**Strategic Planning: Analyzing the Evolution of the U.S. National Cyber Strategy**

**By: Nohl M Patterson**

**Keck Center for International and Strategic Studies**

**Jack Stark Fellowship In Security Studies**

**May 1, 2020**

**Acknowledgements:**

**I would like to thank Professor Jennifer Taw for reviewing this paper and contributing to its inspiration.**

**Thank you to the Keck Center for International and Strategic Studies for sponsoring my trip to the Student Conference on US Affairs (SCUSA) at the United States Military Academy to continue researching cybersecurity and as well as sponsoring this fellowship as a culmination of my research.**

1. **Introduction**

On September 20, 2018 the United States (U.S.) released a national cyber strategy for the first time in fifteen years. The strategy outlines a comprehensive plan to protect the critical infrastructure, deter threats in cyberspace, and foster a peaceful space for American commerce and trade. The new strategy signaled a shift in America’s understanding of warfare’s “fifth domain” and an increased awareness of how to mitigate the risk and address the challenges associated with the increasingly complex battlespace. The last two decades have seen increasing reliance from both the American military and American society on sophisticated technology. The rapid evolution of technology in an uncharted battlespace requires an integrated strategic approach that is more dynamic than those previously seen in conventional strategies. It is a battlespace that is non-physical, yet can levy real physical consequence. It operates at quite literally the speed of light and requires the foresight to prevent infiltration from all possible angles. For this reason, General Keith Alexander, former Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command (CYBERCOM), has deemed cyberspace, “crucial to 21st-century warfare as nuclear arms were in the 20th.”[[1]](#footnote-1) The process for developing effective methods to cope with challenges and adapt to this new battlespace is no different than the development of the tank or atomic bomb. It has been fraught with costly mistakes and painful lessons that laid the groundwork for effectively adapting to changes in the security landscape.

This paper will address the challenges and strategy changes that shaped the U.S. National Cyber Strategy’s evolution over the last seventeen years. Understanding this question first requires an understanding of what makes cyber a unique security environment to operate in with unique dilemmas. This paper will cover the relevant academic, public (open-source), and private sector literature needed to provide a comprehensive overview of the key contributors to the development of this strategy. Additionally, it will analyze specific use cases for the effective leveraging of technology to showcase pivotal moments in the development of effective strategy and the failures that have shaped how the nation responds. This paper will provide a framework to evaluate the most compelling security challenges America has faced in cyberspace and its ability to continue to effectively address America’s future challenges in cyberspace.

1. **Literature Review**
2. **Cyberspace: An Overview**

Cyberspace is defined by scholar Daniel T. Kauhl as the “operational domain framed by the use of electronics to exploit information via interconnected systems and their associated infrastructure.”[[2]](#footnote-2) However, it may be more simply defined as binary information transfer via electronic hardware and signals. Cyber and information technology is growing exponentially. According to IBM[[3]](#footnote-3) 90% of the data in the world has been produced in the last two years, and by 2025 that number will triple. This rapid growth has occurred in under sixty years. The Department of Defense (DoD) first mentioned computers (ARPANET[[4]](#footnote-4)) in a formal report in 1969 and three years later (TCP/IP), condensed information packages precursing formal data appeared. Although internet based technology has been popularized, reiterated, expanded, and modified by the private sector in garage success stories like Facebook, Apple, and Amazon, it is important to bear in mind that the internet was originally a project at the Defense Advanced Research Project Agency (DARPA). The internet had a million users in 1992 -- by 2007 it had more than a billion.[[5]](#footnote-5) The challenges that accompany this are complicated and the consequences far reaching. Its utilization makes it able to affect virtual (domain) and real-world (non-domain) outcomes. Former NSA resident scholar Joseph Nye states “Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace.”[[6]](#footnote-6) A nation’s behavior in cyberspace is shaped by what their preferred outcome and this framework is necessary to contextualize the problem.

Measuring cyber power in contextual terms requires analysis of the objectives that countries are trying to pursue via cyber means.[[7]](#footnote-7) Drawing on military doctrine, objectives are what an actor “*desires to accomplish in a given set of circumstances.”* (23)

While the specific goals that countries try to pursue are specific to each, security theory typically defines three broad overarching objectives that all countries seek to pursue in some form (24):

1. Defense and security. Protecting citizens remains the primary objective of national governments.
2. Economic growth and prosperity. Increasing flows of global trade, strengthening the domestic economy, and increasing government revenues to pay for essential services.
3. International power projection. Projecting influence overseas and growing its international reputation to enhance its defense and security and economic prosperity
4. **Defensive Challenges**

With the vast expanse of the cyber domain come numerous challenges of unusual offensive and defensive dynamics. A military comparison offers an insight into the complexity that arises from attempting to achieve conventional dominance in cyberspace. The epitome of American force projection is the carrier fleet -- it controls everything within a 500 mile radius, allowing for a variety of offensive, defensive, and deterrent capabilities. The economic resources and coordination necessary to create such a weapon are tremendous. The barriers to entry are simply too high for most countries to compete. For this reason, the United States more than quadruples its nearest competitor,[[8]](#footnote-8) allowing for force projection and air superiority. Compare this to the relatively low costs required for a state actor, non-state actor, or individual to begin operating and conducting operations in cyberspace. The necessary cost to effectively train, equip, and maintain a force to wage corporate espionage, cybertheft, or denial of service operations is paltry compared to the necessary equipment to maintain a ship, airplane, or tank.

