (Poulsen, 2007).

The Estonian episode also revealed the stark contrast between the technical community and those responsible for articulating national security policies. Writing for Wired in 2007, Kevin Poulson observed that, "Estonia's computer emergency response team responded to the junk packets with technical aplomb and coolheaded professionalism, while Estonia's leadership … well, didn't. Faced with DDoS and nationalistic, cross-border hacktivism – nuisances that have plagued the rest of the wired world for the better part of a decade – Estonia's leaders lost perspective. Here's the best quote, from the speaker of the Estonian parliament, Ene Ergma: 'When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing'" (Poulsen, 2007). James Lewis, Director of the Technology and Public Policy Program at the CSIS, succinctly summarized the issue by noting that, "the idea that Estonia was brought to its knees – that's when we have to stop sniffing glue" (Schwartz, 2007).

After two months of back and forth, the cybermageddon narrative eventually collapsed under its own weight and Estonian politician had to admit - in the absence of any technical evidence - that attributing the DDoS attacks to the Russian government was shaky at best (Poulsen, 2007; The H Security, 2007). Asked during his House confirmation hearing in 2010 as to whether the DoD is "considering an 'extended deterrence' model similar to that which [the US has] offered through the U.S. nuclear umbrella," Gen. Keith Alexander noted that, "I am not aware of any efforts to develop an extended deterrence model for cyber" (Alexander, 2010). It would take another six years for NATO to make the small step of recognizing cyberspace as a military domain of operations, and an additional two years for US Cyber Command to send defensive teams to Ukraine, Northern Macedonia, and Montenegro, to counter Russian meddling in the 2018 US midterm elections. (NATO, n.d.; Lyngaas, 2019a; Myre, 2019).

2.7 The Comprehensive National Cybersecurity Initiative 2008

In January 2008, President Bush signed National Security Presidential Directive 54 (NSPD-54) and the Homeland Security Presidential Directive 23 (HSPD-23) to better coordinate the US government and improve the "capability of the United States to deter, prevent, detect, characterize, attribute, monitor, interdict, and otherwise protect against unauthorized access to National Security Systems, Federal systems, and private-sector critical infrastructure systems" (The White House, 2008, p. 1).

Domestically, the directives cemented DHS' role by ordering the Secretary of Homeland Security to "lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems" (The White House, 2008, p. 5). Nothing really changed for the Secretary of Defense, as his responsibilities still covered: "directing the operation and defense of the DoD's information enterprise", "providing indications and warning information to DHS regarding threats originating or directed from outside the United States," and coordinating with the Secretary of State to "work with foreign countries and international organizations on international aspects of cybersecurity" (The White House, 2008, p. 7 & 6).

On the specific issue of deterrence in cyberspace, the directives created the Comprehensive National Cybersecurity Initiative (CNCI). A declassified summary of the CNCI lists among other items that within 270 days, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, "shall define and develop a comprehensive and coordinated strategy to deter interference and attacks in cyberspace" for the President's approval. And that within 90 days, the Director of the Office of Science and Technology Policy (OSTP) shall "develop a detailed plan to coordinate classified and unclassified offensive and defensive cyber research" (The White House, 2008, p. 10). Given that neither documents are publicly accessible, it is anyone's best guess what policies were outlined and recommended.

Overall, the CNCI's established numerous cyber-related initiatives that converged on three major goals. First, establishing a "front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government." Second, defending against "the full spectrum of threats by enhancing US counterintelligence capabilities and increasing the security of the supply chain for key information technologies." Third, strengthening the future cybersecurity environment by "working to define and develop strategies to deter hostile or malicious activity in cyberspace" (The President of the United States, 2008, p. 1 & 2). With the US government scrambling to translate the CNCI into practical outcomes, the Pentagon experienced its most significant network breach to date.

2.8 Operation Buckshot Yankee 2008

Wired's Noah Shachtman was the first to get wind of the story when in mid-November 2008 US Strategic Command suspended the use of all removable devices from their networks in an effort to contain a "virus called Agent.btz"; the worm had infected non-government Windows systems since May 2008. According to internal DoD emails, service members were specifically ordered to "cease usage of all USB storage media until the USB devices are properly scanned and determined to be free of malware" (Shachtman, 2008).

A week later, Julien E. Barns over at the LA Times broke the surrounding story. According to Barns, Agent.btz malware "struck hard at networks within US Central Command" – which oversees US involvement in Iraq and Afghanistan - and "penetrated at least one highly protected classified network" (Barns, 2008). The incident even forced senior DoD leaders to take "the exceptional step of briefing President Bush this week on a severe and widespread electronic attack on Defense Department computers that may have originated in Russia - an incursion that posed unusual concern among commanders and raised potential implications for national security" (Barns, 2008). Speaking on the condition of anonymity, one defense official noted that, "this one was significant; this one got our attention" (Barns, 2008).

In an article for Foreign Affairs in September 2010, titled 'Defending a New Domain,' former Deputy Defense Secretary William Lynn III described the incident as "the most significant breach of U.S. military computers ever" (Lynn, 2010). According to Lynn, "the flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. […] That code spread undetected on both classified and unclassified systems establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control" (Lynn, 2010).

In December 2011, the story evolved further when Ellen Nakashima over at the Washington Post reported previously unknown details. According to Nakashima, NSA analysts first became aware of Agent.btz when the malware 'beaconed' out on the Secret Internet Protocol Router Network – which DoD and State use for transmitting lowly-classified material – and the Joint World Wide Intelligence Communication System – which "carries top-secret information to U.S. officials throughout the world" (Nakashima, 2011). Given that both networks maintain only a very thin connection to the public internet, the malware had an extremely low success rate of connecting to its outside host while facing a very high probably of being discovered in the process of beaconing out.

The Post's article remains fuzzy on many significant details which are still unresolved, such as whether the Agent.btz version found on the DoD's network was different from the one infecting non-government systems in the wild, and how much information on how many systems was actually compromised or compiled for exfiltration (if any at all). It is also unclear if the malware was tactically deployed by a foreign operative to infect a specific box – meaning the infection of CENTCOM's network was the result of collateral damage – or whether the broad infection of the DoD's network was the goal.

Today, we do know that, from a technical point of view, there exists somewhat of a lose connection between Agent.btz and other spyware products - such as Red October, Turla, and Flame/Gauss. Alexander Gostev, then Chief Security Expert of the Global Research and Analysis Team at Kaspersky Labs, neatly summarized in 2014 that "it is possible to regard Agent.btz as a certain starting point in the chain of creation of several different cyber-espionage projects. The well-publicized story of how US military networks were infected could have served as the model for new espionage programs having similar objectives, while its technologies were clearly studied in great detail by all interested parties. Were the people behind all these programs all the same? It's possible, but the facts can't prove it" (Gostev, 2014). Interestingly enough, in the aftermath of the 2016 US Presidential election, the FBI and DHS released a Joint Analysis Report, which for the first time attributed the use of Agent.btz to Russian civilian and military intelligence services (DHS/NCCIC & FBI, 2016, p. 4).[8]

To neutralize Agent.btz and protect the DoD networks, the Pentagon reportedly turned to the NSA's Advanced Network Operations team (ANO) – which hunts down suspicious activity within government networks – and the NSA's Tailored Access Operation team (TAO) – which specializes in computer network exploitation (CNE). Under the header of Operation Buckshot Yankee, ANO succeeded on October 25 in writing a program that recognized the beaconing signal of Agent.btz and transmitted a response – putting the malware into a permanent slumber. TAO meanwhile "identified new variants of the malware [outside the DoD's wire] and helped network defenders prepare to neutralize them before they infected military computers" (Nakashima, 2011).

The JFCC-NW also proposed several options to "use offensive tools to neutralize the malware on non-military networks, including those in other countries" (Nakashima, 2011). Based on sources familiar with the

[8] Note: The Joint Analysis Report is widely seen as a bad report. See: Soesanto. 2017. "Grizzly Steppe - One step forward, two steps back?" Medium.com, August 17, 2017.

conversation, the Washington Post reported that senior leaders dismissed this approach, because "Agent.btz appeared to be an act of espionage, not an outright attack, and didn't justify such an aggressive response" (Nakashima, 2011).

Following Operation Buckshot Yankee, the JTF-GNO was placed under the JFCC-NW in order to "better integrate and synchronize defensive cyber operations." Testifying before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats, and Capabilities in May 2009, NSA Director General Keith Alexander explained that, "we had the defense and the operations in one command under the joint task force global network operations. And that task force got one level of intelligence and could see one part of the network. Operating on the other side was the Joint Functional Component Command Net Warfare trained at a different level with different intel insights at a different classification level. Same network, two organizations […] we've brought those two together, merged those. […] The offense and defense cannot be different here because these operations will occur in real time. And I think we have to be prepared to do that. It's not time to say, oh, this is your mission and you're on your own" (Alexander, 2009). In October 2010, both the JTF-GNO and the JFCC-NW were dissolved and incorporated into the newly formed US Cyber Command (STRATCOM, 2018).

3 The Obama administration (2009-2017)

3.1 Cyberspace Policy Review

Recognizing the persistent challenges in the cyber domain, the incoming Obama administration ordered a 60-day 'clean-slate' review in January 2009 to assess existing U.S. cybersecurity policies and structures. Four months later, the White House eventually published the resulting Cyberspace Policy Review which aptly summarized that, "the status quo was no longer acceptable" and that "the United States must signal to the world that it is serious about addressing [the cybersecurity] challenge with strong leadership and vision" (The President of the United States, 2009, p. iii). Building significantly upon the Bush administration's Comprehensive National Cybersecurity Initiative (CNCI), only two recommendations really stuck out of the 75-page Review: (a) Developing a US strategy that is "designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force" (The President of the United States, 2009, p. 20). And, (b) "anchoring and elevating leadership for cybersecurity-related policies" by appointing a cybersecurity policy coordinator at the White House (The President of the United States, 2009, p. 7).

Apart from these two recommendations, Eric Greenwald, then Chief Counsel for the House Permanent Select Committee on Intelligence, noted that the Review was "not fundamentally different from previous iterations of cybersecurity strategy that the U.S. government has issued over the past 12 years. [...] we have heard all of this before – more than once" (Greenwald, 2010, p. 41-42). As Greenwald explains it, "the 60-Day Review itself did not delve deeply into the particulars of the initiatives in the CNCI. Rather, it offered a more general discussion on many of the same broad policy goals that have been outlined in the previous iterations of cybersecurity strategy and leaves the hard work and difficult decisions to the recently named Cybersecurity Coordinator" (Greenwald, 2010, p. 55-56). A GAO report published in July 2010, titled 'Cyberspace: United State faces challenges in addressing global cybersecurity and governance,' arrived at the same conclusion by highlighting that "until the Cybersecurity Coordinator provides top-level leadership, there is an increased risk that U.S. agencies will not formulate and coordinate U.S. international cybersecurity-related positions as envisioned in the President's Cyberspace Policy Review" (GAO, 2010, p. 31). Similarly, the report criticized that "although multiple federal entities are engaged in a variety of

international efforts that impact cyberspace governance and security, the U.S. government has not documented a clear vision of how these efforts, taken together, support overarching national goals" (GAO, 2010, p. 32).

