NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 24, ISSUE 1: OCTOBER 2022

SEEING AND CONNECTING THE DOTS: LEGAL CHALLENGES TO COUNTERING FOREIGN CYBERATTACKS LAUNCHED FROM WITHIN U.S. DOMESTIC CYBERSPACE

Lieutenant Colonel Mark A. Visger*

Last year, General Nakasone, Commanding General of U.S. Cyber Command, testified to Congress that the foreign adversaries who conducted the SolarWinds hack utilized U.S. domestic cyberspace (consisting of leased Amazon Web Services cloud servers). Due to legal restrictions on U.S. Cyber Command operations in U.S. cyberspace, these foreign adversaries were able to avoid U.S. Cyber Command detection. In the words of General Nakasone, American adversaries "exploit[ed] a gap." As a result, he stated, "It's not that we can't connect the dots. We can't see all the dots." This tactic and potential methods of addressing this gap raise serious concerns, from the perspective of the Fourth Amendment, FISA, and the Executive Powers. This Article examines each of these three legal lenses and their intersections as applied to this new tactic, and concludes with considerations for lawmakers to address in attempting to resolve this challenge.

* Academy Professor, Army Cyber Institute at West Point, United States Military Academy. The author would like to thank the members of the Cybersecurity Law and Policy Scholars Conference—in particular, Amy Gaudion of Penn State Dickinson Law School—for their feedback on this Article. The views contained in this Article are those of the author and do not necessarily represent those of the Department of Defense, the United States Army, or the United States Military Academy.

TABLE OF CONTENTS

I. INTRODUCTION.....86
II. DOES THE FOURTH AMENDMENT, STANDING ALONE, PRECLUDE U.S. CYBER COMMAND OPERATIONS IN DOMESTIC CYBERSPACE WITHOUT A WARRANT?.....93
III. DOES FISA RESTRICT PRESIDENTIAL AUTHORITIES TO ENGAGE IN CYBERSPACE OPERATIONS AGAINST FOREIGN ADVERSARIES IN U.S. CYBERSPACE? 100
IV. DOES THE U.S. PRESIDENT HAVE THE CONSTITUTIONAL EXECUTIVE AUTHORITY TO UNILATERALLY DIRECT U.S. CYBER COMMAND OR ANOTHER U.S. GOVERNMENT AGENCY TO ENGAGE IN DOMESTIC CYBER OPERATIONS AGAINST A FOREIGN ADVERSARY? 104
V. CONCLUSION: THE NEED FOR A CYBER DOMESTIC AUTHORITIES STATUTE 110

I. INTRODUCTION

This Article will begin with two scenarios, one fictional and one with a recent real-life parallel.

In the first scenario, a foreign adversary has managed to surreptitiously place a nuclear bomb in a private residence in a major U.S. city. The military command charged with defending the homeland obtains intelligence of this fact and prepares a military operation to secure the bomb and neutralize the threat. In such an instance, the President would direct immediate military action to respond to this threat, with little concern for the Fourth Amendment warrant requirements or concerns about the military operating domestically.

In the second scenario, and one that mirrors real life, an adversary nation-state has initiated cyberspace operations against critical software and cybersecurity providers. This operation is routed through a U.S.-based cloud service, such as Amazon Web Services, with the computer commands needed to conduct the cyberattack sent from the Amazon account. If this cyberspace operation is successful, it will enable the widespread breach of numerous critical infrastructure networks, including the U.S.

government and the U.S. Department of Defense. Such a breach could result in the loss of untold amounts of sensitive data and could even allow a foreign adversary to take control of critical infrastructure—such as nuclear, water, or electrical systems—in such a way that results in widespread destruction and loss of life.

If the President were made aware of this cyberattack, there would be a great deal of questions as to his legal authority to counter this cyber threat, in stark contrast to the President's clear authority in the first scenario. Specifically, one could envision the President asking his Attorney General whether he has the legal authority to order U.S. government agencies to access the Amazon Web Services server to interdict this attack. According to the Congressional testimony of General Paul Nakasone, Commanding General of U.S. Cyber Command, the answer to this hypothetical question may very well be "no."[1]

This second scenario outlined in the previous paragraph is modeled after the recent SolarWinds cyberattack,[2] which has been attributed as the likely work of the Russian government.[3] In his testimony to Congress about the attack, General Nakasone stated that his command does not have the legal authority to operate in U.S. cyberspace to prevent, let alone observe, such an attack.[4] In addition, General Nakasone has indicated that American adversaries are aware of this legal limitation and are actively exploiting it by basing

---

[1] *See* Brad D. Williams, *Nakasone Warns Adversaries Hack Unseen in U.S.*, BREAKING DEFENSE (Mar. 25, 2021), https://breakingdefense.com/2021/03/nakasone-warns-adversaries-hack-unseen-in-us [https://perma.cc/4AGU-VKBW] (citing "legal barriers and disincentives" to obtaining information on "attacks [taking] place within the US" and noting that US adversaries understand and exploit these legal limits).

[2] In this attack, hackers breached SolarWinds' network, using this access to place malicious code in software updates to SolarWinds' Orion software, resulting in the compromise of over 18,000 customers who used the Orion software, including multiple U.S. government agencies.

[3] David E. Sanger et al., *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. TIMES (Jan. 2, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html [https://perma.cc/9QBP-6YKS].

[4] Williams, *supra* note 1.

their cyber operations within the United States, presumably operating out of U.S. networks from overseas.[5]

The advent of cyberspace operations, particularly in the context of the eponymous Great Power Competition, has had profound global and domestic implications. Suggesting that the advent of the internet has profoundly revolutionized every aspect of society is not hyperbolic. These effects extend to the legal context, particularly as it relates to laws governing cyberspace in general and specifically to conflict in cyberspace. Much ink has been spilled on how to apply legal frameworks to cyberspace operations, and many gaps and ambiguities remain, with American adversaries actively taking advantage of these gaps, the so-called "gray zones" of the law.[6] In the arena of domestic authorities for U.S. cyber operations, Congress has been very active in giving the military, particularly the U.S. Cyber Command,[7] the legal authority necessary to conduct operations in foreign cyberspace.[8] Despite these developments, General Nakasone clearly specified in his testimony to Congress

---

[5] *See id.*

[6] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1, 3 (2017), https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf [https://perma.cc/2TQD-2BG7].