Playing defense in cyberspace is fundamentally different from traditional defense tactics. When discussing physical defense tactics, John Mearsheimer states that “the 3:1 rule posits that the attack needs a local advantage of at least 3:1 in combat power to break through a defender’s front.”[[9]](#footnote-9) Mearsheimer summarizes a well known rule of war: attacking a defensive, well-prepared foe is costly and more difficult than being the defender. In contrast, the Harvard’s Belfer Center states the following regarding defensive positioning in cyberspace:

“The complexity of information systems gives the offense certain advantages for purely probabilistic reasons. Imagine a race: offense and defense go hunting for randomly distributed vulnerabilities, with the offense attempting to exploit those vulnerabilities and the defense aiming to patch them. The number of vulnerabilities grows with the size and complexity of the computer system, as do the technological advantages of offense—at least in principle. With a vast number of vulnerabilities, it is unlikely that the defense will be able to find and patch every vulnerability before the offense finds and exploits it.”[[10]](#footnote-10)

The internet was not designed with defense in mind -- machines were not engineered until recently to withstand robust infiltration attempts. As the Yale Review of International Studies summarizes: “The interdependence of computer networks that regulate or control key public infrastructures throughout the world provide fruitful and incredibly susceptible targets for the activities malicious [non-state actors].”[[11]](#footnote-11) Although recent computer systems are engineered with defense in mind, older operating systems and hardware fail to prepare for the significant rise in cyber espionage over the past decade. The increasing susceptibility of machines is only exacerbated by increasingly complex and automated machine processes. Commercial expansion into the internet of things, cloud computing, and non-kinetic machine updating provide additional infiltration points for potential hackers to exploit.

Another complication of defensive posture in cyberspace is attribution error, or failing to identify who conducted the attack. The data trail left by cyberattacks and the ensuing investigation process is labor intensive and imprecise. There are not conventional tell-tale signs and attackers seek to confuse and post blame upon others. As the Office of the Director of National Intelligence (ODNI) states in its *Guide to Cyber Attribution,* “Establishing attribution for cyber operations is difficult but not impossible. No simple technical process or automated solution for determining responsibility for cyber operations exists.”[[12]](#footnote-12) Furthermore, the ODNI and American intelligence community establishes responsibility with varying levels of confidence for suspected offenders. Establishing the perpetrators is “most difficult to assess because we have to link malicious cyber activities to the specific individuals and assess the sponsor and motivators of these individuals.”[[13]](#footnote-13) Assume in a hypothetical scenario the defense believes it has identified the perpetrator of a malicious cyber intrusion. What constitutes a proportional retaliation? The defensive challenge moves beyond attribution and into punitive measures.

The cyber domain is a new environment, where norms are either newly defined by international law or non-existent. The Council on Foreign Relations summarizes U.S. defensive reasoning for striving to implement norms in cyberspace: “First, the United States is vulnerable to cyberattacks and this weakness is difficult to address using conventional tools of military statecraft. Second, it is difficult to ensure that complex information systems are fully defended, since they may have subtle technical weaknesses. Third, classical deterrence is not easy in a world where it is often challenging to identify sophisticated attackers, or even to know when an attack has taken place. Lastly, treaties are hard to enforce because it is so difficult to verify compliance—particularly in cyberspace, where weapons are software, not missiles.”[[14]](#footnote-14) In a realm that is continually developing and changing, establishing international cyber norms is a gradual process and fundamentally different than establishing conventional norms because the victims of cyber attacks are rarely just national governments. Fireeye, a U.S. based cybersecurity company started by former National Security Agency employees (NSA), stated in their 2020 M-Trends report[[15]](#footnote-15) that the most targeted entities of the last three years were non-government: entertainment, financial, and professional services topped the list.

1. **Offensive Challenges**

Conducting offensive operations in cyberspace poses unique challenges that are typical in conventional security dynamics. The Brookings Institute defines cyber offensive operations as   
“the use of cyber capabilities for national security purposes intended to compromise the confidentiality, integrity, or availability of an adversary’s information technology systems or networks; devices controlled by these systems or networks; or information resident in or passing through these systems or networks.”[[16]](#footnote-16) While this provides a reliable summation of the goals and capabilities of nation-states in cyberspace, it fails to account for non-state actors, soloists, and Advanced Persistent Threats (APT’s) conducting cyber crime or proxy attacks. Before delving into the relevant actors conducting cyber offensives, one must understand the challenges that arise from cyber operations. International organizations like the World Economic Forum have coined the term “cyber superpower”[[17]](#footnote-17) and stated “countries which are believed to have the most developed cyber warfare capabilities are China, Israel, Russia, the U.K. and the U.S.”[[18]](#footnote-18) While these cyber superpowers mirror the conventionally defined great powers (with the exception of Israel), the innovation based nature of cyber warfare creates an asymmetric advantage. This is typically not found in conventional combat environments, as “offensive cyber capabilities—in contrast to traditional tools wielded by states—are cheaper, harder to track and exploit vulnerabilities to inflict significant harm on the victim. The asymmetric nature of cyber capabilities means smaller countries can punch above their weight, exerting more influence using cyber means than with traditional tools.”[[19]](#footnote-19) This refers explicitly to small countries, but the same logic can be applied to state sponsored and non-state entities. The ability to innovate technology and create or corner a market is the basis for the current technology market. Innovation can be largely driven by a highly skilled individual or a group of individuals in market based companies, white hat endeavors (ethical hacking), or black hat enterprises. Skilled programmers and black hat professionals possess the ability to leverage already existing hacking tool kits (ransomware, malware, etc.) or seek out network vulnerabilities and security gaps. This greatly alters the barriers to entry that have so commonly defined conventional security dynamics. One skilled individual can greatly affect the outcome of a conflict.