3.2 Operation Olympic Games

While discussions on the Cyberspace Policy Review were taking place in public, the Obama administration tackled Iran's nuclear enrichment program in secret. With operational efforts already implemented under the previous administration, President Obama ordered the deployment of Stuxnet sometime in early 2009. Co-developed by the NSA and Israeli Signal Intelligence Unit 8200, Stuxnet damaged an estimated 1000 Iranian centrifuges between 2009 to August 2010 - when Iran blocked all outbound traffic from its infected sites (Sanger, 2012; Healey, 2013, p. 218). Overall, the strategic objective of Stuxnet hovered somewhere between, temporarily delaying Iran's nuclear enrichment program and averting a unilateral preemptive Israeli air-raid on the one hand, and coercing Tehran away from acquiring nuclear weapons on the other. Washington clearly succeeded on the former but substantially failed on the latter.

Dubbed Operation Olympic Games, the deployment of Stuxnet put a large chunk of foremost theoretical thought into actual practice. On the technical end, Symantec noted that Stuxnet "represents the first of many milestones in malicious code history – it is the first to exploit four 0-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator" (Falliere et al., 2011, p. 55). On the political end, Stuxnet proved that an offensive cyber operation can create kinetic effects, that an attack against critical infrastructure can be conducted during peacetime, and that repercussions on the bi- and international level can be minimal to non-existent. Robert M. Lee, then Air Force Cyberspace Operations Officer, aptly summarized that, "a nation has never been in this situation before. The case studies do not exist. The context has not existed. […] How the [United States] moves forward from here, how it responds to threats, and what strategies are developed will all impact the future of cyber deterrence and the entire cyberspace domain" (Lee, 2012).

But was Stuxnet supposed to deter? For the US, Stuxnet's deployment was all about stalling and/or ending Iran's nuclear program in a clandestine non-attributional way. On the other hand, the Iranian government did not have the technical means and intelligence necessary to retaliate in a tit-for-tat fashion against US/Israeli infrastructure assets at the time. At best, Stuxnet falls into the posturing category of deterrence-by-reputation, which goes back to Thomas Schelling's argument in 1966 that a country's reputation and the resolve to deter are formed through past-iterated encounters - and the expectation of future crises - between the same two actors (Schelling 1966, p. 125). At worst, the US government willfully ignored or discounted any subsequent escalation dynamics in cyberspace.[9]

Hidden behind the veil of secrecy, it is important to note that - on the defensive end - neither the White House nor the DoD or NSA deemed it relevant enough to read-in DHS when Stuxnet spread to US systems. Thus, testifying before the Senate Committee on Homeland Security and Governmental Affairs in November 2010, Sean McGurk, then Acting Director at the National Cybersecurity and Communications Integration Center (NCCIC) at the U.S. Department of Homeland Security, explained that the "malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware. […] [The Industrial Control Systems]-CERT immediately began to analyze the code and coordinate actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers. […] The salient lesson of Stuxnet, and other emerging threats, is that the [coordinated services and supports plan's] mission and coordination between DHS and the control systems community are vital to our efforts to protect the nation's critical infrastructure" (McGurk, 2010, p. 11-12).

3.3 Constraint – PPD-20

The irony of Stuxnet - as Kim Zetter put it in her book 'Countdown to Zero Day' – was that "while Obama was authorizing this new attack against Iran's computer systems, he was also announcing new federal initiatives to secure cyberspace and critical infrastructure in the United States – to protect them, that is, from the very sort of destruction that Stuxnet produced" (Zetter, 2014, p. 334). In May 2011, the White House began to streamline its own narrative by releasing the President's International Strategy for Cyberspace. The document bluntly stated that, "the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and

[9] Note: First exposed in Alex Gibney's documentary 'Zero Days' and later somewhat corroborated by The New York Times, Stuxnet might have just been a smaller operation within a much larger battle plan dubbed 'Nitro Zeus' (Szoldra, 2016; Sanger & Mazzetti, 2016). However, given the absence of any technical evidence to support the narrative that NSA had penetrated everything from Iran's command and control systems, air defenses, power grids, and financial systems etc., and was merely waiting for Washington's go-ahead, Nitro Zeus could be mere NSA posturing or the closest the world has come to unilateral cyber warfare

systems, dissuading and deterring malicious actors, and reserving the right to defend these viral national assets as necessary and appropriate" (The President of the United States, 2011, p. 12). On the deterrence-by-denial[10] end, the Strategy proclaimed that the US will "continue to strengthen [its] network defenses and [its] ability to withstand and recover from disruption and other attacks" (The President of the United States, 2011, p. 13). Clarifying that, when warranted, "we reserve the right to use all necessary means - diplomatic, informational, military, and economic - as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. **In so doing, we will exhaust all options before military force whenever we can**; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible" (The President of the United States, 2011, p. 14).

To implement the objectives of the strategy, President Obama signed five executive orders and Presidential directives authorizing offensive and defensive actions in cyberspace. The most prominent of the five was Presidential Policy Directive 20 (PPD-20), which went into effect in October 2012 (The President of the United States, 2012). The classified document entered the public domain on June 7, 2013 when it was leaked by Edward Snowden and published by The Guardian. The directive laid out the guiding principles for US offensive and defensive cyber effects operations (OCEO & DCEO).

Having learned from the Stuxnet blowback, PPD-20 noted that, "DCEO and OCEO with potential implications for U.S. networks shall be deconflicted as appropriate and coordinated with DHS, appropriate law enforcement agencies, and relevant sector-specific agencies" (The President of the United States, 2012, p. 13). On the policy end, the directive significantly slowed down - and to some extent even curtailed - US offensive operations in cyberspace by defining several comprehensive policy criteria that would guide a new mandatory inter-agency deliberation process – including criteria on impact, risks, methods, geography and identity, transparency, authorities, and civil liberties - while ultimately placing final authority in the President's hands (The President of the United States, 2012, p. 13). As such, PPD-20 for example stated that DCEO and OCEO shall consider, but not be limited to: "Assessments of intelligence gain or loss, the risk of retaliation or other impacts on U.S. networks or interests (including economic), impact on the security and stability of the Internet, and political gain or loss to include impact on foreign policies, bilateral and multilateral relationships (including Internet governance), and the establishment of unwelcome norms of international behavior" (The President of the United States, 2012, p. 13). In the context of deterrence, PPD-20 overcorrected in response to the widespread criticism that Stuxnet was carried out without adequately assessing the operation's larger implications. Over the coming years, the intricate green-lighting process set-up by PPD-20 would go on to frustrated military brass and lawmakers on both sides of the isle.

3.4 US Cyber Command and DoD

Parallel to the policy realignment in the White House, the DoD and NSA consolidated their cyber operations in the newly established US Cyber Command (CYBERCOM). Instead of replicating the NSA's capabilities within Cyber Command and the four service components – which was dismissed as financially inefficient and an unnecessary multiplication of the same capabilities -, the setup of Cyber Command followed the logic of the dual headed-structure already in place at the JFCC-NW. Which made the Director of the NSA also the head of US Cyber Command.

Housed at Fort Meade, Maryland, CYBERCOM's mission was defined as "direct[ing] the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (DoD, 2010). Conceptualized with an authorized staff of 937, and including the operational cyber components in the four service branches, CYBERCOM totaled over 11,000 men and women in 2013 (Alexander 2013, p. 1).

Despite its broad mission objective and large staffing, CYBERCOM did not initially turn out to be the agile giant it was supposed to be. In 2010, Gen. Keith Alexander, then Head of the NSA and CYBERCOM, explained to the House Armed Services Committee that, "it is not my mission to defend today the entire nation. Our mission at Cyber Command is to defend the Defense Department networks. If we are tasked by either the secretary or the president to defend those networks, then we'd have to put in place the capabilities to do that. But today, we could not" (Alexander, 2010). On the offensive end, Alexander highlighted that "any operations that Cyber Command does, defensively, we have the standing rules of engagement laid out there. And any other operations that we would do would have to be done under an executive order through the secretary of Defense and the president" (Alexander, 2010).

[10] Deterrence-by-denial aims at disrupting an adversary's cost-benefit calculation to the degree that it either disincentives an attack, due to the increased likelihood of failure or subsequently exhausts an attacker's time, patience, and/or resources.

In an attempt to mirror and integrate the White House's cyber policies into the DoD's strategic approach in cyberspace, then Deputy Secretary of Defense William J. Lynn III, unveiled "the Department's first ever Strategy for Operations in Cyberspace" on July 14, 2011 (Lawson, 2011).[11] Ominously titled 'Department of Defense Strategy for Operations in Cyberspace,' the 13-page document discusses five strategic initiatives: (1) treat cyberspace as an operational domain, (2) employ new defense operating concepts to protect DoD networks and systems, (3) partner with other agencies and the private sector to enable a whole-of-government cybersecurity strategy, (4) build robust relationships with US allies and partners to strengthen collective cybersecurity, and (5) leverage the nation's ingenuity through an exceptional cyber workforce (DoD, 2011a).

The document naturally faced criticism from all sides. Sean Lawson over at Forbes for instance highlighted that the 2006 National Military Strategy for Cyberspace Operations (NMS-CO) was actually the first DoD strategy, and that in many ways the NMS-CO provided much clearer definitions than the new document did - on for example what the cyber domain entails and what precise strategic goals the DoD wants to attain. According to Lawson, "the seeming confusion over whether or not the 2011 strategy is actually the 'first' and its relationship to the 2006 strategy is indicative of ongoing confusion within and among DoD components when it comes to cyber strategy, roles, missions, authorities, and objectives" (Lawson, 2011). A GAO report published the day after Lynn unveiled the DoD's strategy, highlighted the DoD's overall policy dilemma by noting that "while at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention 'cyberspace operations,' none contained a sufficient discussion of cyberspace operations" (GAO, 2011, p. What Gao found). The DoD's 2011 strategy also left many important questions unanswered. House Representative James Langevin (D-R.I.) therefore asked in a statement: "What are acceptable red lines for actions in cyberspace and what resources can and will the Defense Department provide to the Department of Homeland Security, private companies, and international partners to enable their own defense? Does data theft or disruption rise to the level of warfare or do we have to see a physical event, such as an attack on our power grid, before we respond militarily?" (Serbu, 2011). Similar criticism was voiced by Alan Chvotkin, executive vice president of the Professional Services Council - a group representing government contractors - who noted that, "this strategy is at best a compilation of previously adopted departmental plans and missions covering other critical components of the department's operational domain" (Serbu, 2011). Richard Clarke, former National Coordinator for Security, Infrastructure Protection and Counter-terrorism, even went so far to note that the strategy was not a strategy at all (Lawson, 2011).

Four months after the DoD's public relations disaster, the Department published its 'Cyberspace Policy Report' pursuant to the National Defense Authorization Act for the fiscal year 2011. The report does a much better job at articulating, mirroring and integrating the President's 'International Strategy for Cyberspace.' Overall, it focuses heavily on highlighting the DoD's efforts on deterrence-by-denial, deterrence by de-legitimization,[12] and potential cross-deterrence measures.[13] As such, it states that, "the U.S. is working with like-minded nations to establish an environment of expectations, or norms of behavior, that increase understanding of cyber doctrine, and guide Allied policies and international partnerships. At the same time, should the 'deny objectives' element of deterrence not prove adequate, DoD maintains, and is further developing, the ability to respond militarily in cyberspace and in other domains" (DoD, 2011b, p. 2). In terms of deterrence-by-reputation, the report merely highlights that "the Department has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests" (DoD, 2011b, p. 5). On the relationship between the NMS-CO and the 2011 strategy, it sadly sowed more confusion by stating that, "the Joint Staff does not intend to modify the National Military Strategy for Cyberspace Operations at this time. To guide the Department's activities in cyberspace, the Secretary of Defense has approved the Department of Defense Strategy for Operating in Cyberspace" (DoD, 2011b, p. 10).