[7] U.S. Cyber Command is the United States' military command engaged in cyberspace operations. Composed of military, intelligence, and information technology resources, U.S Cyber Command's "mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. [It] defends the Department of Defense information systems, supports joint force commanders with cyberspace operations, and defends the nation from significant cyberattacks." *Our History*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/History/#:~:text=The%20Command%20comprises%20military%2C%20intelligence,with%20domestic%20and%20international%20partners [https://perma.cc/U9LX-PNTD] (last visited Sept. 29, 2022). The Commander of the U.S. Cyber Command also serves as the Director of the National Security Agency in a "dual-hat" role. *Id.*

[8] *See generally* Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, HOOVER INST. (July 29, 2020), https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf [https://perma.cc/8F72-XUWT] (outlining the congressional action taken to address gaps in the legal authorities for the military to conduct cyber operations).

that it was not the role of U.S. Cyber Command to operate in U.S. cyberspace, citing the Fourth Amendment to the U.S. Constitution.[9]

This Article further examines General Nakasone's contention regarding operations in domestic cyberspace against foreign nation-state adversaries. Specifically, this Article seeks to examine nation-state cyber operations against the United States which use private U.S. cyberspace to accomplish an attack impacting U.S. national security. For instance, in the SolarWinds operations, the attacker (attributed to be Russia) apparently purchased computer server capacity from Amazon Web Services.[10] Such a purchase would be no different than any corporate or personal purchase of cloud computing capacity that is routine today. Then, according to Senator Richard Burr,[11] this cloud computing service was used to host the "secondary command and control nodes . . . exploiting domestic infrastructure for the command and control to hide the nefarious traffic in legitimate traffic."[12] Senator Burr further noted the advantage that such a step affords those engaging in cyber operations from overseas: "Given the legal restrictions on the intelligence community, we don't have the ability to surveil the domestic infrastructure."[13] This Article is intended to examine this limited problem: cyber operations conducted by nation-state actors that utilize private (i.e., non-governmental) U.S. cyberspace to

---

[9] Williams, *supra* note 1.

[10] *See* Donna Goodison & Michael Novinson, *AWS: SolarWinds Hackers Used our Elastic Compute Cloud*, CRN (Feb. 25, 2021, 1:22 PM), https://www.crn.com/news/security/aws-solarwinds-hackers-used-our-elastic-compute-cloud [https://perma.cc/8MQ9-RPVK].

[11] Senator Richard Burr (R-NC) is the former Chair of the Senate Intelligence Committee. *See, e.g.*, Patricia Zengerie & Sarah Lynch, *U.S. Senator Burr Steps Aside as Committee Chair as FBI Probes Stock Trades*, REUTERS (Oct. 4, 2020, 2:11 AM), https://www.reuters.com/article/us-health-coronavirus-usa-burr/u-s-senator-burr-steps-aside-as-committee-chair-as-fbi-probes-stock-trades-idUSKBN22Q0NB [https://perma.cc/PE8U-4ZGD].

[12] Michael Novinson, *10 Boldest Statements from the SolarWinds Senate Hearing*, CRN (Feb. 24, 2021, 10:05 AM), https://www.crn.com/slide-shows/security/10-boldest-statements-from-the-solarwinds-senate-hearing/11 [https://perma.cc/5UK8-M46J]. A video of the hearing is available at: https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary [https://perma.cc/6UGC-XAK5].

[13] *Id.*

effect the attack in order to evade legal restrictions on domestic surveillance.

Another aspect of this problem that should be addressed from the outset is the identity of the federal agency tasked with the responsibility of interdicting or preventing the cyberattack. Generally, the military operates in cyberspace outside of the U.S., acting against foreign adversaries under a "Defend Forward" framework.[14] The intelligence apparatus does have the ability to operate domestically under the Federal Intelligence Surveillance Act ("FISA") authorities, which generally requires a FISA warrant.[15] Domestic cyberspace incident response falls under the purview of the Department of Homeland Security and the Department of Justice, who presumptively would be required to comply with Fourth Amendment limits when operating on private cyberspace within the U.S.[16] Notably, the purview of U.S. Cyber Command has seen expansion into areas not traditionally considered to be military in nature, such as countering foreign information activities and ransomware botnets.[17] No matter the identity of the agency designated to respond and/or prevent such an incident, the potential for the Fourth Amendment and FISA to conflict with executive authority to defend the nation will present a challenge to any potential federal response.

---

[14] *See generally* Erica Lonergan, *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior*, LAWFARE (Mar. 12, 2020, 3:28 PM), https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior [https://perma.cc/QN6J-VZ4Z] (describing the benefits of U.S. Cyber Command operating in foreign adversary networks to impose costs and deter cyber attacks under the Defend Forward framework). The Defend Forward framework involves ongoing operations by U.S. Cyber Command to counter adversary cyber operations through U.S. Cyber Command operations in their adversaries' cyberspace. *Id.*

[15] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–85.

[16] *Presidential Policy Directive 41—United States Cyber Incident Coordination*, WHITE HOUSE PRESS SEC'Y (July 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident [https://perma.cc/SGK9-QW8Q].

[17] Jason Healey, *When Should U.S. Cyber Command Take Down Criminal Botnets?*, LAWFARE (Apr. 26, 2021, 2:51 PM), https://www.lawfareblog.com/when-should-us-cyber-command-take-down-criminal-botnets [https://perma.cc/4NYV-9DZT].

Given that American adversaries are aware of this limitation in domestic cyberspace, there is no doubt that they will continue to exploit this gap and expand these types of cyber operations against the U.S. Such attacks could readily reach the point where the President deems it necessary to order U.S. Cyber Command to operate against foreign adversaries in domestic cyberspace. In such an instance, the President would likely cite his Commander-in-Chief duty to defend the homeland.[18] If foreign nation-state attacks of this nature were more common, it would not be surprising to see the President direct such domestic operations based on a claim of both inherent executive authority, as well as his duty to defend the nation. Thus, there is a need to clearly define the legal authorities involved and the circumstances under which such activities would be legally justified and appropriate.

That said, the prospect of unilateral presidential orders to conduct military cyber operations in domestic cyberspace should give pause for several reasons. First, there is the serious risk of government intrusion into private property on U.S. soil. Private entities generally do not report cyberattacks, let alone seek government assistance to counter cyberattacks.[19] Most corporations would likely refuse to allow government personnel on their networks to respond to an attack such as SolarWinds. In addition, there is a concern of executive overreach, much like the excessive and abusive domestic wiretapping identified in the Church Commission Report, resulting in the passage of FISA.[20] More recently, the exercise of FISA wiretaps against members of the Trump 2016 presidential campaign has resulted in additional controversy over this statute.[21]

---

[18] The Prize Cases, 67 U.S. 635, 668 (1862).

[19] Gerritt De Vynck, *Many Ransomware Attacks Go Unreported. The FBI and Congress Want to Change That*, WASH. POST (July 27, 2021, 7:32 PM), https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/ [https://perma.cc/ARF8-NV2M].

[20] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 581–82 (5th ed. 2011).

[21] *See generally* Bernard Horowitz, *FISA, The "Wall," and Crossfire Hurricane: A Contextualized Legal History*, 7 NAT'L SEC. L. J. 1, 4 (2019) (describing the use of FISA warrants in connection with the 2016 Trump presidential campaign and the political and legal controversy that followed).