However, those conducting offensive cyber operations run into non-traditional obstacles when scaling effective strategies. The development of any new innovation and its subsequent use makes it difficult to employ that same tool again. Suppose the United States has the ability to trace an attack back to a cyber actor, complications arise for that actor's future offensive strategy. The actor has exposed their entry mechanism or structural weakness, and they are unlikely to be able to use the same method again. A research team at the National Academy of Sciences in a paper titled “Strategic Aspects of Cyberattack, Attribution, and Blame”[[20]](#footnote-20) states that two of the driving factors for strategic deterrence and response in cyberspace are *evidence spoofing* and *lack of appropriate response.* Utilizing a blame game model, they illustrate that the combination of confidence level classification (the ODNI utilizes a three step classification measure- low, medium, and high confidence for cyber attack attribution assessments) and the ability to subvert or pin blame with relative ease creates a highly dangerous environment in cyberspace when looking to retaliate. This article further elaborates on how this model explains a lack of [unclassified] responses : “In the cyber domain, assigning blame for an attack or intrusion is complicated by both technical factors and lack of agreement on basic definitions (e.g., what constitutes an attack or what counts as critical infrastructure). Sources in or close to the US Government assert that its ability to trace back a cyber operation to its geographic origin (e.g., an urban neighborhood in China) is excellent ([**2**](https://www.pnas.org/content/114/11/2825#ref-2)). However, unlike its response to aggression in the physical world, the United States has been surprisingly restrained in responding to incidents, such as the Chinese theft of databases containing the personal information of 21.5 million federal employees or intellectual property. Similarly, the Russian data theft from JP Morgan Chase, and Iranian cyberattacks against the United States.”[[21]](#footnote-21) These complications create a divide in typical offensive security dynamics for the United States.

1. **Developing Innovation**

Technology continues upward in an exponential growth cycle that creates huge room for societal improvement and economic opportunity, but also challenges for securing these new changes. Innovation is the driving force in cyberspace, responsible for new methods for aggregating data, better hardware, and pushing the constraints of classical computing. Colonel Stoney Trent Ph.D, states in the Cyber Defense Journal: “innovation in operations, training, and technology will ensure these forces can overmatch [U.S.] adversaries.”[[22]](#footnote-22) Innovation is also a crucial factor in conventional conflicts; inventions such as the atomic bomb or trebuchet have dramatically altered physical security dynamics. The unique problem that cyberspace presents for the United States military is that such innovations are often not driven by an advanced military industrial complex but by the private sector, presenting problems for both regulation and developing technology. As previously stated, the internet was a brainchild of DARPA, but the accompanying landscape is dominated by ground-up, market centric companies, like Microsoft, Apple, and Google. These companies are multinational corporations that do not cater to the interests and demands of the U.S. government in the same manner as defense contractors like Raytheon or Lockheed Martin. There becomes a variety of objectives and tradeoffs that the United States has to juggle when attempting to foster innovation. The U.S. National Cyber Strategy 2018 states one of its four pillars is “nurturing a secure digital economy and domestic innovation.”[[23]](#footnote-23) Researchers from Harvard’s Belfer Center for Science and International Affairs state cybersecurity is a “delicate policy balance”[[24]](#footnote-24) that must be struck to maintain the competitive model that has allowed technology to flourish while maintaining the national security interest. The public sector holds less relative power as the cyber battlespace changes at an increasingly steep rate, while policy regulations and norms struggle to keep up. A former intelligence community intelligence expert states that “private sector tools are almost exclusively leveraged when defending and preventing cyber incursions.”[[25]](#footnote-25) This leaves nations in the unique position of simultaneously defending against state and non-state actors, while monitoring corporations for susceptibility to cyber incursions while fostering innovation.

**III. U.S. In Cyberspace: An Overview**

Despite being classified as a great power in cyberspace, the United States has been operating within this domain for less than twenty years. Following the conclusion of the Cold War, the Director of the Defense Information Systems Agency (DISA) warned of the upcoming risk associated with network exploitation, “highlighting defense vulnerabilities and potential risk for network exploitation”[[26]](#footnote-26) in 1995. For the next decade, cyber operations and network liabilities fell under the purview of U.S. Strategic Command (USSTRATCOM). Under General James Cartwright the Joint Functional Component Command for Network Warfare was created. This eventually became the operational component of the U.S. Cyber Command (CYBERCOM). In 2009, Secretary of Defense Robert Gates directed the creation of an independent combatant command to serve the increasing demands of defense for American networks. The command would occupy a “dual hat”[[27]](#footnote-27)- the commander controls both the combatant command and CYBERCOM. Under the commander’s purview is the largest intelligence resource in the world and authority over the four military branches’ active cyber components: 10th Fleet, 2nd Army, the 24th Air Force, and Marine Force Cyber Command. Over the course of its eleven year lifespan, the young combatant command has gained increasing power, personnel, and operational reach. CYBERCOM has become the foremost defender and offensive component for securing the national interests in cyberspace.

The *National Strategy to Secure Cyberspace* was released by the DOD in 2003 and identified three strategic objectives: preventing cyber attacks against America’s critical infrastructure, reducing national vulnerability to cyber attacks, and minimizing damage and recovery time from attacks that do occur. The three objects are preventive, symptomatic responses to cyber incursions. The strategy itself was one that detailed defensive responses, without an understanding of how the battlespace would evolve, that stands in stark contrast to the current stratgem’s unofficial model: defend forward. Thomas M. Chen of the Strategic Studies Institute in his “An Assessment of the Department of Defense Strategy for Operating in Cyberspace”[[28]](#footnote-28) postulates that the creation of the Department of Defense’s subsequent Strategy for Operating in Cyberspace 2011, an updated manual for operating in cyberspace has some key differences than the National Cyber Strategy. The first is *Strategic Initiative 4* which states: “DoD will build robust relationships with U.S. allies and international partners to strengthen collective cyber security.”[[29]](#footnote-29) Likewise, the second difference is *Strategic Initiative 5* : “DoD will leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.”[[30]](#footnote-30) While these seem like minor differences, the discrepancy between the two strategies is not simply attributable to the progression of time: it was the product of costly lessons learned.