In January 2013, the DoD's Defense Science Board Task Force rattled the cage when it published its take on the DoD's cyber strategy. Titled, 'Resilient Military Systems and the Advanced Cyber Threat,' the report's findings were largely ignored by the policy crowd in Washington. The DSB for example noted that "DoD red teams, using cyber attack tools, which can be downloaded from the Internet, are very successful at defeating our systems," and that "U.S. networks are

[11] The DoD also published a classified version of the Department of Defense Strategy for Operations in Cyberspace. (See: DoD DSB, 2013, p. 32). As of this writing, the document has not been declassified.

[12] Deterrence by de-legitimization, also known as naming and shaming, has its origins in the deliberations on creating norms and rules for state behavior in cyber space (ex. UN GGE talks) and the discussions on the applicability of international law to the cyber domain (ex. the two Tallinn Manuals). The overall aim of de-legitimization measures are threefold: To create a general principle of restraint, raise the reputational costs of bad behavior, and shrink the battlespace to only encompass military combatants in line with the law of armed conflict

[13] Cross-domain deterrence describes the spectrum of strategic measures that a nation state is willing to leverage outside the cyber domain in reaction to an event in cyberspace. This can range from criminal indictments of cyber-operatives and trolling campaigns in the information warfare space, to leveling economic sanctions and launching nuclear strikes.

built on inherently insecure architectures with increasing use of foreign-built components" (DoD DSB, 2013, p. 1). The report therefore concluded that, "with present capabilities and technology, it is not possible to defend with confidence against the most sophisticated cyber attacks" (DoD DSB, 2013, p. 31).

The solution the DSB put forward was to raise the confidence level for selected systems - such as the US nuclear deterrent, conventional strike capabilities, and command-and-control systems elemental to the functioning of government - to be "protected from cyberattacks and therefore available for deterrence" in support of an escalation ladder (DoD DSB, 2013, p. 32). For all other systems, defenses ought to be incrementally raised while network monitoring and intrusion detection would provide situational awareness. On the offense end, the DSB advocated for "build[ing] a world-class cyber offensive capability with well-defined authorities and rules," that would be supported by "refocus[ing] intelligence collection to understand adversary cyber plans and intentions, and to enable counter strategies" (DoD DSB, 2013, p. 32). In essence, the DBS realized that "a defense-only strategy against this threat is insufficient to protect U.S. national interests and is impossible to execute" (DoD DSB, 2013, p. 1 & 40). To this end, it stipulated that cyber deterrence "require[s] an escalation framework with associated signaling and red thin-line strategies, and credible survivable military capabilities" (DoD DSB, 2013, p. 40).

3.5 The DoJ, State, and Treasury

The Obama administration did not heed the call of the DSB report and instead emphasized deterrence-by-denial and deterrence by de-legitimization measures as outlined in the President's International Strategy for Cyberspace. The latter measures were primarily guided by the applicability of international law to the cyber domain, and the differentiation between legitimate state conduct in cyberspace – such as espionage for non-commercial purposes – and illegitimate activities, stretching from destructive attacks, disruptions of critical infrastructure, and commercial espionage. Overall, the aim of deterrence by de-legitimization measures are threefold: To create a general principle of restraint, raise the reputational costs of bad behavior, and shrink the battlespace to only encompass military combatants in line with the law of armed conflict.

While the President's strategy was sound theoretically, it failed at deterring foreign adversaries from continuously hitting US assets.

Between 2012-2013, members of Iran's Revolutionary Guard Corps DDoS'd at least 46 major financial institutions in the United States, including JPMorgan Chase, Wells Fargo, and American Express (Volz & Finkle, 2016). According to then Attorney General Loretta Lynch, "these attacks were relentless, they were systematic, and they were widespread. They threatened our economic well-being and our ability to compete fairly in the global marketplace" (Johnson, 2016). In August 2013, the same group obtained remote access to the supervisory control and data acquisition system for the Bowman Avenue Dam in Rye Brook, New York. Luckily enough, the dam's sluice gate was manually disconnected for maintenance at the time of the intrusion (Thompson, 2016). In January 2016, the DoJ unsealed indictments against seven Iranian operatives for the 2013 DDoS attacks against the US financial sector and the intrusion into the Bowman Avenue Dam (DoJ, 2016).

In September 2013, a group working "directly for Iran's government [or] acting with the approval of Iranian leaders," hacked into the unclassified Navy Marine Corps Intranet. According to the Wall Street Journal, it took the Navy four months to purge the hackers from the network – no classified information was exfiltrated (Barnes & Gorman, 2013). In February 2014 Iranian hackers penetrated the systems of the Sands Hotel and Casino and wiped three-quarters of the company's servers. This incident marked the first time a foreign adversary conducted a destructive cyberattack against a US company (Brandom, 2014).

In November, a group of North Korean state-sponsored hackers breached the computer systems of Sony Pictures entertainment in response to the Sony-backed film 'The Interview.' According to the Washington Post's Andrea Peterson, the attackers "stole huge swaths of confidential documents from the Hollywood studio and posted them online in the following weeks -- exposing them to everyone from potential cybercriminals to journalists who have been poring through the documents and reporting everything from the details of recent film productions to the extent of the employee data laid vulnerable on the Internet" (Peterson, 2014). In September 2018, the DoJ unsealed a criminal complaint against North Korean citizen Park Jin Hyok for being "a member of [the North Korean] government-sponsored hacking team known to the private sector as the 'Lazarus Group,'" and being actively involved in the group's numerous malicious activities including the 2014 attack against Sony Pictures Entertainment (DoJ, 2018b).

The North Korean playbook would be used two years later, when Russian military intelligence (GRU) leaked internal emails from the Democratic National Convention to influence the 2016 US Presidential Election (Nakashima & Harris, 2018). On July 13, 2018, the US District Court for the District of Columbia indicted 12 GRU officers for "gain[ing] unauthorized access (to "hack") into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election" (DoJ, 2018a).

In April 2015, the US Office of Personnel Management discovered that its networks were breached and the attackers exfiltrated the private information of 21.5 million former, current, and prospective government employees as well as their spouses and close relatives (Fruhlinger, 2018). The stolen data also included 5.6 million fingerprints and other biometric data that unlike passwords and social security numbers cannot be changed (Peterson, 2015). In June 2018, the DoJ mistakenly claimed that data from the OPM hack was used by a woman in Maryland to obtain fraudulent loans (Miller, 2018). So far none of the OPMs stolen data has appeared in the wild which suggests that most likely a foreign government agency is possessing and trying to utilize the data for operational support. According to the then Director of National Intelligence James Clapper, China was the "leading suspect" behind the breach (Sciutto, 2015). In August 2017, the DoJ arrested Chinese citizen Yu Pingan at Los Angeles International Airport for being a malware broker and proving Chinese hacking groups with - among others - the rarely-used Sakula Trojan that has been used in the OPM hack (Condon, 2017). Given the amount of data exfiltrated, and the inherent documentation chaos within the OPM, the Chinese government will have to expedite immense resources to sift through and categorize the millions of documents to turn them into something that might be operationally useful.

As Gen. Nakasone eloquently summarized it, "in a period of 10 years, nation-states progressed from exploitation, to disruption, and finally to destructive attacks against [the United States] in cyberspace (Nakasone 2019b, p. 5)."

US defense planners had little to offer to combat the onslaught as the White House was unwilling to categorize the numerous incidents mentioned above as touching the right to self-defense or necessitating the use of force for deterrence purposes. Testifying before the House Intelligence Committee on September 10, 2015, then head of NSA and US Cyber Command, Admiral Rogers therefore noted that, "there is still uncertainty about how would you characterize what is offensive and what is authorized. Again, that boils down, ultimately, to a policy decision. And to date we have tended to do that on case-by-case basis." Adding that, "a purely reactive defensive strategy is not, ultimately, I think, going to change the dynamic where we are now. And the dynamic we find ourselves in now, I don't think is acceptable to anyone" (CSPAN, 2015, min. 44:37-45:13). In his testimony before the Senate Select Intelligence Committee two weeks later, Admiral Rogers further explained that, "I think we as a nation need to have a very public discussion about how do we achieve this idea of deterrence. Because if we do not change the current dynamic, we are not in a good place. We have to fundamentally change the dynamic we are dealing with now" (CSPAN, 2015, min. 42:05-42:19).

With US Cyber Command unable to respond offensively to the barrage of cyber intrusions and attacks, the Department of Justice eventually stepped onto the plate. On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five Chinese military operatives for computer hacking and economic espionage against "six American victims in the U.S. nuclear power, metals and solar products industries." According to then U.S. Attorney General Eric Holder, the case "represents the first ever charges against a state actor for this type of hacking," while FireEye noted that the five defendants belonged to "exactly the same unit, designation, and location identified in the 2013 Mandiant report, APT1: Exposing One of China's Cyber Espionage Units" (DoJ, 2014; Bejtlich, 2014).

Note: While companies do occasionally attribute attacks to certain governments and agencies, there are no set standards as to how, when, and why they will make an attribution call. Given that attribution assessments could produce political fallout, might create business repercussions, and may even lead to the targeting of individual researchers, not every company will publish everything they know about every state-linked actor. As Martijn Grooten, an editor with VirusBulletin, correctly observed, "everyone makes a choice" (Bing, 2018).

Over the years, the indictment of nation-state cyber-operatives for crimes committed against US-based entities has become the fulcrum to hold individuals personally liable for their actions taken and orders followed. While some analysts claim this to be evidence of a concerted naming and shaming strategy by the US government (e.g. deterrence by de-legitimization), the DoJ's overarching legal aim is, and has always been, to attribute attacks and to hold individuals - both adversarial cyber-operators that hit non-military targets and foreign civilians that hit US entities – accountable in a US court. As Tonya Ugoretz, deputy assistant director of the FBI's Cyber Division, eloquently put it, "nothing says attribution like an indictment" (Lyngaas, 2019b).

Parallel to the DoJ's efforts, the State Department increased its momentum within the UN General Group of Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Since 2004, the Group has been trying to formulate and reach consensus on international norms for state behavior in cyberspace. In 2013, the UN GGE's 15 members finally agreed that "international law, and in particular the Charter of the United Nations, is applicable" to cyberspace, and that "international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities" (UNGA, 2013, p. 8). In 2015, the group's 20 member states – including China and Russia – published their last and most comprehensive consensus report.

Testifying before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy on May 25, 2016, Christopher Painter, then Coordinator for Cyber Issues, proudly noted that, "the United States and its allies have made substantial progress in recent years towards advancing our strategic framework of international cyber stability" (Painter, 2016).

In April 2015, the Treasury Department made its entry onto the cyber stage when President Obama signed Executive Order 13694, which provided the Secretary of the Treasury the authority to block the property of certain persons engaging in significant malicious cyber-enabled activities (The White House, 2015a). Prior to EO 13694, the administration merely defended its imposition of economic sanctions by mentioning hostile cyber conduct as one among many justifying reasons. In January 2015 for example, President Obama signed EO 13687 on 'Imposing Additional Sanctions With Respect To North Korea,' which mentions North Korea's "destructive, coercive cyber-related actions during November and December 2014" (The President of the United States, 2015, p. 819). Yet, EO 13687 was never specifically directed at North Korean cyber operators. EO 13694 changed this dynamic. Between April 2015 and January 2017, the US Treasury Department's Office of Foreign Assets Control (OFAC) imposed cyber-related sanctions on a mere 6 individuals and 5 companies hailing all from Russia (OFAC, 2016).