Due to the importance of these issues and the significant legal and policy concerns they generate, Congress and the President should work together to develop a framework for countering foreign nation-state cyberattacks operated from within U.S. cyberspace. The prospect of such cyberspace operations challenges many pre-existing paradigms, and the exercise of this authority requires a good deal of circumspection and negotiation from both Congress and the President in developing the framework for such possibilities.

This Article argues that the nature of current cyberspace operations requires a more detailed examination of the legal framework addressing foreign adversary cyber operations that utilize domestic U.S. civilian cyberspace to evade current U.S. domestic legal restrictions. While FISA currently has a strong, and perhaps controlling, bearing on such operations, the nature of malign foreign cyberspace operations more directly implicates the President's authority to repel attacks on the homeland than what FISA contemplates. FISA is focused on intelligence collection and the electronic surveillance of substantive communications of foreign powers, agents of foreign powers, and terrorists. As the title of the statute implies, the focus is on intelligence. For example, in a terrorist situation, the government seeks to intercept communications about a pending attack in order to thwart the attack. In cyberspace operations, the communication is the attack.[22] As a rough (and admittedly imperfect) analog, imagine the Attorney General seeking a FISA warrant before the National Command Authority authorized the downing of the fourth hijacked plane during the September 11 terrorist attack. A hijacked U.S. plane being used as a weapon to conduct an attack on U.S. soil could be engaged with no thought given to whether a warrant was required. On the other hand, a domestic cyberattack with similar kinetic effects might require a warrant to interdict because the attack is sent as computer code through communication lines, where expectations

[22] Even in a phishing attack, where the attacker sends a malicious email to an unwitting recipient, the substance of the actual communication in the email is largely irrelevant. Instead, the attacker's main purpose is to trick the recipient into clicking a website link in the email or open an attachment to the email containing malicious code. *See* BRIAN W. KERNIGHAN, UNDERSTANDING THE DIGITAL WORLD 192–94 (2d ed. 2021) (describing various forms of phishing attacks).

of privacy are at play. This key difference should drive a new way of looking at domestic cyberspace operations.

However, the prospect of U.S. Cyber Command, or any U.S. government entity, rooting around on private Amazon Web Services accounts or other domestic cyberspace is also greatly concerning. Such actions would potentially entail a much higher level of intrusion, dwarfing the additional authorities granted in the Patriot Act passed in the wake of the September 11 attacks—with the attendant opposition from large parts of American civil society. Because the President has a much stronger claim to inherent executive authority to act in the case of cyberattacks threatening grave harm to the nation, and because the policy considerations and potential problem areas are much more significant, Congress and the President should come together to enact a statute that provides a legal framework to resolve these challenges. Thorough consideration and discussion between the political branches are needed to arrive at a mutually agreeable solution.

This Article reviews the legal landscape surrounding General Nakasone's testimony. Specifically, it examines the Fourth Amendment jurisprudence, the applicability of FISA, and the inherent executive authority. This Article concludes with recommended considerations that should be addressed when drafting a legal framework to address this topic.

II. DOES THE FOURTH AMENDMENT, STANDING ALONE, PRECLUDE U.S. CYBER COMMAND OPERATIONS IN DOMESTIC CYBERSPACE WITHOUT A WARRANT?

In examining the legal framework for potential domestic U.S. Cyber Command operations, it is important to separate out the Fourth Amendment requirements and FISA requirements. The question of Fourth Amendment search and seizure law is a complex one, and a detailed review of the specifics of the warrant requirement and the various exceptions to the warrant requirement is beyond the scope of this Article. However, a higher-level review of the larger themes of Fourth Amendment search and seizure law, as well as its linkages to FISA, is needed to provide a backdrop to

the issue, especially in light of claims that the Fourth Amendment precludes U.S. Cyber Command domestic operations.

First, although the Supreme Court has not directly ruled on the issue, there is widespread acceptance that Fourth Amendment warrants are not required in the context of surveillance of foreign powers to defend national security. In establishing a warrant requirement for electronic surveillance, *United States v. Katz* specifically declined to address "situation[s] involving the national security."[23] Similarly, while the Supreme Court in *United States v. United States District Court (Keith)* ruled that warrantless surveillance of domestic security threats violated the Fourth Amendment, the Court was careful to distinguish between domestic security threats and threats involving foreign powers.[24] Further, foreign persons located outside the United States are not protected by the Fourth Amendment.[25]

Additional development of case law surrounding the warrantless surveillance of foreign powers was circumscribed by the passage of FISA, although the Fourth Circuit opinion in *United States v. Truong Dinh Hung* is widely cited as establishing the principle that the Fourth Amendment does not require a warrant "when the object of the search or the surveillance is a foreign power, its agent or collaborators."[26] It is important to note that *Truong Dinh Hung* was decided in the FISA "twilight zone." In other words, *Truong Dinh Hung* arose prior to FISA, thus the terms of the statute did not apply, but FISA had been passed into law before the court's decision. The court's language in footnote four recognized the delicate nature of the subject and the resulting judicial deference to the political branches:

> [T]he complexity of the statute also suggests that the imposition of a warrant requirement, beyond the constitutional minimum described in this opinion, should be left to the intricate balancing performed in the course of the legislative process by Congress and the President. The elaborate structure of the statute demonstrates that the political branches

---

[23] United States v. Katz, 389 U.S. 347, 358 n.23 (1967).

[24] *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 309 n.8 (1972).

[25] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

[26] United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982).

> need great flexibility to reach the compromises and formulate the standards which will govern foreign intelligence surveillance.[27]

Second, where a warrant is not required, the base Fourth Amendment requirement is reasonableness. A reasonableness assessment requires the balancing of "the degree of the government's intrusion on individual privacy [and] the degree to which that intrusion furthers the government's legitimate interests."[28] In analyzing FISA surveillance against the Fourth Amendment reasonableness standard, the government interests are considered from a programmatic perspective, such as examining the overall purpose of the government program in question. In *In re Sealed Case*,[29] the court reviewed FISA requirements, as amended by the Patriot Act, and noted that "FISA's general programmatic purpose" was "to protect the nation against terrorists and espionage threats directed by foreign powers."[30] This programmatic purpose was a large part of the reason that the court concluded that the amended FISA met the Fourth Amendment reasonableness requirement.[31] National security is traditionally described as being of the highest order.[32] The government interests in countering foreign malicious cyberspace activities would also likely qualify as furthering the national security interest.

While there are a number of Foreign Intelligence Surveillance Court ("FISC") opinions relating to Fourth Amendment analysis of various aspects of FISA surveillance, the most comprehensive reasonableness analysis took place in the FISC opinion in *In re Certified Question of Law*.[33] At issue in this case was the

---

[27] *Id.* at 914 n.4.

[28] *In re* Certified Question of Law, 858 F.3d 591, 607 (FISA Ct. Rev. 2016) (citing Wyoming v. Houghton*,* 526 U.S. 295 300 (1999)).