1. **Operation Yankee Buckshot**

In 2008, Operation Yankee Buckshot resulted in the “most significant breach of U.S. military computers ever.”[[31]](#footnote-31) William J. Lynn III, former Deputy Secretary of Defense, summarized the attack in Foreign Affairs in 2010:

“In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. 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. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.”[[32]](#footnote-32)

The attack had several direct effects. It dealt a devastating blow to the presumed security of DoD networks, drawing into question the reliability of other networks. As a result of this, the creation of U.S. Cyber Command was expedited and the process to Initial Operational Capability was greatly accelerated. Less than a year after this breach General Keith Alexander was appointed to oversee USCYBERCOM and his reputation grew in proportion to the scope of his command. The following excerpt is from his 2013 cover on Wired technology magazine: “This is the undisputed domain [Fort Meade] of General Keith Alexander, a man few even in Washington would likely recognize. Never before has anyone in America’s intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy.”[[33]](#footnote-33) The valuable lesson on defensive posture in cyberspace resulted in the rapid evolution of offensive capabilities. EXPAND

1. **Stuxnet**

In January 2010, Iran discovered the existence of a malicious computer worm within the industrial operating systems that regulated Iranian enrichment facilities. The digital “worm”, which would later be known as Stuxnet, worked in three phases: “First, it analyzed and targeted Windows networks and computer systems. The worm, having infiltrated these machines, began to continually replicate itself. [1] Next, the machine infiltrated the Windows-based Siemens Step7 software. Lastly, by compromising the Step7 software, the worm gained access to the industrial program logic controllers.”[[34]](#footnote-34) The exploitation of four zero day flaws- a compute software loophole that has existed since its original development and the subsequent damage done to Iran's nuclear program was remarkable. It demonstrated very tangibly to the world that cyber events could have physical effects. First, it showed that kinetic outcomes could be derived through non-kinetic means. According to McAfee, a well-known cybersecurity firm with public sector ties lists the number of machines caused to physically degrade at over 1,000[[35]](#footnote-35), causing a 20% reduction in Iran’s nuclear production capacity. The actual degradation of the equipment was the result of the worm gaining access through a gap in an old SQL (Search Query Language) infrastructure flaw, allowing it to gain system-level control over the centrifuges, spinning them out of control utilizing a sophisticated malware mechanism called man-in-the-middle. McAfee cities how “anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct,”[[36]](#footnote-36) ultimately resulting in the infection of more than 100,000 hosts.

When Stuxnet was released and its origins were still ambiguous, it was officially denied by the United States government. Der Spiegel in 2011 labeled Stuxnet the “first digital weapon of geopolitical importance”[[37]](#footnote-37), signaling the evolution of U.S. cyberstrategy and the inception of the global power struggle for cyberspace. It was from this point forward that cyber would be considered a domain no different than air or sea for the United States government. However, it would not be until later that former STRATCOM commander General James Cartwright pleaded guilty to lying to FBI agents regarding information he leaked about Stuxnet and the United States long suspected involvement was confirmed. The aftermath of Stuxnet changed the norms for retaliatory attacks. In 2012, the three largest financial services in the United States, JPMorgan Chase, Citigroup, and Bank of America came under a coordinated denial of service attack in late 2011. Iran’s Head of Defense Agency, Gholam Reza Jalali, stated “We officially announce that we haven’t had any attacks”[[38]](#footnote-38), despite Iranian involvement confirmed later by the DoD. The initiation into critical private sector infrastructure marked a trend that would continue until today: there is no target off-limit. Stuxnet demonstrated that retaliation is not limited to public sector or defense entities, but the financial sector, hospitals, and power grids are viable pressure points for non-kinetic attacks.

1. **Russian Election Interference**

The 2016 Presidential Election is yet another significant cyber milestone. ODNI in its unclassified report lists the following summary for Russian motives: “We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia’s goals were to undermine public faith in the US democratic process.”[[39]](#footnote-39) Russia, prior to its actions during the 2016 election, had expressed advanced capabilities in cyberspace. A joint report from the Center for Strategic and International Strategy and McAfee states: “the complex and close relationship between the Russian state and organized crime means that Russia provides a sanctuary for the most advanced cybercriminals...The best cybercriminals in the world live in Russia, and as long as they do not travel to countries where they could be arrested, they are largely immune from prosecution. For example, one of the cybercriminals who hacked Yahoo at the behest of Russian intelligence services, compromising millions of accounts and transferred the PII to the Russian government, also used the stolen data for spam and credit card fraud for personal benefit.”[[40]](#footnote-40)

Following well documented cyber incursions into the U.S. financial sector by Iran in 2011 and SONY in 2014 that was attributed to North Korea, Russia emerged into the battlespace. Russia’s behavior in cyberspace has been conducted through government proxies or government sanctioned hackers that operate within the purview of Russian foreign policy and intelligence goals: “FireEye determined that APT28’s cyber operations are consistent with government sponsorship and control. Specifically, APT28 has relied on a steady supply of sophisticated tools only available to a nation state or state-protected contractor.”[[41]](#footnote-41) According to FireEye, APT 28[[42]](#footnote-42) (Advanced Persistent Threat) is a group based out of Russia that had continually ramped up operational tempo since 2014[[43]](#footnote-43) leading up to the election. APT28 operations have consisted of malware, phishing emails, and utilizing zero day exploits to target persons of interests (POIs) to the Russian government. These have included but were not limited to prominent journalists, Western European politicians, and members of the DNC. These mass attacks are conducted in coordination with affiliate APT29, also deemed a proxy of the Russian Federation.