The White House itself also became pro-active by putting cybersecurity on the agenda when Chinese President Xi Jinping visited the US in September 2015. During the Obama-Xi meeting both Presidents agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" (The White House, 2015b). Hailed by some analysts as a stepping stone toward 'cyber arms control,' the real-world impact of the Obama-Xi meeting was generally met with skepticism (Nye Jr., 2015). Given an "overall decline in China-based intrusion activity against private and public sector organizations since mid-2014," FireEye notably assessed in July 2016 that "rather than viewing the Xi-Obama agreement as a watershed moment, we conclude that the agreement was one point amongst dramatic changes that had been taking place for years. We attribute the changes we have observed among China-based groups to factors including President Xi's military and political initiatives, the widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government" (FireEye, 2016, p. 10 & 15).

The DoD meanwhile published another cyber strategy in April 2015, which did not bring anything substantially new to the table. On deterrence, the strategy highmindedly noted that, "the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems." As a policy document, the 2015 strategy was operating on such a high threshold level that its posturing rhetoric of "the United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law," sounded more hollow than ever before (DoD, 2015a, p. 11). President Obama would go on to use similar rhetoric in response to Russia's interference in the 2016 US Presidential election by noting that, "I think there is no doubt that when any foreign government tries to impact the integrity of our elections . . . we need to take action. […] And we will — at a time and place of our own choosing. Some of it may be explicit and publicized; some of it may not be" (Eilperin, 2016). Ultimately, even the President's posturing did not materialize into anything substantial – apart from another set of economic sanctions and expelling 35 Russian diplomats (Sanger, 2016).

The inability of the Obama administration to both deter and effectively respond to Russia's hacking and information warfare operation during the 2016 Presidential election, collapsed the President's entire vision for a de-escalatory deterrence approach. Talking to the Washington Post, President Obama's former chief of staff Denis McDonough for example noted that, "it is the hardest thing about my entire time in government to defend. […] I feel like we sort of choked" (Miller et al., 2017). Michael McFaul, US ambassador to Russia between 2012 to 2014, meanwhile decried that "the punishment did not fit the crime […] Russia violated our sovereignty, meddling in one of our most sacred acts as a democracy — electing our president. The Kremlin should have paid a much higher price for that attack. And U.S. policymakers now — both in the White House and Congress — should consider new actions to deter future Russian interventions" (Miller et al., 2017). Probably to most accurate assessment as to why the Obama administration failed in its deterrence approach was coming from Obama's deputy national security adviser Ben Rhodes, who noted that, "in many ways … we dealt with this as a cyber threat and focused on protecting our cyber infrastructure. Meanwhile, the Russians were playing this much bigger game, which included elements like released hacked materials, political propaganda and propagating fake news, which they'd pursued in other countries" (Miller et al., 2017).

President Obama's most powerful response was actually one that was never triggered. According to a Washington Post report from June 2017, President Obama did authorized two offensive cyber missions.

One 'loud' short-term operation "designed to be detected by Moscow but not cause significant damage," whose primary aim was to remind Moscow of US capabilities in cyberspace (Miller et al., 2017). And a 'silent' long term operation, under which the President directed the NSA, CIA, and U.S. Cyber Command to develop a plan to disrupt Russian critical infrastructure. While little to nothing is known about how far the relevant agencies progressed in their build-up to execute both missions, the strategic overlap between Obama's preparatory cyber-approach toward Russia, and the Bush administration's preparations to strike Iran in and through cyberspace, are glaringly similar in terms of strategic posturing and passing the political buck. According to the Washington Post, "the project, which Obama approved in a covert-action finding, was still in its planning stages when Obama left office. It would be up to President Trump to decide whether to use the capability" (Miller et al., 2017). As far as open source goes, President Trump never triggered the silent option nor halted it. The loud option might have been triggered in mid-2018 in preparation for the US mid-term elections.

4 The Trump administration (2017-2019)

When President Trump took office in January 2017, the incoming administration faced immense public pressure to aggressively confront the Russian Federation. Wobbling between agreeing with the intelligence community that Russia interfered in the US Presidential election and arguing that it "could have been other people and other countries, […] nobody really knows for sure," punishing Moscow took a backseat during the first year of the new administration (Calamur, 2018). In contrast, the political discussions on a much more aggressive cyber-deterrence posture picked up steam in the DoD, Congress, and ultimately the White House.

In February 2017, the DoD's Defense Science Board published the final report of its Task Force on Cyber Deterrence. Overall, the Task Force recycled many recommendations that were already highlighted by the DSB report in 2013. This should not come as a real surprise as James Gosler – then senior fellow at Johns Hopkins - co-chaired both DSB reports, and James Miller, who co-chaired the 2017 report was the DoD's Under Secretary of Defense for Policy when the 2013 report was published.

On deterrence-by-denial for instance, the report notes that "the unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures" (DoD DSB, 2017, p. 4). Overall, the Task Force put forward eight guiding principles stretching from "deterrence by cost imposition requires credible response options at varying levels" to "norms and rules of the road may be both viable and highly valuable" (DoD DSB, 2017, p. 7-8). The one principle that stuck out in both tone and substance, was the notion that "responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation (and quite possibly intelligence loss), but not responding carries near certainty of suffering otherwise deterrable attacks in the future" (DoD DSB, 2017, p. 7). Reading between the lines, the report was a not so subtle criticism of the Obama administration, and clearly framed expectations for the way forward under the Trump administration.

Testifying before the Senate Committee on Armed Services on May 9, the Head of US Cyber Command Admiral Rogers, explained that, "when we say prevent [an attack on US critical infrastructure] … it is one of the reasons why deterrence becomes so important. The goal should be, we want to convince actors that you do not want to do this, regardless of whether you could be successful or not. It is not in your

best interests, and you do not want to engage in this behavior" (CSPAN, 2017). When asked to define what would constitute an act of war in the cyber domain, Rogers answered that "we haven't reached a broad consensus on how you would define in clear actionable terms what an act of war within the cyber arena looks like. […] What I look to do ... could we define a set of criteria, intent, impact, the tactic or techniques that were used, […] to help us define this, rather than this […] general conversation we often tend to find ourselves in" (CSPAN, 2017). When specifically queried on the impact of PPD-20, Rogers frankly noted that "I am the first to acknowledge [that the PPD-20 is] not the fastest process in the world. […] Everything I am hearing from the team is that they acknowledge that the structures currently in place are not fast enough" (CSPAN, 2017).

On May 11, 2017, President Trump signed EO 13800 titled 'strengthening the cybersecurity of federal networks and critical infrastructure.' Among other items, the EO directed the Secretaries of State, Defense, Treasury, Commerce, Homeland Security, and the Attorney General, to submit a report to the President on the "Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats" (The President of the United States, 2017). While the report remains classified, the Office of the Coordinator for Cyber Issues within the Department of State released an unclassified 3-page overview on May 31, 2018. According to the overview, the report determined that "strategies for deterring malicious cyber activities require a fundamental rethinking," to achieve the desired end state of (a) "a continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies;" and (b) "a significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force" (State Department, 2018, pp. 1-2). Not only did the report move the goalpost on what kind of foreign state activities the US ought to deter, but it also fundamentally blurred the threshold of the use of force – if not even aimed at entirely erasing it over time. Curiously enough, the summary never mentions the discussion on norms and state behavior in cyberspace – which the State Department has championed over the past decade. To bring about the re-think on deterrence in cyberspace, the report proposed to develop "a broader menu of consequences that the United States can swiftly impose following a significant cyber incident, and taking steps to help resolve attribution and policy challenges that limit U.S. flexibility to act" (State Department, 2018, p. 1). While the summary does not mention any specific measures, it does highlight that the US "should develop tailored strategies for deterring each of its key adversaries in cyberspace" (State Department, 2018, p. 3). Meaning, that the US response to malicious conduct by a North Korean state operative ought to be markedly different from malicious conduct by a Russian state operative. In theoretical terms, this approach moves the deterrence-by-reputation logic into the domain of deterrence-by-punishment,[14] as state reputation and the resolve to deter are formed through past-iterated encounters - and the expectation of future crises - between the same two actors.

In June 2017, the fifth session of the UN GGE ended without the release of a consensus report, as fundamental disagreements on the applicability of International Humanitarian Law, self-defense, and state responsibility pertaining to cyberspace, proved unbridgeable. In her final remarks to the group, Michele Markoff, Deputy Coordinator for Cyber Issues in State Department, explained that, "I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions. That is a dangerous and unsupportable view, and it is one that I unequivocally reject" (Markoff, 2017). Speaking at Cyber Week in June 26, 2017, US Homeland Security Advisor Tom Bossert noted in reference to the UN GGE collapse that, "it's time to consider other approaches. We will also work with smaller groups of likeminded partners to call out bad behavior and impose costs on our adversaries. We will also pursue bilateral agreements when needed" (Bossert, 2017). One day later, NotPetya – the most devastating cyberattack in history according to Wired - spread around the globe (Greenberg, 2018). Bossert explained that, "while there was no loss of life, [NotPetya] was the equivalent of using a nuclear bomb to achieve a small tactical victory. That's a degree of recklessness we can't tolerate on the world stage" (Greenberg, 2018).

4.1 Elevation of US Cyber Command

In August 2017, the DoD initiated the elevation of US Cyber Command to become the nation's 10th Unified Combatant Command (Garamone & Ferdinando, 2018). Three months later President Trump approved the new Unified Command Plan, which turned CYBERCOM into a Joint Force Provider "responsible for the planning and execution of global cyberspace operations" (Rogers, 2018, p. 8). Meaning, CYBERCOM gained the "authority to balance risk across the Joint Force by focusing cyber capacity where it is most needed, both in time and space, [and it] allows it to deter and respond to or

[14] Deterrence-by-punishment comes down to one simple thing: "*You hurt me, I'm going to hurt you worse. I have the tools to do it, and if you don't believe me, than step over the line*," as Vice Chairman of the Joint Chiefs of Staff Gen. Paul J. Selva eloquently put it (Garamone, 2017).

preempt cyber threats in all phases of conflict and to synchronize cyberspace operations globally" (Rogers, 2018, p. 14). On May 4, 2018, CYBERCOM was official elevated (Lange, 2018). As a functional combatant command, it was now allowed to directly engage with foreign partner equivalents and deploy liaison officers to key foreign partners to broaden collaboration and interoperability (Rogers, 2018, p. 13).

In January 2018, the DoD released an unclassified summary of the National Defense Strategy (NDS), subtitled 'Sharpening the American Military's Competitive Edge.' In relation to the cyber domain, the NDS acknowledged that the "homeland is no longer a sanctuary" from "malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion" (DoD, 2018a, p.3). To counter this new normal the NDS noted that the DoD will invest in capabilities to "gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks" (DoD, 2018a, p.6). The latter being especially significant, as the threshold for the use of force de-facto dissolved for the DoD.