[29] 310 F.3d 717 (FISA Ct. Rev. 2002).

[30] *Id.* at 746. *See also In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011–12 (FISA Ct. Rev. 2008) (containing similar programmatic purpose analysis).

[31] *See In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

[32] *In re* Certified Question of Law*,* 858 F.3d at 608 (citing Haig v. Agee, 453 U.S. 280, 307 (1981)).

[33] *See id.* at 607–08.

interception of what are called "post-cut-through digits," as part of the pen register/trap-and-trace device:[34]

> "Post-cut-through digits" are numbers or characters that are dialed after the call is initially connected or "cut through." Frequently, those numbers are other telephone numbers, as when a caller places a calling card, credit card, or collect call by first dialing a carrier access number and then, after the initial call is "cut through," dialing the telephone number of the intended recipient.[35]

The FISC judge authorized collection of this data, despite the fact that such information might include content. For example, data could include content if a caller entered bank account information instead of dialing a secondary phone number. However, the FISC judge included the proviso that the investigators could not use captured digits that did not constitute dialing information.[36] In ruling on the reasonableness of the capture of the post-cut-through digits, the court cited seven factors:

> (1) [T]he paramount interest in investigating possible threats to national security;
>
> (2) the investigative importance of having access to the dialing information provided by post-cut-through digits;
>
> (3) the incidental nature of the collection of content information from post-cut-through digits;
>
> (4) the relatively slight intrusion on privacy entailed by the acquisition of post-cut-through digits;
>
> (5) the prohibition against the use of any content information obtained from the pen register or trap-and-trace device;
>
> (6) the steps taken by the government to minimize the dissemination of post-cut-through digits; and
>
> (7) the fact that FISA pen register interceptions are conducted only with the approval and under the supervision of a neutral magistrate, in this case a FISC judge.[37]

Applying the reasonableness analysis from *Certified Question of Law* to the prospect of domestic cyber operations to counter foreign cyberattacks, the considerations are largely the same, with two significant differences. First, assuming the FISA process was not

---

[34] *Id.* at 592.
[35] *Id.* at 593–94.
[36] *Id.* at 594.
[37] *Id.* at 607–08.

utilized to authorize such operations and the operation was based on inherent executive power, the lack of judicial oversight or process raises concern from a Fourth Amendment perspective. Second, the level of intrusiveness into U.S. cyber infrastructure and the concomitant potential for incidental collection of U.S. persons' information are much greater than what might occur in a search for post-cut-through digits. For example, if a foreign adversary compromised a U.S. person's Amazon Web Services account and used the hacked account to launch attacks, U.S. government personnel responding to the attack might incidentally have access to the private information on that account, such as photos, correspondence, and other private documents.

The FISC Court's Fourth Amendment analysis of Section 702 collection, which is based on certifications made to the FISC by the Attorney General and the Director of National Intelligence, likely provides a more apt parallel and addresses these two particular concerns.[38] In examining the reasonableness of these certifications, in light of the risk of incidental U.S. person surveillance, the court focused on two considerations. First, the proposed targeting list was "reasonably designed to limit acquisitions to those targets reasonably believed to be non-United States persons located outside the United States."[39] Second, the minimization and querying procedures "adequately guard[ed] against error and abuse,"[40] thereby "reduc[ing] the intrusiveness of the acquisition for Fourth Amendment purposes by restricting use or disclosure of such information."[41] While the recent FISC Section 702 ruling was not without its critics in light of previously-identified missteps in Section 702 collection,[42] the primary focus of those criticisms was

[38] *Re* Section 702 2020 Certification, FISA Ct. Memorandum Opinion Nov. 18, 2020 (FISA Ct. 2020), https://www.intelligence.gov/assets/documents/20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf [https://perma.cc/Q5SY-TNWZ].

[39] *Id.* at 32.

[40] *Id.* at 34–35.

[41] *Id.* at 32.

[42] *See* George Croner, *To Oversee or to Overrule: What is the Role of the Foreign Intelligence Surveillance Court Under FISA Section 702?*, LAWFARE (May 18, 2021, 8:01 AM), https://www.lawfareblog.com/oversee-or-overrule-what-role-foreign-intelligence-surveillance-court-under-fisa-section-702

the court's acceptance of the certifications in light of alleged significant errors in previous certifications.[43] The constitutional analysis is not implicated by this critique and controversy that has ensued.

If the government were to engage in nonconsensual access to U.S. servers, whether through Congressional authorization or through inherent executive authority, meeting the base Fourth Amendment reasonableness requirement would likely utilize similar considerations. Factors for potential consideration are: (1) the degree of confidence that the target is a foreign power or agent of a foreign power operating from outside the United States; (2) the identified programmatic purposes of the operation, with an emphasis on specifying high-level national security concerns; (3) any minimization procedures emplaced to mitigate the possibility of U.S. persons' information being collected and/or retained; and (4) the degree to which the operation intercepts computer code (e.g., technical instructions to the computer or dialing/routing/addressing/signaling information) vs. substantive communications content (e.g., emails or other actual conversations between humans).

In this context, it is not difficult to design a process within the executive branch that would meet Fourth Amendment reasonableness standards. It is advisable to design minimization procedures similar to those found in FISA that would reduce the level of intrusion and potential for misuse against communications by U.S. persons.[44] Other considerations that the executive branch should consider include: (1) the degree of certainty that the

---

[https://perma.cc/LVW2-U8VC] (outlining the criticisms of Section 702 collection and FISA Court approval of 702 certifications).

[43] *Id.*

[44] *See* 50 U.S.C. § 1801(h). Minimization procedures, in the FISA context, are defined as procedures adopted by the Attorney General which are "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." Prior to issuing a FISA warrant, a FISA judge must find that the proposed minimization procedures meet these standards and order that they be followed. §§ 1805(a)(3), (c)(2)(A).

malicious actor is an agent of a foreign government, (2) the types and degrees of intrusiveness of U.S. persons' information, and (3) a clearly identified and articulated national security nexus. With the national security programmatic justification, a government cyber operation in U.S. cyberspace to interdict a foreign attack would likely pass Fourth Amendment scrutiny if sufficient procedures were in place to protect U.S. persons from unwarranted intrusion.

As a result, the Fourth Amendment, standing alone, is not a significant roadblock to a potential U.S. Cyber Command operation against foreign nation-state adversaries using U.S. cyber infrastructure from overseas to engage in cyberattacks, assuming that the program is designed in a way that meets the reasonableness requirements. That said, it is very difficult to conduct a Fourth Amendment analysis in a vacuum without considering the FISA framework, which codified and channelized the process by which the executive exercised this Fourth Amendment foreign surveillance exception. Due to the passage of FISA and the general executive compliance in following the FISA framework, case law interpreting the contours of national security surveillance authority is limited. There are a few publicly available reported cases from the FISC and scattered federal decisions arising from the pre-FISA timeframe.[45] This Fourth Amendment/FISA interplay is likely what contributed to General Nakasone's conclusion that the Fourth Amendment prevented U.S. Cyber Command operations in domestic networks. Including FISA considerations raises additional questions: How would FISA be implicated in a situation where a malign foreign actor co-opts a private Amazon Web Services account and uses the account to stage significant cyberattacks? Is a FISA warrant required in such instances? The next section addresses these questions.