The ODNI report *Assessing Russian Activities and Intentions In Recent Elections* states the following assessment of Russian interference:

“Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties. We assess Russian intelligence services collected against the US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies. In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016.”[[44]](#footnote-44)

The official intelligence assessment has APT29 mobilizing data collection methods, phishing emails, and malware inside the DNC since 2015. Over this time period, Russia sought to decrease the credibility of Secretary Clinton and influence the outcome of America’s election. These infiltrations were non-partisan, but mainly targeted the local, state, and national efforts of the DNC via media manipulation. While Russian infiltration was not unprecedented, the scale, scope, and degree of this infiltration was unparalleled: “Russia’s effort to influence the 2016 US presidential election represented a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections.”[[45]](#footnote-45) Russia’s strategy exposed structural weaknesses across the entirety of America’s political system. While financial, entertainment, and defense industries had become the subject of sustained cyber attacks, Russia’s strategy exposed both structural weaknesses and new levers for exerting influence that had not been previously considered. These measures were aimed at swaying election outcomes and disillusioning U.S. voters; steps taken by the Russian Federation proxies included leveraging social media platforms such as Twitter and Instagram to spread disinformation (troll farming), releasing notable Democratic politicians' emails via Wikileaks, and stealing sensitive information in possession of the Democratic Congressional Campaign Committee (DCCC).

These efforts were far more sophisticated and nuanced than brute force bot attacks or Distributed Denial of Service (DDOS) attacks toward critical infrastructure. The infiltrations leading up to the 2016 election were part of a long term strategic plan executed via multiple, diversified avenues of attack, which the CYBERCOM and NSA were unequipped to defend against. This cyber campaign spurred a shift in defensive strategy response among CYBERCOM and the NSA. It was no longer feasible for the United States to attempt to breach defensive gaps, use predictive algorithms, or delay on deterrence for defense. The attacks were simply too numerous and the response time too long for the current defensive approach. The 2018 National Cyber Strategy introduced a new defensive strategy- its operational effectiveness and will be judged in the next section

**III. 2018 National Cyber Strategy: Defending Forward**

The 2018 National Cyber Strategy and its strategic approach has two main components that were operationalized by National Security Presidential Memorandum (NSPM) 13 in August 2018. This memo allows CYBERCOM to initiate defensive and offensive actions without presidential approval, dramatically cutting down on response time for cyber operations. Accompanying this operational discretion are two new strategies put into place by current CYBERCOM director General Paul Nakasone. The first component, “defending forward”, refers to the pro-active ability of cyber defense teams to now move into allied networks for support and direct action roles. When conducting cyber operations, your base of operations is your home network. If you wish to conduct a non-kinetic incursion, data collection, or penetration test, you have to traverse allied, neutral, or hostile networks in the same manner as if you were flying through that space. This approach yields two positive benefits- you are able to support allies in their operations and it dramatically decreases response time. Fifth Domain states the following:

“We’re also working with our partners, participating in defending U.S. critical infrastructure from malicious cyber activity,” David Luber, executive director of Cyber Command, said at CyberCon 2019. “That’s where we have a chance to see what our adversaries are doing in cyberspace because we now have the authority under the National Defense Authorization Act 2019 to operate outside the DoD networks to help our allies defend forward. That’s a big difference, because in the past the DoD could only operate in its own networks. But, when invited by our allies, we can now work and help defend inside of their networks.”[[46]](#footnote-46) The ability to defend forward allows the United States to substantially increase their support of allied networks, decreasing response time for cyber operations, and empowering domestic and international partners to join in collective defense. Additionally, when engagement arises, these conflicts take place away from American networks, decreasing the risk for mass attack or infiltration into “home networks”.

The second component is “persistent engagement”, maintaining consistent contact with competitors in cyberspace. General Paul Nakasone defines it as the following: “Persistent engagement is the concept that states we are in constant contact with our adversaries in cyberspace, and success is determined by how we enable and act. In persistent engagement, we enable other interagency partners. Whether it’s the FBI or DHS, we enable them with information or intelligence to share with elements of the CIKR [critical infrastructure and key resources] or with select private-sector companies.”[[47]](#footnote-47) This strategy presents a more nuanced and complete picture for how cyberspace operates. It accepts that defense is an extremely difficult position to be in- there are simply too many infiltration points. In order to defend, you have to be consistently engaged with adversaries, collecting intelligence on their capabilities. Nakasone summarizes, “This is a domain that requires constant action because we’re going to get reactions from our adversary. From that reaction stems our next move.”[[48]](#footnote-48) These strategies have yielded effective results. During the 2018 midterm elections, Chris Krebs, Director of the Cybersecurity and Infrastructure Agency stated to the Senate: “The most secure election held in the modern era in the U.S.”[[49]](#footnote-49) The Council on Foreign Relations reiterates the point that while these elections were secure, “election cybersecurity requires consolidating and expanding the progress achieved in 2018.”[[50]](#footnote-50)

**IV. Conclusion**

This paper has developed a framework to examine the National Cyber Strategy and the demands that cyberspace presents for the United States. The security environments encountered in cyberspace are fundamentally different than those found in conventional security dynamics. Cyberspace is a battlespace that will continue to grow increasingly complex, requiring an approach that is comprehensive, innovative, and responsive enough to deal with this non-conventional challenge. The current strategy has learned from costly mistakes and displays a more complete understanding for the unique threats cyber presents. Both persistent engagement and defending forward combine to form a more cohesive strategy to deal with the challenges cyberspace presents. In order to continue securing the national interest in cyberspace and encouraging cyber norms, the current administration needs to continue to foster innovative, dynamic strategies that consistently engage and deter American adversaries.