In March 2018, US Cyber Command outlined its new strategic vision to 'Achieve and Maintain Cyberspace Superiority.' In many ways, the new vision was fundamentally build on the 2006 NMS-CO. Acknowledging that "adversaries continuously operate against [the US] below the threshold of armed conflict […] without fear of legal or military consequences," the vision put forward the strategic concept of persistent engagement to confront the day-to-day great power competition in cyberspace (US Cyber Command, 2018a, p. 3). As the document explains, "superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver" (US Cyber Command, 2018a, p. 6). Realizing that such a drastic offensive shift in the US deterrence posture would face its fair share of criticism, the vision pre-emptively noted that, "the Command makes no apologies for defending US interests […] in a domain already militarized by our adversaries" (US Cyber Command, 2018a, p. 10).

Parallel to the DoD's change in attitude, the US Senate started drafting its version of the National Defense Authorization Act 2019 (NDAA) in June 2018. Recognizing the deterrence shortcomings under the Obama administration, the Senate specifically crafted Section 1621, which under point b directed the executive branch to "plan, develop, and **demonstrate** response options to address the full range of potential cyber attacks" (US Senate, 2018, p. 713). Under point d, the sentiment appeared again in the form of "the United States shall develop and **demonstrate**, or otherwise make known to adversaries of the existence of, [US] cyber capabilities" (US Senate, 2018, p. 714). The Senate also expressed under Section 1623 its wish that the administration ought to implement an active defense posture in cyberspace to "disrupt, defeat and deter" attacks conducted by the Russian government (US Senate, 2018, p. 720). The final version of the NDAA not only implemented all the Senate's language (in Section 1636 and 1642), but it also called for an active defense posture against the Chinese, North Korean, and Iranian governments (US Congress, 2018, Stat. 2132). Robert Chesney, Professor in Law at the University of Texas, explained in Lawfare that, "while Congress cannot make the president issue orders to take more aggressive actions in response to malicious foreign cyber activities, it can express its wish that he would do so and it can pave the way a bit by granting preauthorization for some such responses. That's what Section 1642 is all about" (Chesney, 2018). On the political stage, Congress fully endorsed and supported CYBERCOM's new vision of persistent engagement.

On August 15, 2018, President Trump finally rescinded PPD-20 and replaced it with the still classified National Security Presidential Memorandum 13 (NSPM-13). Although, as of this writing, it is unclear what exact process now governs the authorization of offensive cyber operations, NSPM-13 certainly pushed the decision-making authority down the chain of command. As one former US government official explained to the Wall Street Journal, "it's not so much to let Cyber Command off the leash as to let [the head of] Cyber Command act like any other combatant commander" (Volz, 2018). For the State Department, the elimination of PPD-20 translates into a significant blow to the department's ability to block offensive cyber operations that might conflict with international law and undermine the discussions on norms for state behavior in cyber space. As one FBI official explained to Politico, "that policy piece of paper became a scapegoat for bigger issues. Whether people liked it or not, the PPD-20 process highlighted some very real legal issues regarding the extent of Cyber [Command's] authority to take certain actions in cyberspace" (Geller, 2018).

4.2 Defending Forward & Persistent Engagement

On September 18, 2018, the DoD published its new Cyber Strategy 2018. Echoing CYBERCOM's new vision, the DoD explained under the header of 'strategic competition in cyberspace,' that the Department "seeks to preempt, defeat, or deter malicious cyber activities targeting US critical infrastructure that could cause a significant incident regardless of whether that incident would impact DoD's warfighting readiness or capability" (DoD, 2018b, p. 2). In essence, the DoD's primary role on homeland defense shifted from supporting DHS domestically to a persistent posture of defending

forward. While it is still unclear how exactly DoD intends to coordinate its activities with the private sector at large, the DoD's posture of persistent engagement does include the notion of "working with the private sector and our foreign allies and partners to contest cyber activity [outside the US wire]" (DoD, 2018b, p. 4).

Two days after the publication of the DoD's take, the White House released the President's National Cyber Strategy, which in many ways reflected the failure of the UN GGE and shifted the administration's focus on deterring adversaries in cyberspace. As such, the strategy notes, under the header of 'Preserve peace through Strength,' that although the US will continuously work toward norms, "we must also work to ensure that there are consequences for irresponsible behavior that harms the US and our partners" (The President of the United States, 2018, p. 21). The Strategy thus envisioned a cyber deterrence initiative under which the US will "work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors" (The President of the United States, 2018, p. 21). On October 4, the DoJ in conjunction with the Royal Canadian Mounted Police coordinated the criminal indictments against three Russian military operatives for the OPCW hack, and a coordinated release of public attribution assessments by the Five Eyes members and the Netherlands (DoJ, 2018c).

Note: According to Shannon Vavra over at Cyberscoop, current deputy assistant secretary of state for cyber and international communications and information policy, Rob Strayer, noted on August 1, 2019 that "one of the State Department's priorities for the remainder of 2019 is to build this joint [cyber deterrence] coalition." All in all the goal is to have more than 25 countries involved and "get a corpus of a general agreement […] on sharing information, responsive actions, and how we would identify the types of malicious activity that we want to counter" (Vavra, 2019).

It did not take long for Cyber Command to put its own vision into practice. In the context of protecting the 2018 US mid-term elections, the Command first deployed cyber defense teams to the Ukraine, Northern Macedonia, and Montenegro. According to the current head of US Cyber Command, Gen. Nakasone, this was the "the first time, we sent our cyberwarriors abroad to secure networks outside the DOD Information Network" (US Senate, 2019, p. 21). Tasked with increasing interoperability and helping the three countries to defend their own networks, the teams also collected intelligence on US adversaries. In addition, the Command furthermore specifically targeted individual Russian operatives, in an attempt to "deter them from spreading disinformation to interfere in elections, [by] telling them that American operatives have identified them and are tracking their work" (Barnes, 2018). At home, CYBERCOM worked in conjunction with the FBI and the Treasury, to kick off a new initiative by uploading unclassified malware samples onto the crowdsourcing analysis and malware repository site Virus Total (US Cyber Command, 2018b; US Cyber Command, 2018c; Nakasone 2019a, p. 4). On the eve of the mid-term elections, the Command also preemptively DDoS'd the Internet Research Agency, a Kremlin-linked information warfare hub (Greenberg, 2019). Testifying before the Senate Committee on Armed Services on 14, February 2019, current head of US Cyber Command Gen. Nakasone, explained that "our efforts in defense of the 2018 elections taught us the value of persistent engagement to contest adversary campaigns, the power of enabling partners, and the ability to impose costs" (Nakasone 2019a, p. 6). US officials and lawmakers have hailed the command's efforts to protect the midterm elections a resounding success. According to a February 2019 classified joint assessment by the Department of Justice and Homeland Security, "there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections" (DoJ, 2019).

5 Open Questions

Writing in Orbis in May 2017, Fischerkeller and Harknett were the first to comprehensively outline the case for persistent engagement by explaining that, "a strategy of deterrence seeks to avoid operational contact, whereas cyberspace participants are interconnected, and consequently, all operations in cyberspace always involve operational contact. […] The cyberspace operational domain calls for a strategy of cyber persistence, a strategy based upon the use of [cyber operations, activities, and actions] (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace so that the United States could ultimately deliver direct effects in, through, and from cyberspace at a time and place of its choosing" (Fischerkeller & Harknett, 2017).

While both anticipated the global scale of US persistent engagement, it is unclear whether US defense planners within in the DoD would be equally happy if US allies and partners were to mimic US policy and started defending forwarding in US infrastructure. From a US point-of-view, advanced consent, coordination, and information sharing would be critical for such a scenario to be acceptable for Washington. However, the US has not extended the same courtesy in 2017 when Cyber Command hacked and deleted content from a server located in Germany that hosted ISIS propaganda. According to US logic at the time, "Pentagon officials argued that under an existing authority they had to counter terrorists' use of the Internet they did not need to request the permission of countries in which they were zapping propaganda" (Nakashima, 2017). According to the Washington Post, "they also argued that if notice is given, word of the operation could leak. That could tip off the target and enable other adversaries to discover the command's cyber capabilities" (Nakashima, 2017). An alternative explanation is that, because the US was de-facto at war with the Islamic State, allied consent was not deemed necessary to wipe an adversarial asset.

Max Smeets, cybersecurity postdoctoral fellow at Stanford's CISAC, put the finger in the wound when he noted in May 2019 that, "adversaries don't randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer? [...] Russia is already good at exploiting divisions between the U.S. and its allies. Cyber Command's new strategy might give it another avenue to do so" (Smeets, 2019). Responding to this criticism, former US Homeland Security Advisor Thomas Bossert, boldly explained that, "many of our allies have adopted the same approach. Most feel we should neither seek permission nor provide notice. They won't. Allies rightly ask that we limit effects: discrimination & proportionality, below an act of war, and not for commercial gain" (Bossert, 2019). Absent any proof, Bossert's assertion is difficult to swallow, and mostly likely so narrowly defined, that it only applies to smaller European nations which either have very nascent defensive capabilities in cyberspace, or seek to leverage closer US defense cooperation in resistance to closer EU defense integration. For better or for worse, at its heart, persistent engagement is a unilateral US approach to cyber defense.

A second point of contention is whether persistent engagement conforms to international law and can co-exist while the US participates in the UN GGE and the UN Open-ended Working Group (OEWG). Fischerkeller tried to re-brand persistent engagement in 2018 by arguing that it serves as a framework to create the impetus for tacit bargaining and agreed competition in the future (Fischerkeller, 2018). Meaning that, on a broader basis, persistent engagement encourages adaptive learning by US adversaries to prevent armed conflict in cyberspace (including coercion, crisis management, and escalation dominance). While on a more narrow basis, agreed competition will foster periodic contact between the US and its adversaries so that they can compete for strategic advantages and relative gains in national power. How this theoretical framework will actually play out in practice and whether its promise of stability in cyberspace can be realized is anyone's best guess.

A third point of uncertainty surrounds the question as to what will happen when persistent engagement fails to disrupt, defeat and deter US adversaries in cyberspace. Will the next step beyond persistent engagement be more engagement? Or just endless conflict or war? Similarly, if pushing against an adversaries infrastructure, tooling, and operators is not being perceived as persistent enough – maybe the next step will be to shift into the cybercriminal/APT space by targeting bulletproof hosting servers, open source penetration tooling - such as Mimikatz, Metasploit, and Powershell Empire -, and high profile cybercriminals that maintain rudimental links to APT threat actors.

It is also not entirely clear whether persistent engagement – a concept formulate for Cyber Command – conforms to the Pentagon's interpretation of defending forward. Meaning, the latter seems to be more oriented toward periodic engagements - in both space and time - in line with active defense measures, while the former is persistently deployed forward all the time everywhere. At least to this author, it seems highly likely that Pentagon officials must be at least somewhat worried that persistent engagement could increase enmity to such a degree that an adversary will pop-up outside of cyberspace, e.g. the 'computer nerds' kicking off a shooting war in meatspace, or will evade US efforts

and instead target US ally and partner networks as a mean to hurt Washington by proxy.