---

[45] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 912–14 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), *cert. denied*, 419 U.S. 88 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974).

III. DOES FISA RESTRICT PRESIDENTIAL AUTHORITIES TO ENGAGE IN CYBERSPACE OPERATIONS AGAINST FOREIGN ADVERSARIES IN U.S. CYBERSPACE?

The history of electronic surveillance in the post-*Katz* era has been well-documented, particularly in the era of Patriot Act expansion of surveillance authorities in connection with the War on Terror. This Article does not go into great detail about this history, as it has been covered extensively in other literature.[46] For the purposes of this Article, this section outlines several key observations that can be drawn from the history of FISA, as it relates to the prospect of the U.S. government operating against foreign actors in U.S. cyberspace.

First, Congressional intent for FISA to serve as the sole statutory framework and the exclusive means by which the executive branch engages in domestic national security surveillance is clear. Accordingly, Congress' position means that any executive action in this field outside of the FISA framework places the President in Category 3, "Lowest Ebb," in the *Youngstown Steel* framework.[47] The clearest expression of this fact is the provision for criminal and civil liability for one who "engages in electronic surveillance under color of law except as authorized by [FISA] or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of [FISA]."[48] In case there was any question as to Congress' intent, Section 1812(a) highlights that "the procedures of [Title III and FISA] shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications

---

[46] *See generally* STEWART BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010) (providing a comprehensive history of FISA, particularly as it relates to the 9-11 attacks).

[47] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637–38 (1952) (Jackson, J., concurring). This concurring opinion lays out three categories of presidential authority. In the first, "the President acts pursuant to an express or implied authorization of Congress," and "his authority is at its maximum." *Id.* at 635. In the second, "the President acts in absence of either a congressional grant or denial of authority," which results in the President acting in a "zone of twilight." *Id.* at 637. In the third, referenced above, "the President takes measures incompatible with the expressed or implied will of Congress." *Id.*

[48] 50 U.S.C. §§ 1809(a)(1) (criminal liability), 1810 (civil liability).

may be conducted."[49] Further, "[o]nly an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications" may serve as an additional authority for executive branch electronic surveillance.[50] As if it did not make its point clear enough, Congress also repealed the provision in its Title III wiretap laws recognizing the "constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack [and] to obtain foreign intelligence information deemed essential to the security of the United States."[51]

Second, by its terms, FISA seems to require a FISA warrant in order to nonconsensually breach a private domestic network to repel a foreign attack. Such an outcome is not surprising given the expansive language embodying Congress' attempt to preclude any possible claim of inherent executive authority to conduct surveillance. Even though the statute was written before the prospect of cyberattacks was a consideration, the definitions are broad enough to include even the computer communications associated with a cyberattack. A review of the terms of FISA, followed by an application of these provisions to a SolarWinds-type attack, demonstrates this fact.

Several FISA definitions are worthy of mention, by way of review. Foreign intelligence is defined as follows:

> (1) [I]nformation that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> (A) the national defense or the security of the United States; or

---

[49] § 1812(a).
[50] § 1812(b).
[51] 82 Stat. 214 (1968) (formerly codified at 18 U.S.C. § 2511(3)).

(B) the conduct of the foreign affairs of the United States.[52]

This broad definition would encompass potential cyberattacks by foreign powers, particularly if the attack was intended to gather information (thus constituting "clandestine intelligence activities") or was intended to create negative effects within the United States (defined as an "actual or potential attack or other grave hostile acts of a foreign power"). The relevant provision defining "electronic surveillance" includes: "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States."[53] In addition, the definition of "United States person" includes United States corporations and other unincorporated associations comprised of a majority of United States persons.[54] If these definitions are met, and the executive branch seeks to engage in surveillance within the United States to obtain foreign intelligence information, a FISA warrant is generally required unless a specified exception is utilized.[55]

Considering how these definitions might apply to a situation like the SolarWinds attack, where the attackers utilized "leased virtual private servers hosted within US data centers,"[56] one can understand why General Nakasone testified that this activity is a "blind spot" for U.S. Cyber Command.[57] Internet service providers and similar cloud service providers located in the United States would qualify as "United States persons" under the FISA definition, and the malicious cyber activities in question would likely qualify as "foreign intelligence information" (assuming that it could be

---

[52] 50 U.S.C. § 1801(e).

[53] § 1801(f)(2). The definition then exempts the acquisition of communications of computer trespassers as defined by 18 U.S.C. § 2511(2)(i). This exemption provides little additional support, however, because Section 2511 requires that "the owner or operator of the protected computer authorize[] the interception." 18 U.S.C. § 2511(2)(i)(I).

[54] 50 U.S.C. § 1801(i).

[55] *See* § 1812 (specifying the "exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronics communications may be conducted").

[56] Williams, *supra* note 1.

[57] *Id.*

established that the threat actor was a foreign power or agent of a foreign power—if not, then the even more restrictive Title III wiretap provisions may apply). As a result, it appears that a FISA warrant would be required in order to operate in domestic cyberspace to respond to a cyberattack by a foreign power.

When examining these attacks from a FISA perspective, two implications should be considered. First, General Nakasone was clear that he was not requesting the authority to operate from within the United States, either in his capacity as the Director of the National Security Agency ("NSA") or as the Commander of U.S. Cyber Command. Instead, in testimony which was described as "highly nuanced,"[58] General Nakasone identified a key gap that needs to be addressed by policy makers and legislators, not by intelligence and cyber personnel. In fact, this blind spot would apply to any U.S. government agency attempting to interdict cyberattacks in domestic cyberspace.

Second, when one examines FISA and the purposes of FISA, there appears to be a disconnect between the concept of electronic surveillance to intercept substantive communications to gather foreign intelligence and the prospect of countering a foreign adversary engaging in a cyberattack routed through domestic cyberspace. The statutory definitions are written very broadly to include cyberattacks—even though Congress likely did not contemplate or consider the prospect of international cyberattacks when FISA was enacted in the 1970s. The main goal of electronic surveillance is to intercept substantive communications (e.g., conversations). Generally, this surveillance is conducted in order to develop intelligence about threats to the national security or to gather foreign intelligence. Since *Katz*, substantive communication has generally been protected under the Fourth Amendment.