**Bibliography**

Bamford, James. “NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us into Cyber War.” Wired Magazine. June 6, 2012. Accessed March 27, 2020. <https://www.wired.com/2013/06/general-keith-alexander-cyberwar/>

Bradshaw, Leslie. “Big Data and What it Means.” U.S. Chamber Foundation. December 2012. Accessed March 12, 2020. <https://www.uschamberfoundation.org/bhq/big-data-and-what-it-means>

Breeve, Keith. “Who are the Cyberwar Superpowers?” World Economic Forum. May 4, 2016. Accessed April 2, 2020. <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>

Chen, Thomas M. “*AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*.” Strategic Studies Institute, US Army War College. 2013. Accessed April 2, 2020 [www.jstor.org/stable/resrep11200](http://www.jstor.org/stable/resrep11200).

Corrigan, Jack. “2018 Midterm Elections Were ‘the Most Secure’ in U.S. History, DHS Cyber Chief Says”. Next Government. March 13, 2019. Accessed April 20, 2020.

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, Robert Axelrod. “Strategic aspects of cyberattack and blame.” Proceedings of the National Academy of Sciences. March 2017, Accessed April 20, 2020.

Farrell, Henry. “Promoting Norms for Cyberspace”. Council on Foreign Relations. April 6, 2015. Accessed March 17, 2020. <https://www.cfr.org/report/promoting-norms-cyberspace>

Fidler, David. “Year in Review: Cyber Threats and the Midterm U.S. Elections”. Council on Foreign Relations. January 2, 2019. Accessed April 20, 2020. cfr.org/blog/year-review-cyber-threats-and-mid-term-us-elections

Holger Stark. ["Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War"](http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html). *Der Spiegel*. August 8, 2011. Accessed March 2, 2020.

Holloway, Michael. “Stuxnet Worm Attack on Iranian Nuclear Facilities”. Stanford University, Computer Science Department. July 16, 2015. Accessed March 27, 2020. <http://large.stanford.edu/courses/2015/ph241/holloway1/>

Kuehl, Daniel T. “From Cyberspace to Cyberpower: Defining the Problem”. Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009). Accessed March 2, 2020

Lewis, James Andrew. “A Map of the Most Dangerous Sources of Cybercrime.” McAfee. Center for International and Strategic Studies. March 6, 2018. Accessed April 2, 2020. <https://www.mcafee.com/blogs/enterprise/map-dangerous-sources-cybercrime/>

Lin, Herbert. Zegart, Amy. “Offensive Cyber Operations in US National Security.” Brookings Institute. April 26, 2019. Accessed April 2, 2020. <https://www.brookings.edu/wp-content/uploads/2018/10/978081573547_ch1.pdf>

Lynn, William J. “Defending a New Domain: The Pentagon’s New Cyber Strategy”. Foreign Affairs. September 2010. Accessed March 6, 2020. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>

Mearsheimer, John J. “Assessing the Conventional Balance: The 3:1 Rule and Its Critics.”`*International Security*, vol. 13, no. 4, 1989, pp. 54–89. *JSTOR*, www.jstor.org/stable/2538780. Accessed April 7, 2020.

Nye, Joseph S.. “CyberPower.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Accesed March 2, 2020. <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf>

Pomerleau, Mark. “Here’s How Cyber Command is Using ‘Defend Forward’”. Fifth Domain. November 12, 2019. Accessed April 20, 2020. <https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/>

Slayton, Rebecca. “Why Cyber Operations Do Not Always Favor the Offense.” Policy Brief, *Quarterly Journal: International Security,* February 2017. Accessed March 15, 2020. <https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense>

Trent, Stoney. “Cultivating Technology Innovation for Cyberspace Operations.” *The Cyber Defense Review*, vol. 3, no. 3, 2018, pp. 115–134. *JSTOR*, www.jstor.org/stable/26555001. Accessed 20 Apr. 2020.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. “Reconceptualizing Cyber Power.” Belfer Center, Harvard University. April 2020. Accessed April 15, 2020. <https://www.belfercenter.org/publication/reconceptualizing-cyber-power>

“A Guide to Cyber Attribution”. Office of the Director of National Intelligence. September 14, 2018. Accessed March 10, 2020. <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf>

“An Interview with Paul Nakasone”. 92nd NFQ. February 2019. Accessed April 20, 2020. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf>

“ARPANET”. Defense Advanced Research Projects Agency. Accessed March 2, 2020. <https://www.darpa.mil/about-us/timeline/arpanet>

“Background to Assessing Russian Activities in Recent US Elections: The Analytic Process and Cyber Incident Attribution”. Director of National Intelligence. January 6, 2017. Accessed April 4, 2020. <https://www.dni.gov/files/documents/ICA_2017_01.pdf>

“Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals”. Yale Review of International Studies. December 2017. Accessed March 15, 2020. <http://yris.yira.org/comments/2214>

“Iran Denies Hacking into American Banks”. Reuters. September 18, 2012. Accessed March 12, 2020.