Furthermore, it is somewhat of an open question as to how the DoD and Cyber Command define 'superiority' in cyberspace. As security researcher the Grugq rightly asked, is it "even possible to have superiority in an environment which is so asymmetrically skewed toward offense?" (The Grugq, 2019). At least to this author, the DoD's talk on superiority has at least three meanings. First, it is policy speak for pulling the 2006 NMS-CO forward and sending the DoD's 2011 Strategy for Operations in Cyberspace into oblivion. Second, it serves as a DoD internal messaging tool to reassure the other services that their missions and operations will continue unhindered. The 2018 Joint Chiefs of Staff Joint Publication 3-12 on Cyberspace Operations underscores this point by noting that, because "permanent global cyberspace superiority is not possible due to the complexity of cyberspace," superiority in cyberspace is defined as the "degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference" (JCS, 2018, p. I-2 & GL-4). And third, the term 'superiority' is aimed at directing Cyber Command to develop and maintain capabilities that can cripple an adversary's entire IT ecosystem. In other words, Cyber Command's R&D and preparatory actions for cyberwarfare are aimed at developing tooling that ranges from Eternal Blue to Stuxnet, ready to hit foreign civilian and military targets across the board if directed to do so.

Lastly, given the absence of a clear threshold that clarifies when an action in cyberspace translates into a kinetic response in meatspace, the DoD currently operates under the notion that "there is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality" (DoD, 2015b, p. 1017). However, while it is certainly tempting to cross-connect pre-existing deterrence frameworks elsewhere to the cyber domain, it remains highly questionable whether this will lead to a more robust deterrence posture in cyberspace. For example, connecting nuclear deterrence to cyberspace is probably one of the areas where it will be either meaningless, counter-productive or potentially even destabilizing. Amy Zegart, senior fellow at the Hoover Institution, pointedly noted that, "do we really think the United States government would launch a nuclear retaliatory strike after a cyberattack of how ever consequential damage might be on the United States? […] Lots of debate about that. Is that really a robust deterrence strategy? Probably not" (Pomerleau, 2019). Similarly, conventional kinetic strikes against individual targets, such as the US drone strike killing ISIS hacker Junaid Hussain in 2015, certainly work in a meatspace conflict zone, but have little to no applicability between nation states at peace. Thus, rather than trying to build a full spectrum deterrence posture for cyberspace, the DoD might be better served by positing that: What happens in cyberspace will stay in cyberspace. And develop technical thresholds - based on intent, impact, tactics, techniques, and tooling used - to create a comprehensive response framework on the operational level.

6 Conclusion

At its core, the evolution of US defense strategy in cyberspace follows a clear trajectory: It is incident driven, riddled with experimentation, and sprinkled with uncertain success stories in between. Over the last three decades, US businesses and government agencies have been hammered by APT campaigns and cybercriminals from around the globe, with the DoD having little to nothing to offer in defense of the nation in cyberspace. The application of persistent engagement and defending forward produced some notable results limited in both time and space. It remains to be seen whether persistent engagement can actually be persistent and turn the tide in the long run. Being everywhere all the time, sounds beautiful in theory, but might be unachievable in practice.

In terms of the future outlook, we will most likely witness an increase in strategic, tactical, and operational experimentation by numerous other governments and cyber commands during their own search for a feasible defense posture in cyberspace. Some of these approaches will be similar to persistent engagement, while others might potentially be even more aggressive, intrusive, and ignorant of meatspace diplomatic relations and the norms discussion.

There are several lessons learned that can be extracted from the US evolutionary path:

(1) Live experimentation is key to the development of operational, tactical, and strategic defense concepts in cyberspace (Stuxnet & persistent engagement)
(2) Unlike meatspace, new defense policy implementations do not seem to illicit adversarial re-posturing or even spill-over effects into other domains. Meaning that defensive actions in cyberspace are currently not held to the same meatspace standards (Stuxnet & persistent engagement).
(3) Coordination within the executive branch needs to be streamlined and trained on a regular basis. No-notice exercises seem to be the most informative ones to adequately test cyber defense readiness (Eligible Receiver 97).
(4) In pretty much all discussions on deterrence in cyberspace, the operational art of cyber – e.g. how militaries actually defend, fight, and win in cyberspace is largely ignored. As long as this exclusion persists, the conversation on cyber deterrence will remain deductive, reductive, and superficial.
(5) Defending critical infrastructure is not an exclusively civilian task – the military has a leading role to play when it comes to protecting the nation in cyberspace.
(6) On the strategic level, governments need to clarify what they want to defend against in cyberspace. International law lays down one set of thresholds, national defense and counter-intelligence an other.
(7) Unclassified government systems are as important as classified ones (Solar Sunrise). What matters is not the information per se, but how chaos and friction could potentially be introduced and cascade throughout the system. Thus it might be prudent to assess a network's vulnerability in terms of potential collateral damage, rather than merely in terms of network security per se.
(8) On attribution, law enforcement has naturally taken the lead to identify and indict foreign cyber operators. While this has created some success, it might be prudent for the military to take a more prominent role in attributing attacks, for the sake of moving attribution away from the criminal sphere and push it into the domain of international relations and state-to-state conflict.

7 Abbreviations

AFB	Air Force Base
ACERT	Army Computer Emergency Response Team
AFCERT	Air Force Computer Emergency Response Team
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigations
ANO	Advanced Network Operations
APT	Advanced Persistent Threat
CENTCOM	Central Command
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CSIS	Center For Strategic and International Studies
CSPAN	Cable-Satellite Public Affairs Network
CTAD	Cyber Threat Analysis Division
CYBERCOM	Cyber Command
DCEO	Defensive Cyber Effects Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoJ	Department of Justice
DSB	Defense Science Board
EO	Executive Order
ER97	Eligible Receiver 97
FBI	Federal Bureau of Investigations
FIWC	Fleet Information Warfare Center
GAO	Government Accountability Office
GRU	Main Intelligence Directorate
HSPD-23	Homeland Security Presidential Directive
IRC	Internet Relay Chat
ISP	Internet Service Provider
JCS	Joint Chiefs of Staff
JFCC-NW	Joint Functional Component Command – Network Warfare
JTF-CND	Joint Task Force – Computer Network Defense
JTF-CNO	Joint Task Force – Computer Network Operations
JTF-GNO	Joint Task Force – Global Network Operations
LIWA	Land Information Warfare Activity
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration
NDAA	National Defense Authorization Act
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NMS-CO	National Military Strategy – Computer Operations
NSA	National Security Agency
NSPD-54	National Security Presidential Directive 54
NSPM-13	National Security Presidential Memorandum 13
OCEO	Offensive Cyber Effects Operations
OEWG	Open-ended Working Group
OFAC	Office of Foreign Assets Control
PPD-20	Presidential Policy Directive 20
PD-63	Presidential Directive 63
QDR	Quadrennial Defense Review
R&D	Research & Development
SAGE	Semi-Automatic Ground Environment
TAO	Tailored Access Operations
UN GGE	United Nations General Group of Experts
UNGA	United Nations General Assembly
USSTRATCOM	United States Strategic Command

8 Bibliography

Abrams, Mitch. 1999. "Israel Computer Hacker Wanted by FBI Speaks Out." *Jewish Telegraphic Agency*, February 12, 1999. https://www.jta.org/1999/02/12/lifestyle/israel-computer-hacker-wanted-by-fbi-speaks-out.

Alexander, Keith. 2010a. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." US Congress. https://fas.org/irp/congress/2010_hr/041510alexander-qfr.pdf.

Alexander, Keith. 2010b. "House Armed Services Subcommittee, Cyberspace Operations Testimony." https://www.stratcom.mil/Media/Speeches/Article/986513/house-armed-services-subcommittee-cyberspace-operations-testimony/.

Alexander, Keith. 2013. "Statement of General Keith B. Alexander, Commander United States Cyber Command, before the Senate Committee on Armed Services." https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf

Barns, Julian E. 2008. "Pentagon Computer Networks Attacked." *Los Angeles Times*, November 28, 2008. https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28-story.html.

Barns, Julian E. 2018. "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections." *The New York Times*, October 23, 2018. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

Barns, Julian E., and Siobhan Gorman. 2013. "U.S. Says Iran Hacked Navy Computers." *The Wall Street Journal*, September 27, 2013. https://www.wsj.com/articles/us-says-iran-hacked-navy-computers-1380314771?tesla=y.

BBC News. 1998. "Timeline of the Iraqi Crisis," December 21, 1998. http://news.bbc.co.uk/2/hi/events/crisis_in_the_gulf/road_to_the_brink/216264.stm.

Bejtlich, Richard. 2007. "Network Security Monitoring History." *TaoSecurity*, April 11, 2007. https://taosecurity.blogspot.com/2007/04/network-security-monitoring-history.html.

Bing, Chris. 2018. "In the opaque world of government hacking, private firms grapple with allegiances." *Cyberscoop*, July 23, 2018. https://www.cyberscoop.com/cybersecurity-research-reports-kaspersky-symantec-microsoft-us-government/

Bejtlich, Richard. 2014. "Executive Perspectives: DoJ Indicts Chinese Military Hackers: First Impressions." *FireEye*, May 19, 2014. https://www.fireeye.com/blog/executive-perspective/2014/05/doj-indicts-chinese-military-hackers-first-impressions.html.

Bossert, Thomas P. 2017. "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017." The White House. https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

Bossert, Thomas P.2019. "Disagree. In Fact, Many of Our Allies Have Adopted the Same Approach. Most Feel We Should Neither Seek Permission nor Provide Notice. They Won't. Allies Rightly Ask That We Limit Effects: Discrimination & Proportionality, below an Act of War, and Not for Commercial Gain." *Twitter*, June 5, 2019. https://twitter.com/TomBossert/status/1136272553385824257.

Brandom, Russell. 2014. "Iran Hacked the Sands Hotel Earlier This Year, Causing over $40 Million in Damage." *The Verge*, December 11, 2014. https://www.theverge.com/2014/12/11/7376249/iran-hacked-sands-hotel-in-february-cyberwar-adelson-israel.

Brock Jr., Jack L. n.d. "Computer Security: Hackers Penetrate DOD Computer Systems." GAO. https://www.gao.gov/assets/110/104234.pdf.

Calamur, Krishnadev. 2018. "Some of the People Trump Has Blamed for Russia's 2016 Election Hack." *The Atlantic*, July 18, 2018. https://www.theatlantic.com/international/archive/2018/07/trump-russia-hack/565445/.

Carden, Michael J. 2010. "Cyber Task Force Passes Mission to Cyber Command." *American Forces Press Service*, September 7, 2010. https://www.stratcom.mil/Media/News/News-Article-View/Article/983498/cyber-task-force-passes-mission-to-cyber-command/.

Carlin, John P. 2018. "Inside the Hunt for the World's Most Dangerous Terrorist." *Politico*, November 21, 2018. https://www.politico.eu/article/junaid-hussain-isis-islamic-state-hacker-inside-the-hunt-for-the-worlds-most-dangerous-terrorist/.

Caton, Jeffrey L. 2015. *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. US Army War College Press & Strategic Studies Institute. https://ssi.armywarcollege.edu/pdffiles/PUB1246.pdf.

CFR. 2005. "Titan Rain." *Cyber Operations Tracker*, August 2005. https://www.cfr.org/interactive/cyber-operations/titan-rain.

Chesney, Robert. 2018. "The Law of Military Cyber Operations and the New NDAA." *Lawfare*, July

26, 2018. https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

CNN. 1998. "U.S. Gearing up for Air Strikes on Iraq," January 26, 1998. http://webcache.googleusercontent.com/search?q=cache:cLDwuCIOotUJ:www.cnn.com/WORLD/9801/26/iraq.developments/&hl=en&gl=ch&strip=0&vwsrc=0.