In the case of cyberattacks, the actual "communication" (e.g., the bits and bytes crossing the wire) does not follow the traditional understanding of communication between two individuals. Instead, the communication is likely computer code, computer commands, or similar information directed at a computer system, directing the computer system to engage in specific activities. These

[58] *Id.*

communications are similar to the non-content "dialing, routing, addressing, and signaling" information described in *Certified Question of Law*.[59] The Court of Review in that case noted a distinction between content information (e.g., interception of communications or content of email)[60] and non-content information, (e.g., dialing information).[61] There is one further distinction besides the content/non-content dichotomy: In many cases, the cyberattack is not a communication *about* the attack, it *is* the attack. It is difficult to envision a situation where substantive conversations could have the same effect as a cyberattack. In addition, as will be noted in the next section, the prospect of a cyberattack strongly implicates the inherent executive authority that a President would have to counter the attack, even outside of the FISA framework.

In the case of an ongoing cyberattack threatening grave harm to the nation, the President may deem it so serious that he directs U.S. Cyber Command (or another U.S. government agency) to operate on domestic networks, without the knowledge or consent of the network owners, in order to defend the nation. This possibility raises an additional question: does the President have inherent executive authority to order military action in U.S. cyberspace? The prospect of an attack on the nation would no doubt implicate inherent executive authority as well. The next section addresses this issue.

IV. DOES THE U.S. PRESIDENT HAVE THE CONSTITUTIONAL EXECUTIVE AUTHORITY TO UNILATERALLY DIRECT U.S. CYBER COMMAND OR ANOTHER U.S. GOVERNMENT AGENCY TO ENGAGE IN DOMESTIC CYBER OPERATIONS AGAINST A FOREIGN ADVERSARY?

FISA's broad scope creates the potential for conflict between Congress' intent to strictly regulate surveillance and channelize all foreign intelligence surveillance into the FISA framework against the constitutional authority/duty of the President to defend the nation. With FISA, Congress intended to wholly encompass all domestic intelligence gathering operations and negate any possible

---

[59] *In re* Certified Question of Law, 858 F.3d 591, 592 (FISA Ct. Rev. 2016).
[60] *Id.* at 604 (citations omitted).
[61] *Id.* (citing Smith v. Maryland, 442 U.S. 735 (1979)).

claims of inherent executive authority to engage in surveillance outside of this framework—with criminal and civil liability to those who violate its provisions.[62] However, the President's Commander-in-Chief authority is considerable, with the attendant gravity of his/her duty to protect the nation from attack.[63] As a result, the line between Congress and the President in this regard is murky and undefined—which is not a particularly good state of affairs given the ongoing threat and the demonstrated willingness of foreign adversaries to exploit this blind spot.

The starting point in examining this area is to review the controversy that arose over the Terrorist Surveillance Program in the aftermath of the September 11 attacks. Here, President Bush asserted inherent executive authority, as well as the Congressional Authorization to Use Military Force ("AUMF"), against those who perpetrated the September 11 attacks to justify surveillance outside of the FISA framework—specifically, monitoring phone calls and emails into or outside of the United States involving one party who was linked to al Qaeda or affiliated organizations.[64] The Executive's rationale was that FISA did not provide the "speed and agility" needed to combat the ongoing terrorism threat.[65] A review of the President's position and the resolution of this controversy will be helpful to the issue at hand.

In this instance, President Bush relied on the inherent executive authority of the President as Commander in Chief, with the "responsibility to protect the Nation from further attacks."[66] The President also asserted additional authority from the AUMF against

---

[62] *See supra* text accompanying notes 49–53.

[63] *See generally* Saikrishna Prakash, *Unleashing the Dogs of War: What the Constitution Means by "Declare War,"* 93 CORNELL L. REV. 45 (2007); Michael D. Ramsey, *The President's Power to Respond to Attacks*, 93 CORNELL L. REV. 169 (2007).

[64] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/92PL-VNJX].

[65] Letter from William E. Moschella, Assistant Att'y Gen., to The Honorable Pat Roberts, Chairman, Senate Select Comm. on Intel., *et al.* (Dec. 22, 2005) [hereinafter Moschella Letter].

[66] *Id.* at 2.

the perpetrators of the September 11 attacks.[67] Drawing from the Supreme Court's decision in *Hamdi*, which recognized detention as an inherent part of the use of force authorized by Congress, the Department of Justice argued that communications intelligence was also included as a "fundamental incident of the use of military force."[68]

This AUMF argument had two apparent weaknesses. First, the AUMF did not specifically include an exception to FISA, as required by the FISA statute.[69] Second, the fact that FISA contained a fifteen day limited exception in cases of declaration of war suggests that Congress did not intend for FISA to be superseded in cases of military conflict.[70] The executive branch sought to sidestep these concerns by arguing for an expansive interpretation of the AUMF (i.e., arguing that the AUMF in fact included the authorization to engage in the interception of domestic signals within the overall authorization to use military force) in order to avoid a constitutional violation—specifically, to avoid the claimed unconstitutional limitation of the President's inherent executive authority.[71] The Bush Administration's claims were never tested in court, however, and no court ruled on the substantive legal claims that the Administration advanced to justify the program.[72]

While the lack of a legal resolution to these arguments does little to illuminate the resolution of our hypothetical domestic cyberattack, the political outcome provides some help. The Executive apparently sought to move the Terrorist Surveillance Program within the FISA framework and had mixed success before the FISA court.[73] The Administration ultimately abandoned the program in May 2007.[74] One year later, Section 702 of the FISA

---

[67] *Id.* at 2–3.

[68] *Id.* at 3.

[69] 50 U.S.C. § 1812(a).

[70] *See* § 1811. *See also* Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea 37 (Jan. 5, 2006) (on file with the Congressional Research Service).

[71] Moschella Letter, *supra* note 65, at 4.

[72] DYCUS ET AL., *supra* note 20, at 600. Cases challenging the program were dismissed primarily on standing and state secrets grounds. *Id.*

[73] *Id*. at 619.

[74] *Id*.

Amendments Act provided substantially the same authority.[75] In essence, the political branches negotiated a truce: The President backed away from his claims of unilateral executive authority, and Congress then granted the authority that the President had been exercising. This outcome is not surprising, as Congress likely does not want to be held responsible, in the event of an attack, for failing to give the President the tools that he asserted were necessary to prevent the attack. From a political perspective, this outcome is probably best described as a tie, with no clear winner or loser.