<https://www.reuters.com/article/us-iran-cyberattacks-denial/iran-denies-hacking-into-american-banks-idUSBRE88M06O20120923>

“National Cyber Strategy of the United States of America”. The Office of the White House. September 2018. Accessed January 6, 2020. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

Senate Intelligence Committee: Russian and 2016 Election. FireEye. March 30, 2017. Accessed March 27, 2020. <https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf>

“US Cyber Command History”. US Cyber Command. May 2020. Accessed April 2, 2020 <https://www.cybercom.mil/About/History/>

*“What is Stuxnet?*”. McAfee Corporation. July 2011. Accessed March 2, 2020. <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html>

1. Bamford, James. “NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us into Cyber War.” Wired Magazine. June 6, 2012. Accessed March 27, 2020. <https://www.wired.com/2013/06/general-keith-alexander-cyberwar/> [↑](#footnote-ref-1)
2. Kuehl, Daniel T. “From Cyberspace to Cyberpower: Defining the Problem”. Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009). Accessed March 2, 2020 [↑](#footnote-ref-2)
3. Bradshaw, Leslie. “Big Data and What it Means.” U.S. Chamber Foundation. December 2012. Accessed March 12, 2020. <https://www.uschamberfoundation.org/bhq/big-data-and-what-it-means> [↑](#footnote-ref-3)
4. “ARPANET”. Defense Advanced Research Projects Agency. Accessed March 2, 2020. <https://www.darpa.mil/about-us/timeline/arpanet> [↑](#footnote-ref-4)
5. Nye, Joseph S.. “Cyber Power.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Accesed March 2, 2020. <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf> [↑](#footnote-ref-5)
6. Nye, Joseph S.. “Cyber Power.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Accessed March 2, 2020. <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf> [↑](#footnote-ref-6)
7. Nye, Joseph S.. “CyberPower.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Accessed March 2, 2020. <https://www.belfercenter.org/publication/reconceptualizing-cyber-power#toc-2-0-0> [↑](#footnote-ref-7)
8. China as of January 2020 has two operational carriers- the United States has eleven. [↑](#footnote-ref-8)
9. Mearsheimer, John J. “Assessing the Conventional Balance: The 3:1 Rule and Its Critics.”`*International Security*, vol. 13, no. 4, 1989, pp. 54–89. *JSTOR*, www.jstor.org/stable/2538780. Accessed April 7, 2020. [↑](#footnote-ref-9)
10. Slayton, Rebecca. “Why Cyber Operations Do Not Always Favor the Offense.” Policy Brief, *Quarterly Journal: International Security,* February 2017. Accessed March 15, 2020. <https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense> [↑](#footnote-ref-10)
11. “Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals”. Yale Review of International Studies. December 2017. Accessed March 10, 2020. <http://yris.yira.org/comments/2214> [↑](#footnote-ref-11)
12. “A Guide to Cyber Attribution”. Office of the Director of National Intelligence. September 14, 2018. Accessed March 10, 2020<https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf> [↑](#footnote-ref-12)
13. “A Guide to Cyber Attribution”. Office of the Director of National Intelligence. September 14, 2018. <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf> [↑](#footnote-ref-13)
14. Farrell, Henry. “Promoting Norms for Cyberspace”. Council on Foreign Relations. April 6, 2015. Accessed March 17, 2020. <https://www.cfr.org/report/promoting-norms-cyberspace> [↑](#footnote-ref-14)
15. “M-Trends 2020: Special Report”. FireEye. December 30, 2019. Accessed March 10, 2020. <https://content.fireeye.com/m-trends/rpt-m-trends-2020> [↑](#footnote-ref-15)
16. Lin, Herbert. Zegart, Amy. “Offensive Cyber Operations in US National Security.” Brookings Institute. April 26, 2019. Accessed April 2, 2020. <https://www.brookings.edu/wp-content/uploads/2018/10/978081573547_ch1.pdf> [↑](#footnote-ref-16)
17. Breeve, Keith. “Who are the Cyberwar Superpowers?” World Economic Forum. May 4, 2016. Accessed April 2, 2020. <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/> [↑](#footnote-ref-17)
18. Breeve, Keith. “Who are the Cyberwar Superpowers?” World Economic Forum. May 4, 2016. Accessed April 2, 2020. <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/> [↑](#footnote-ref-18)
19. Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. “Reconceptualizing Cyber Power.” Belfer Center, Harvard University. April 2020. Accessed April 15, 2020. <https://www.belfercenter.org/publication/reconceptualizing-cyber-power> [↑](#footnote-ref-19)
20. Benjamin Edwards, Alexander Furnas, Stephanie Forrest, Robert Axelrod. “Strategic aspects of cyberattack and blame.” Proceedings of the National Academy of Sciences. March 2017, Accessed April 20, 2020. [↑](#footnote-ref-20)
21. Benjamin Edwards, Alexander Furnas, Stephanie Forrest, Robert Axelrod. “Strategic aspects of cyberattack and blame.” Proceedings of the National Academy of Sciences. March 2017 Accessed April 20, 2020. [↑](#footnote-ref-21)
22. Trent, Stoney. “Cultivating Technology Innovation for Cyberspace Operations.” *The Cyber Defense Review*, vol. 3, no. 3, 2018, pp. 115–134. *JSTOR*, www.jstor.org/stable/26555001. Accessed 20 Apr. 2020. [↑](#footnote-ref-22)
23. “National Cyber Strategy of the United States of America”. The Office of the White House. September 2018. Accessed January 6, 2020. [↑](#footnote-ref-23)
24. Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. “Reconceptualizing Cyber Power.” Belfer Center, Harvard University. April 2020. Accessed April 15, 2020. <https://www.belfercenter.org/publication/reconceptualizing-cyber-power> [↑](#footnote-ref-24)
25. Interview with Government Source [↑](#footnote-ref-25)
26. “US Cyber Command History”. US Cyber Command. May 2020. Accessed April 2, 2020 <https://www.cybercom.mil/About/History/> [↑](#footnote-ref-26)
27. “US Cyber Command History”. US Cyber Command. May 2020. Accessed April 2, 2020 <https://www.cybercom.mil/About/History/> [↑](#footnote-ref-27)
28. Chen, Thomas M. “*AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*.” Strategic Studies Institute, US Army War College. 2013. Accessed April 2, 2020 [www.jstor.org/stable/resrep11200](http://www.jstor.org/stable/resrep11200).. [↑](#footnote-ref-28)
29. Chen, Thomas M. “*AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*.” Strategic Studies Institute, US Army War College. 2013. [www.jstor.org/stable/resrep11200](http://www.jstor.org/stable/resrep11200).. [↑](#footnote-ref-29)
30. Chen, Thomas M. “*AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*.” Strategic Studies Institute, US Army War College. 2013. [www.jstor.org/stable/resrep11200](http://www.jstor.org/stable/resrep11200).. [↑](#footnote-ref-30)
31. Lynn, William J. “Defending a New Domain: The Pentagon’s New Cyber Strategy”. Foreign Affairs. September 2010. Accessed March 6, 2020. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain> [↑](#footnote-ref-31)
32. Lynn, William J. “Defending a New Domain: The Pentagon’s New Cyber Strategy”. Foreign Affairs. September 2010. Accessed March 6, 2020. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain> [↑](#footnote-ref-32)
33. Bamford, James. “NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us into Cyber War.” Wired Magazine. June 6, 2012. Accessed March 27, 2020. <https://www.wired.com/2013/06/general-keith-alexander-cyberwar/> [↑](#footnote-ref-33)
34. Holloway, Michael. “Stuxnet Worm Attack on Iranian Nuclear Facilities”. Stanford University. July 16, 2015. Accessed March 27, 2020. <http://large.stanford.edu/courses/2015/ph241/holloway1/> [↑](#footnote-ref-34)
35. *“What is Stuxnet?*”. McAfee Corporation. July 2011. Accessed March 2, 2020. <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html> [↑](#footnote-ref-35)
36. *“What is Stuxnet?*”. McAfee Corporation. July 2011. Accessed March 2, 2020. <https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf> [↑](#footnote-ref-36)
37. Holger Stark. ["Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War"](http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html). *Der Spiegel*. August 8, 2011. Accessed March 2, 2020. [↑](#footnote-ref-37)
38. “Iran Denies Hacking into American Banks”. Reuters. September 18, 2012. Accessed March 12, 2020.