Condon, Stephanie. 2017. "FBI charges Chinese national with distributing malware used in OPM hack." *ZDNet*, August 27, 2017 https://www.zdnet.com/article/fbi-charges-chinese-national-with-distributing-sakula-malware/

CSPAN. 1998. *US Senate Committee on Governmental Affairs*. L0pht Heavy Industries. https://www.youtube.com/watch?v=VVJldn_MmMY.

CSPAN. 2015. *US Permanent Select Committee on Intelligence - Hearing: World Wide Cyber Threats*. https://www.c-span.org/video/?328021-1/hearing-worldwide-cybersecurity-threats.

CSPAN. 2017. *US Senate Armed Services Committee: Hearing on: United States Cyber Command*. https://www.c-span.org/video/?428023-1/nsa-director-rogers-russia-poses-threat-congressional-elections.

Department of the Army. 1997. "Strategic Departmental, and Operational IEW Operations (Preliminary Draft)." https://fas.org/irp/doddir/army/fm34-37_97/3-chap.htm.

DHS. 2015. "Creation of the Department of Homeland Security," September 24, 2015. https://www.dhs.gov/creation-department-homeland-security.

DHS/NCCIS & FBI. 2016. "Joint Analysis Report: GRIZZLY STEPPE – Russian Malicious Cyber Activity." https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

DISA. n.d. "Our History." https://www.disa.mil/about/our-history/1990s.

DoD. 2006. "Quadrennial Defense Review Report." https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf.

DoD. 2010. "U.S. Cyber Command Fact Sheet." https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf.

DoD. July, 2011a. "Department of Defense Strategy for Operating in Cyberspace." https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

DoD. November, 2011b. "Department of Defense Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934." https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

DoD. 2015a. "The Department of Defense Cyber Strategy." https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

DoD, 2015b. "Department of Defense Law of War Manual." *Office of General Counsel*, June 2015 (Updated December 2016). https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190

DoD. 2018a. "Summary of the 2018 National Defense Strategy of the United States of America - Sharpening the American Military's Competitive Edge." https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

DoD. September, 2018b. "Summary - Department of Defense Cyber Strategy 2018." https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

DoD DSB. 2013. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat." https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.

DoD DSB. 2017. "Task Force on Cyber Deterrence." https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf.

DoJ. 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." *Office of Public Affairs*, May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

DoJ. 2016. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector." *Office of Public Affairs*, March 24, 2016. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

DoJ. 2018a. "United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Ivan Sergeyevich Badin etc." *United States District Court for the Central District of Columbia*, July 13, 2018.

https://www.justice.gov/opa/press-release/file/1092091/download

DoJ. 2018b. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." *Office of Public Affairs, September 6, 2018.* https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

DoJ. 2018c. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." *Office of Public Affairs*, October 4, 2018. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

DoJ. 2019. "Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections." *Office of Public Affairs*, February 5, 2019. https://www.justice.gov/opa/pr/acting-attorney-general-and-secretary-homeland-security-submit-joint-report-impact-foreign.

Drea et al. 2013. History of the Unified Command Plan 1946-2012. Joint History Office, Office of the Chairman of the Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/History/Institutional/Command_Plan.pdf

Eilperin, Juliet. 2016. "Obama Says 'We Will' Retaliate against Russia for Election Hacking," December 16, 2016. https://www.washingtonpost.com/news/post-politics/wp/2016/12/15/obama-says-we-will-retaliate-against-russia-for-election-hacking/?utm_term=.62a78d9b8bc5.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stunet Dossier." Symantec. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

FAS. 2004. "Fleet Information Warfare Center (FIWC)," March 4, 2004. https://fas.org/irp/agency/navsecgru/fiwc/index.html.

Federal Register. 1996. "Executive Order 13010 - Critical Infrastructure Protection." https://www.hsdl.org/?view&did=1613.

FireEye. 2016. "Redline Drawn: China Recalculates Its Use of Cyber Espionage." FireEye. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Fischerkeller, Michael P. 2018. "Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition." https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-and-tacit-bargaining-a-strategic-framework-for-norms-development-in-cyberspaces-agreed-competition/d-9282.ashx.

Fischerkeller, Michael P., and Richard J. Harknett. 2017. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis* 61 (3): 381–93.

Fitzgerald, Michael. 2007. "L0pht in Transition." *CSO Online*, April 17, 2007. https://www.csoonline.com/article/2121870/lopht-in-transition.html.

Fogleman, Ronald R., and Sheila E. Widnall. 1997. "Cornerstones of Information Warfare." US Air Force. https://apps.dtic.mil/dtic/tr/fulltext/u2/a323807.pdf.

Fruhlinger, Josh. 2018. "The OPM Hack Explained: Bad Security Practices Meet China's Captain America." *CSO Online*, November 6, 2018. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.htmls.

GAO. 2010. "Cybersecurity: United States Faces Challenges in Addressing Global Cybersecurity and Governance." https://www.gao.gov/new.items/d10606.pdf.

GAO. 2011. "Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities." https://www.gao.gov/assets/330/321818.pdf.

GAO. n.d. "DHS Management - High Risk Issue." https://www.gao.gov/key_issues/dhs_implementation_and_transformation/issue_summary.

Garamone, Jim. 2017. "Selva Discusses Nature of Nuclear Deterrence at Mitchell Institute Forum." *Defense Acquisition University*, August 13, 2017 https://www.dau.mil/News/Selva-Discusses-Nature-of-Nuclear-Deterrence-at-Mitchell-Institute-Forum

Garamone, Jim, and Lisa Ferdinando. 2017. "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command." *Department of Defense*, August 18, 2017. https://dod.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/.

Geller, Eric. 2018. "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand." *Politico*, August 16, 2018. https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095.

Gostev, Alexander. 2014. "Agent.Btz: A Source of Inspiration?" *SecureList*, March 12, 2014. https://securelist.com/agent-btz-a-source-of-inspiration/58551/.

Gourley, Bob. 2010. "JTF-CND to JTF-CNO to JTF-GNO to Cybercom." *CTOvision.Com*, September 8,

2010. https://ctovision.com/jtf-cnd-to-jtf-cno-to-jtf-gno-to-cybercom/.
Graham, Bradley. 1998. "U.S. Studies a New Threat: Cyber Attack." *The Washington Post*, May 24, 1998. https://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm.
Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
Greenberg, Andy. 2019. "US Hackers Strike on Russian Trolls Sends a Message - but What Kind?" *Wired*, February 27, 2019. https://www.wired.com/story/cyber-command-ira-strike-sends-signal/.
Greenwald, Eric A. 2010. "History Repeats Itself: The 60-Day Cyberspace Policy Review in Context." *Journal of National Security Law & Policy* 4 (41): 41–60.
Hamre, John J. 1998. "House Military Procurement and Military Research & Development Subcommittees: Critical Infrastructure Protection - Information Assurance - Statement by the Honorable John J. Hamre, Deputy Secretary of Defense." US House of Representatives. https://fas.org/irp/congress/1998_hr/98-06-11hamre.htm.
Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Cyber Conflict Studies Association.
JCS. 2006. "The National Military Strategy for Cyber Operations." https://www.hsdl.org/?view&did=35693.
JCS. 2018. "Joint Publication 3-12 - Cyberspace Operations." https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
Johnson, Carrie. 2016. "Justice Department Charges 7 Iranians For Hacking U.S. Banks." *NPR*, March 24, 2016. https://www.npr.org/2016/03/24/471762386/justice-department-charges-7-iranians-for-hacking-u-s-bankss.
K, Joseph. 1999. "Guide To Tech Terminology." *Crypt Newsletter*, 1999. http://c4i.org/eligib.html.
Kaplan, Fred. 2016a. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.
Kaplan, Fred. 2016b. "Inside 'Eligible Receiver.'" *Slate*, March 7, 2016. https://slate.com/technology/2016/03/inside-the-nsas-shockingly-successful-simulated-hack-of-the-u-s-military.html.
Lamb, Robert J. Winter 98/99. "Joint Task Force for Computer Network Defense." IAnewsletter. https://www.csiac.org/wp-content/uploads/2016/02/Vol2_No3.pdf.
Lange, Katie. 2018. "Cybercom Becomes DoD's 10th Unified Combatant Command." *DoD Live*, May 3, 2018. http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command.
Lasker, John. 2005. "U.S. Military's Elite Hacker Crew." *Wired*, April 18, 2005. https://www.wired.com/2005/04/u-s-militarys-elite-hacker-crew/.
Lawrence, J.p. 2017. "Dutch Hacker Case in Early 90s Was a Test for San Antonio Cyber Pioneers." *San Antonio Express-News*, August 4, 2017. https://www.expressnews.com/sa300/article/Dutch-hacker-case-in-early-90s-was-a-test-for-San-11735535.php.
Lawson, Sean. 2011a. "Richard Clarke Responds to Administration Cybersecurity Proposals." *Forbes*, June 3, 2011. https://www.forbes.com/sites/seanlawson/2011/06/03/richard-clarke-responds-to-administration-cybersecurity-proposals/#2dad16c960bc.
Lawson, Sean. 2011b. "DOD's 'First' Cyber Strategy Is Neither First, Nor a Strategy." *Forbes*, August. https://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/#4ae76185419c.
Lee, Robert M. 2012. "Stuxnet and Cyber Deterrence." *Infosec Island*, August 13, 2012. http://www.infosecisland.com/blogview/22168-Stuxnet-and-Cyber-Deterrence.html.
Lee, Timothy B. 2013. "How a grad student trying to build the first botnet brought the Internet to its knees." *The Washington Post*, November 1, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/.
Lyngaas, Sean. March 14, 2019a. "Cyber Command's Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia." *Cyberscoop*, March 14, 2019a. https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.
Lyngaas, Sean. April 4, 2019b. "SamSam Outbreak Led to FBI Restructuring, Top Official Says." *Cyberscoop*, April 4, 2019b. https://www.cyberscoop.com/samsam-investigation-fbi-tonya-ugoretz/.
Lynn, William J. 2010. "Defending a New Domain." *Foreign Affairs*, no. September/October 2010 Issue.

Markoff, John. 1991. "Dutch Computer Rogues Infiltrate American Systems With Impunity." *The New York Times*, April 21, 1991. https://www.nytimes.com/1991/04/21/us/dutch-computer-rogues-infiltrate-american-systems-with-impunity.html.

Markoff, Michele. 2017. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." United States Mission to the United Nations. https://usun.state.gov/remarks/7880.

Martelle, Michael. 2018. "Eligible Receiver 97." *Cyber Vault Library, George Washington University*, August 1, 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations.

McGurk, Sean P. 2010. "Statement for the Record of Seán P. McGurk - Acting Director, National Cybersecurity and Communications Integration Center Office of Cybersecurity and Communications National Protection and Programs Directorate Department of Homeland Security, before the United States Senate Homeland Security and Governmental Affairs Committee." US Senate. https://www.hsgac.senate.gov/imo/media/doc/TestimonyMcGurk20101117REVISED.pdf.

McMillan, Robert. 2017. "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!" *The Wall Street Journal*, August 7, 2017. https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118.

Miller, Greg, Ellen Nakashima, and Adam Entous. 2017. "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *The Washington Post*, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.5ae7a8597553.

Miller, Jason. 2019. "Justice walks back claims of data from OPM breach was used in a crime." *Federal News Network*, July 10, 2018. https://federalnewsnetwork.com/opm-cyber-breach/2018/07/justice-walks-back-claims-of-data-from-opm-breach-was-used-in-a-crime/

MIT. n.d. "SAGE: Semi-Automatic Ground Environment Air Defense System." *Lincoln Laboratory*. https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system.