Despite this outcome, there is likely a point where the President does have inherent authority to engage in surveillance outside of the FISA requirements. Even the congressional staff attorneys reviewing the Executive's Terrorist Surveillance Program arguments grudgingly conceded this point:

> Court cases evaluating the legality of warrantless wiretaps for foreign intelligence purposes provide some support for the assertion that the President possesses inherent authority to conduct such surveillance. The Court of Review, the only appellate court to have addressed the issue since the passage of FISA, "took for granted" that the President has inherent authority to conduct foreign intelligence electronic surveillance under his Article II powers, stating that, "assuming that was so, FISA could not encroach on that authority."[76]

Not surprisingly, the congressional staff attorneys caveated their conclusion by noting that "no court has ruled on the question of Congress'[] authority to regulate the collection of foreign intelligence information."[77] Despite the hedging, there is slender but significant support for the proposition that the President could, in some circumstances, engage in domestic surveillance relying solely on inherent executive authority. The combination of pre-FISA

---

[75] Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified at 50 U.S.C. § 1881a *et seq.*). Section 1881a allows for the issuance of a court order upon the joint authorization of the Attorney General and Director of National Intelligence targeting "persons reasonably believed to be located outside the United States to acquire foreign intelligence information" for a period of up to one year. 50 U.S.C. § 1881a(a).

[76] Bazan & Elsea, *supra* note 70, at 44.

[77] *Id.*

Circuit Court cases upholding this authority and the dicta from *In re Sealed Case*[78] likely would be enough support.

This authority would be even stronger if the President is confronted with the need to protect the nation against an attack, bringing the *Prize Cases'* authorities and duties into play.[79] As a result, the combination of the President's apparent authority to conduct foreign intelligence surveillance noted in the previous paragraph, combined with the prospect of a *Prize Cases* theory of repelling an actual attack on the nation would place the President in a very strong position to act unilaterally. This would be subject to one caveat—what constitutes an attack on the nation in cyberspace? Certainly, a cyberattack threatening to cause a meltdown in a nuclear power plant would qualify, and probably also cyberattacks on critical infrastructure, such as water, electricity, or the transportation grid. But the salami can always be sliced thinner, and closer cases can be readily identified: What about attacks on the electoral process? Ransomware attacks on other critical infrastructure? Foreign misinformation campaigns? Denial of service attacks on the banking systems?

Recall that our original scenario based on SolarWinds best resembled an espionage campaign. An espionage attack is more likely to implicate foreign intelligence concerns—thus bringing it within the FISA framework—and not raise significant concern about a potential attack on the nation, which would more directly implicate Presidential authorities. Another major complicating factor is that it is very difficult to determine what shape an attack might take when an adversary obtains illicit access to a system.[80]

---

[78] *See In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (noting "the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance").

[79] The Prize Cases, 67 U.S. 635, 668 (1862) ("If a war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force.").

[80] *See* Bruce Schneier, *There's No Real Difference Between Online Espionage and Online Attack*, ATLANTIC (Mar. 10, 2014), https://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/ [https://perma.cc/9Q6S-NTG9] ("[F]rom the point of view of the object of an attack, [Computer Network Exploitation] and [Computer Network Attack] look the same as each other, except for the end result.").

Such access could be mere reconnaissance, or a foothold for unspecified future actions, or an opportunity to create a jumping off point to access another system (or even to engage in a supply chain attack like SolarWinds), or espionage.[81] Even worse, such access could quickly result in much more serious outcomes, such as "bricking" a system (e.g., rendering a computer system permanently inoperable) or encrypting the contents of a system via ransomware. Most seriously, access could result in a significant adverse physical effect, such as a power outage, particularly if a critical infrastructure node is compromised. Despite this wide range of possibilities, it is very difficult to discern a cyber attacker's ultimate objective.

As a result, there is likely a quantum of inherent executive authority to act outside of a FISA context against foreign adversaries in U.S. cyberspace. However, as the constitutional discussion makes clear, the extent of this authority is murky and ill-defined on several different fronts. Making matters worse, Congress appears to have intended to substantially restrict Presidential authority through FISA, preemptively outlining the exclusive legal framework for domestic national security electronic surveillance with civil and criminal penalties in store for members of the executive branch who operate outside the law. The executive branch is left to operate in the *Youngstown Steel* "Lowest Ebb" category, with jail and/or civil liability as a possible outcome if the courts disagree with the executive branch's actions. Much like the "gray zones" in international law, where foreign adversaries take advantage of legal ambiguity to gain an advantage,[82] there is a gray zone in U.S. domestic law, which adversaries are similarly exploiting.

This issue is too important to leave to murkiness, particularly when these problems will likely arise and need to be addressed in the context of an ongoing cyberattack—a serious threat which requires a concrete and efficient plan to combat. In such instances, circumspection and detailed analysis of the potential pitfalls are going to be difficult—instead, there will be pressure for immediate action. Just as Congress acted in varying degrees of cooperation with the President in establishing procedure for criminal wiretap (in

---

[81] *See id.*
[82] Schmitt, *supra* note 6.

response to *Katz*), and a procedure for foreign intelligence surveillance (in response to *Keith* and the Church Commission report, and adjusted in the aftermath of the September 11 attacks), so too Congress and the President should work together to create a framework for a national security response to foreign cyberattacks being routed through U.S. cyberspace to evade detection. There are too many sensitive policy issues at play to not act, and the nature of cyberattacks places them in a different category than electronic surveillance. While the executive branch has historically been hesitant to commit to statutory frameworks that channel and define the interplay between the political branches (e.g., the War Powers Resolution), the executive branch would benefit from increased clarity in this instance. In addition, private entities' concerns about a federal government presence on their networks could also be addressed within the statute, possibly increasing the likelihood of private entities' cooperation with federal agencies responding to cyberattacks.

V. CONCLUSION: THE NEED FOR A CYBER DOMESTIC AUTHORITIES STATUTE

The Terrorist Surveillance Program presented a slightly different problem than the one discussed in this Article. In the case of domestically-routed cyberattacks, claims of inherent executive authority to justify domestic operations against foreign cyberattacks are likely to fare better than the claims asserted in the Terrorist Surveillance Program. The extensions of cyber authorities in recent National Defense Authorization Acts suggests that Congress is keen to give U.S. Cyber Command the authorities it needs to counter foreign adversaries' cyber operations.[83] As a result, the mere identification of this issue in General Nakasone's testimony to Congress may result in some congressional action.

For several reasons, it is not advisable to develop a statutory framework within the existing FISA. First, despite the fact that the U.S. Cyber Command Commanding General is dual-hatted as the Director of the NSA, U.S. Cyber Command is a military command distinct from the Intelligence Community, and further blurring of

[83] *See* Chesney, *supra* note 8, at 1.

Title 50[84] (intelligence) authorities and legal requirements with Title 10[85] (military) authorities would likely be counterproductive.[86] Further, the FISA framework itself has become very controversial, particularly with respect to the recent concerns regarding FISA surveillance and potential missteps which occurred during the surveillance of members of the Trump campaign in 2016.[87] Amending FISA to allow for domestic cyber operations is likely to bring the existing FISA baggage and limit the possibility that such a legal framework would be successfully enacted. In addition, the considerations and processes needed to enable effective government responses while limiting intrusion on privacy are likely to significantly vary from the FISA framework.