    <https://www.reuters.com/article/us-iran-cyberattacks-denial/iran-denies-hacking-into-american-banks-idUSBRE88M06O20120923> [↑](#footnote-ref-38)
39. “Background to Assessing Russian Activities in Recent US Elections: The Analytic Process and Cyber Incident Attribution”. Director of National Intelligence. January 6, 2017. Accessed April 4, 2020. <https://www.dni.gov/files/documents/ICA_2017_01.pdf> [↑](#footnote-ref-39)
40. Lewis, James Andrew. “A Map of the Most Dangerous Sources of Cybercrime.” McAfee. Center for International and Strategic Studies. March 6, 2018. Accessed April 2, 2020. <https://www.mcafee.com/blogs/enterprise/map-dangerous-sources-cybercrime/> [↑](#footnote-ref-40)
41. Senate Intelligence Committee: Russian and 2016 Election. FireEye. March 30, 2017. Accessed March 27, 2020. <https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf> [↑](#footnote-ref-41)
42. Alias: Fancy Bear [↑](#footnote-ref-42)
43. For further information look at   
    “APT 28: At the Center of the Storm. Russia Strategically Evolves Its Cyber Operations”. FireEye.

    <https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf> [↑](#footnote-ref-43)
44. “Background to Assessing Russian Activities in Recent US Elections: The Analytic Process and Cyber Incident Attribution”. Director of National Intelligence. January 6, 2017. Accessed April 4, 2020. <https://www.dni.gov/files/documents/ICA_2017_01.pdf> [↑](#footnote-ref-44)
45. “Background to Assessing Russian Activities in Recent US Elections: The Analytic Process and Cyber Incident Attribution”. Director of National Intelligence. January 6, 2017. Accessed April 4, 2020. <https://www.dni.gov/files/documents/ICA_2017_01.pdf> [↑](#footnote-ref-45)
46. Pomerleau, Mark. “Here’s How Cyber Command is Using ‘Defend Forward’”. Fifth Domain. November 12, 2019. Accessed April 20, 2020. <https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/> [↑](#footnote-ref-46)
47. “An Interview with Paul Nakasone”. 92nd NFQ. February 2019. Accessed April 20, 2020. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf> [↑](#footnote-ref-47)
48. “An Interview with Paul Nakasone”. 92nd NFQ. February 2019. Accessed April 20, 2020. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf> [↑](#footnote-ref-48)
49. Corrigan, Jack. “2018 Midterm Elections Were ‘the Most Secure’ in U.S. History, DHS Cyber Chief Says”. Next Government. March 13, 2019. Accessed April 20, 2020.

    <https://www.nextgov.com/cybersecurity/2019/03/2018-midterm-elections-were-most-secure-us-history-dhs-cyber-chief-says/155539/> [↑](#footnote-ref-49)
50. Fidler, David. “Year in Review: Cyber Threats and the Mid-Term U.S. Elections”. Council on Foreign Relations. January 2, 2019. Accessed April 20, 2020. cfr.org/blog/year-review-cyber-threats-and-mid-term-us-elections [↑](#footnote-ref-50)