Myre, Greg. 2019. "The U.S. Pledges A Harder Line In Cyberspace — And Drops Some Hints." *NPR*, March 26, 2019. https://www.npr.org/2019/03/26/705822275/the-u-s-pledges-a-harder-line-in-cyberspace-and-drops-some-hints.

Nakashima, Ellen. 2011. "Cyber-Intruder Sparks Response, Debate." *The Washington Post*, December 8, 2011. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?utm_term=.536b472036f1.

Nakashima, Ellen. 2017. "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies." *The Washington Post*, May 9, 2017. https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.b3b78dce7ae5.

Nakashima, Ellen. 2019. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.9e2c9e44e34b.

Nakashima, Ellen, and Shane Harris. 2018. "How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks." *The Washington Post*, July 13, 2018. https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

Nakasone, Paul M. 2019a. "Statement of General Paul M. Nakasone, Commander United States Cyber Command, before the Senate Committee on Armed Services." https://www.armed-services.senate.gov/download/nakasone_02-14-19.

Nakasone, Paul M. 2019b. "An Interview with Paul M. Nakasone." Joint Force Quarterly, Issue 92. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

NATO. 2018. "Cyber Defence," July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

NCC & FBI. n.d. *Solar Sunrise*. Wired. https://youtu.be/bOr5CtqYnsA.

NSA. 2017. *Eligible Receiver 97 After Action Report*. University of Maryland. https://www.youtube.com/watch?time_continue=10&v=iI3iZAq0Nh0.

Nye Jr., Joseph S. 2015. "The World Needs New Norms on Cyberwarfare." *The Washington Post*, October 1, 2015. https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.6024eec3a603.

OFAC. 2016. "Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities." *US Department of the Treasury*, December 29, 2016. https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

Ottis, Rain. 2008. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Painter, Christopher. 2016. "Christopher Painter, Coordinator for Cyber Issues, Statement before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy." https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

Pegoraro, Rob. 2018. "20 Years on, L0pht Hackers Return to D.C. with Dire Warnings." *The Parallax*, May 24, 2018. https://the-parallax.com/2018/05/24/l0pht-hackers-return-dire-warnings.

Peters, Ralph. 2007. "Washington Ignores Cyberattack Threats, Putting Us All at Peril." *Wired*, August 23, 2007. https://www.wired.com/2007/08/ff-estonia-america/.

Peterson, Andrea. 2014. "The Sony Pictures Hack, Explained." *The Washington Post*, December 18, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained.

Peterson, Andrea. 2015. "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought." *The Washington Post*, September 23, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/

Pomerleau, Mark. 2019. "Is There Such a Concept as 'Cyber Deterrence?'" *Fifth Domain*, April 30, 2019 https://www.fifthdomain.com/dod/2019/04/30/is-there-such-a-concept-as-cyber-deterrence

Poulsen, Kevin. 2001a. "No Jail for 'Analyzer.'" *SecurityForcus*, June 15, 2001. https://www.securityfocus.com/news/217.

Poulsen, Kevin. 2001b. "Solar Sunrise Hacker 'Analyzer' Escapes Jail." *The Register*, June 15, 2001. https://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/.

Poulsen, Kevin. 2007a. "Estonia Drops Cyberwar Heory, Claims Packets Were 'Terrorism.'" *Wired*, June 7, 2007. https://www.wired.com/2007/06/estonia-drops-c/.

Poulsen, Kevin. 2007b. "'Cyberwar' and Estonia's Panic Attack." *Wired*, August 22, 2007. https://www.wired.com/2007/08/cyber-war-and-e/.

Rhodes, Keith A. 2001. "Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures." GAO. https://www.gao.gov/new.items/d011073t.pdf.

Riley, Michael, and Dune Lawrence. 2012. "Hackers Linked to China's Army Seen From EU to D.C." *Bloomberg*, July 27, 2012. https://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.

Rogers, Michael S. 2018. "Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, before the Senate Committee on Armed Services." US Senate Armed Services Committee. https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf.

Sanger, David E. 2012. "Obama Ordered Wave of Cyberattacks against Iran." *The New York Times*, June 1, 2012. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Sanger, David E. 2016. "Obama Strikes Back at Russia for Election Hacking." *The New York Times*, December 29, 2016. https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=0.

Sanger, David E., and Mark Mazzetti. 2016. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." *The New York Times*, February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Thomas Schelling, Arms and Influence. New Haven: Yale University Press, 1966

Schwartz, John. 2007. "When Computer Attack." *The New York Times*, June 24, 2007. https://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html.

Sciutto, Jim. 2015. "Director of National Intelligence Blames China for OPM Hack." *CNN*, June 25, 2015. https://edition.cnn.com/2015/06/25/politics/james-clapper-china-opm-hacking/index.html.

Serabian Jr., John A. 2000. "Cyber Threats and the US Economy - Statement for the Record before the Joint Economic Committee on Cyber Threats and the US Economy." *CIA*, February 23, 2000. https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

Serbu, Jared. 2011. "DoD Cyber Strategy Aims at Deterrence." *Federal News Network*, July 15, 2011. https://federalnewsnetwork.com/defense/2011/07/dod-cyber-strategy-aims-at-deterrence/.

Shachtman, Noah. 2008. "Under Worm Assault, Military Bans Disks, USB Drives." *Wired*, November 19, 2008. https://www.wired.com/2008/11/army-bans-usb-d.

Sizer, Richard A. 1997. "Land Information Warfare Activity." *Military Intelligence Professional Bulletin*, 1997. https://fas.org/irp/agency/army/mipb/1997-1/sizer.htm.

Smeets, Max. 2019. "Cyber Command's Strategy Risks Friction With Allies." *Lawfare*, May 28, 2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

Soesanto, Stefan. 2017. "Grizzly Steppe — One step forward, two steps back?" *Medium.com*, August 17, 2017. https://medium.com/@iiyonite/grizzly-steppe-one-step-forward-two-steps-back-c3a249a7940f.

Soesanto, Stefan. 2018. "In Cyberspace, Governments Don't Know How to Count." *Defense One*, September 27, 2018. https://www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/.

State Department. 2018. "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats." Office of the Coordinator for Cyber Issues. https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

STRATCOM. 2018. "History," January 2018. https://www.stratcom.mil/About/History/.

Szoldra, Paul. 2016a. "I Spoke with a Hacker Who Could Have Taken down the Internet in 30 Minutes." *Business Insider*, June 6, 2016. https://www.businessinsider.com/space-rogue-l0pht-1998-testimony-2016-6?r=US&IR=T.

Szoldra, Paul. 2016b. "The US Could Have Destroyed Iran's Entire Infrastructure without Dropping a Single Bomb." *Business Insider*, July 6, 2016. https://www.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7?r=UK.

The Grugq. 2019. "Is It Even Possible to Have Superiority in an Environment Which Is so Asymmetrically Skewed towards Offense? On Almost Any Metric China Dominates in Cyber. Russia Is a Power Player with a KO vs the US. The US Can Do Magic, but Only after a Dozen Meetings and Committee Approval." *Twitter*, June 4, 2019. https://twitter.com/thegrugq/status/1136026380347404289.

The H Security. 2007. "Estonian DDoS - A Final Analysis," May 31, 2007. http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html.

The President of the United States. 2008. "The Comprehensive National Cybersecurity Initiative." https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf.

The President of the United States. 2009. "Cyberspace Policy Review." https://fas.org/irp/eprint/cyber-review.pdf.

The President of the United States. 2011. "International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World." https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The President of the United States. 2012. "Presidential Policy Directive/PPD-20." https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

The President of the United States. 2015. "Executive Order 13687—Imposing Additional Sanctions With Respect To North Korea." Federal Register. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13687.pdf.

The President of the United States. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

The President of the United States. 2018. "National Cyber Strategy of the United States of America." https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The White House. 1998. "Presidential Decision Directive/NSC-63." https://fas.org/irp/offdocs/pdd/pdd-63.htm.

The White House. 2003. "The National Strategy to Secure Cyberspace." https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

The White House. 2008. "National Security Presidential Directive/NSPD-54 & Homeland Security Presidential Directive/HSPD-23." https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

The White House. April 1, 2015a. "Executive Order - 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.'" https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

The White House. September 25, 2015b. "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015b. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Thompson, Mark. 2016. "Iranian Cyber Attack on New York Dam Shows Future of War." *Time*, March 24, 2016. http://time.com/4270728/iran-cyber-attack-dam-fbi/.

Thornburgh, Nathan. 2005. "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)." *Time Magazine*, September 5, 2005. https://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm.

UNGA. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

US Congress. 2001. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf.

US Congress. 2018. "John S. McCain National Defense Authorization Act for Fiscal Year 2019." https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

US Cyber Command. April, 2018a. "Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command." https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

US Cyber Command. November 5, 2018b. "#CNMF Has Posted New Malware to @VirusTotal." *Twitter*, November 5, 2018b. https://twitter.com/CNMF_VirusAlert/status/1059523249640558592.

US Cyber Command. November 5, 2018c. "#CNMF Has Posted New Malware to @VirusTotal." *Twitter*, November 5, 2018c. https://twitter.com/CNMF_VirusAlert/status/1059514838173577216.

US Senate. 2018. "Engrossed Amendment Senate - John S. McCain National Defense Authorization Act for Fiscal Year 2019." https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515eas.pdf.

US Senate. 2019. "Stenographic Transcript before the Subcommittee on Personnel - United States Senate: Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program." https://www.armed-services.senate.gov/imo/media/doc/19-13_02-14-19.pdf.

Vavra, Shannon. 2019. "25 nations are working to create a deterrence coalition to jointly impose costs on malicious state actors in cyberspace, @robstrayer told me on the side of a @CSIS 5G event." *Twitter*, August 1, 2019. https://twitter.com/shanvav/status/1156994111104258049

Vijayan, Jaikumar. 2007. "Reverse Hacker Wins $4.3M in Suit against Sandia Labs." *Computerworld*, February 14, 2007. https://www.computerworld.com/article/2543470/reverse-hacker-wins--4-3m-in-suit-against-sandia-labs.html.

Volz, Dustin. 2018. "Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive." *The Wall Street Journal*, August 15, 2018. https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721?tesla=y&mod=article_inline.

Volz, Dustin, and Jim Finkle. 2016. "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam." *Reuters*, March 24, 2016. https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

Warner, Gary. 2008. "Is The Analyzer Really Back? (The Return of Ehud Tenenbaum)." *Cybercrime & Doing Time*, September 7, 2008. http://garwarner.blogspot.com/2008/09/is-analyzer-really-back-possible-return.html.

Warner, Michael. 2017. *Understanding Cyber Conflict - Fourteen Analogies*. Georgetown University

Press. https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch1.pdf.

Wikileaks. 2008. “Diplomatic Security Daily.” https://wikileaks.org/plusd/cables/08STATE116943_a.html.

Wilner, Alex S. 2019. “US Cyber Deterrence: Practice Guiding Theory. Journal of Strategic Studies.” *Journal of Strategic Studies*, February. https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1563779?af=R&.

Zetter, Kim. 2014. *Countdown to Zero Day*. New York: Broadway Books.

Zuckerman, Laurence. 1998. “Satellite Failure Is Rare, And Therefore Unsettling.” *The New York Times*, May 21, 1998. https://www.nytimes.com/1998/05/21/business/satellite-failure-is-rare-and-therefore-unsettling.html.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.