When examining the parameters of what such a statute would look like, a number of considerations should be addressed. Specifically:

1. *Legal Threshold for Action*. This threshold should be considered both in terms of burden of proof and standard of proof, both of which are relatively low in the context of FISA. Under FISA, the required burden of proof is probable cause, and the required standard of proof is whether a person is a foreign power or an agent of a foreign power.[88] The political branches may want to consider whether probable cause is the appropriate threshold here. In the FISA context, the concern is the incidental collection of U.S. persons' conversations. In the cyber domain, the prospect of breaching U.S. cyberspace contains the potential for a much more severe infringement of privacy interests and may warrant a higher

---

[84] 50 U.S.C. §§ 1–4852.

[85] 10 U.S.C. §§ 1–18506.

[86] As an illustration, Robert Chesney has written on the controversy over whether U.S. Cyber Command cyber operations were classified under Title 50 and the Covert Action Statute or instead constituted "traditional military activities" governed by Title 10 authorities. *See* Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE (July 26, 2018, 2:07 PM), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa [https://perma.cc/BBP5-SZPU]. This controversy restricted U.S. Cyber Command's ability to engage in cyber operations and resulted in congressional action to clarify that cyber operations were traditional military activities. *Id.*

[87] *See* Horowitz, *supra* note 21, at 5–7.

[88] 50 U.S.C. § 1805(a).

level of certainty. Second, the seriousness of the prospective cyberattack that triggers these heightened authorities should be specified. A cyberattack conducted for espionage purposes might continue to fall under the FISA rules. A cyberattack with relatively minor national impacts—such as a denial-of-service attack against a bank or a ransomware attack on a private organization not tied to critical infrastructure—would likely not qualify under this proposed statutory scheme.

2. *Foreign Power Nexus*. Another significant issue for resolution is the nexus between the individual responsible for the cyberattack in question and a foreign power. Notwithstanding significant issues related to attribution of a cyberattack, the "who" behind the attack may require different levels of approval, burdens, and standards of proof. On the one hand, much like the possibility of a "lone wolf" terrorist attacker,[89] a single individual (or group of individuals) unaffiliated with a foreign government or terrorist organization, can create substantial harm. A similar "lone wolf" provision may be advisable. On the other hand, lower burdens and standards of proof may be appropriate in instances of action by a foreign power or agent of a foreign power (particularly agents of foreign powers who are not U.S. persons). In such cases, the President's authority would be at its apogee, implicating the President's foreign affairs authority[90] and duty to defend the nation from attack.[91]

3. *Differentiation between Types of Domestic Cyberspace*. Another consideration might be the type of domestic cyberspace that the foreign adversary is breaching, and to which U.S. government or military personnel might need access. For example, lesser concerns might be raised in systems engaged in traditional functions of "dialing, routing, addressing, and signaling" (e.g., routers or switches), which are important to keep the internet traffic moving, but which do not raise the same potential for access to information

---

[89] The term "lone wolf" is used to describe individuals committing terrorism on an individual basis without an affiliation with a foreign power or terrorist organization. *See* DYCUS ET AL., *supra* note 20, at 593.

[90] *See* United States v. Curtiss-Wright Exp. Co., 299 U.S. 304, 319 (1936) ("The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." (quoting 6 ANNALS OF CONG. 613 (1800)).

[91] The Prize Cases, 67 U.S. 635, 668 (1862).

to which a reasonable expectation of privacy might extend. By contrast, if U.S. government personnel need to access a U.S. person's cloud account or personal email to interdict an attack, then the privacy interests are significantly greater. Higher burdens and standards of proof may be warranted in these instances.

4. *Notice to Affected Parties*. At some point, U.S. persons whose cyber "property" was breached by U.S. government personnel to interdict a foreign attack should receive notice of this action. Notice prior to or contemporaneous with such a breach is inadvisable due to the prospect of tipping off the foreign intruder, whether intentionally or inadvertently. In addition, there is also the possibility of private organizations not cooperating with or actively opposing prospective government operations on its networks. As a result, policymakers should consider a delayed notification requirement in specified situations.

5. *Government Liability for Damage*. The prospect of allowing an affected organization to make a claim against the U.S. government for damages caused by nonconsensual access to their systems has countervailing concerns. On the one hand, the organization may be at fault for allowing foreign nation-state access to their system in the first place, particularly if it was not following best practices for cybersecurity. To allow for claims in such instances creates the potential for a moral hazard, potentially increasing the incentive for organizations to be lax on their cybersecurity practices. On the other hand, even the best and most secure systems can be breached due to no fault on the part of the organization. FireEye, one of the best cybersecurity companies in the world, was hacked by the supply chain attack that followed the SolarWinds breach.[92] A middle ground might be to authorize claims against the government if the affected organization can show that they complied with their industry's best cybersecurity practices.

6. *Designate Government Agency Responsibilities*. Another possibility to consider is whether U.S. Cyber Command is the

---

[92] David E. Sanger & Nicole Perloth, *FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State*, N.Y. TIMES (Dec. 8, 2020), https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html [https://perma.cc/5NBJ-USFP].

appropriate organization to operate within domestic cyberspace. The increased role of U.S. Cyber Command in responding to non-military threats such as botnet takedowns has been subject to criticism.[93] In fact, under Presidential Policy Directive 41, the general paradigm is that the Department of Homeland Security and Department of Justice are responsible for responding to domestic cyberspace incidents.[94] It might be advisable to provide the authorities at the Department of Homeland Security or the Department of Justice with the ability to engage in these domestic cyber operations described in this Article. However, this change would require a significant increase in the resourcing necessary for those organizations to be able to counter the sophisticated attacks that nation-state-level actors can conduct. Even if non-military agencies are viewed to be the proper responders, the law would still need to be clarified as to the applicability of FISA, as well as the circumstances under which authority is granted to operate nonconsensually in domestic cyberspace.

While the exploitation of gray zones in international law will be difficult to address due to the slow-changing nature of international law, the domestic legal gray zone identified in this Article can be addressed by Congress and should be remedied. Now that this gap has been identified in public Congressional testimony, foreign adversaries will increasingly take advantage of this gray zone, free of U.S. Cyber Command's ability to see—let alone counter—such attacks. Instead of relying on the murky boundary between the constitutional authorities of the political branches and a Vietnam-era law which did not even consider the possibility of devastating cyberattacks, there should be clear lines of authority and procedure for responding to foreign nation-state cyberattacks on the homeland.

---

[93] *See e.g.,* Jason Healy, *When Should U.S. Cyber Command Take Down Criminal Botnets?*, LAWFARE (Apr. 26, 2021, 2:51 PM), https://www.lawfareblog.com/when-should-us-cyber-command-take-down-criminal-botnets [https://perma.cc/LJ4D-HPFT].

[94] *Presidential Policy Directive 41—United States Cyber Incident Coordination*, WHITE HOUSE PRESS SEC'Y (July 26, 2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident [https://perma.cc/SGK9-QW8Q].