The Heritage Foundation

BACKGROUNDER
No. 3670 | NOVEMBER 10, 2021
CENTER FOR TECHNOLOGY POLICY

For Cybersecurity, the Best Defense Is a Good Offense

Dustin Carmack and Michael Ellis

KEY TAKEAWAYS

As foreign-sponsored cyberattacks increase in scale and frequency, the Biden Administration's response strategy is unclear.

Diplomatic pressure, economic sanctions, and criminal prosecutions are insufficient to deter adversaries.

The Administration should use offensive cyber operations to degrade adversaries' capabilities and create credible deterrence.

Cyberattacks against U.S. networks continue to grow in scale and number. Recently, a series of high-profile "ransomware attacks," where criminal groups shut down networks until they receive payment, have gained national attention. This year alone, ransomware attacks disabled the pipeline carrying nearly half of the gasoline on the East Coast, shut down one of the country's largest meatpacking companies, and caused a large-scale IT firm to deliver malicious software to its customers, compromising the networks of thousands of businesses.[1] These criminal groups predominantly operate from Eastern Europe, Russia, and the former Soviet Union, and other ransomware and cyber threats emanate from China, North Korea, and Iran.[2] At the same time, broader exploitation and

espionage campaigns, such as the SolarWinds and the Hafnium Microsoft Exchange intrusions,[3] have continued to wreak havoc on the U.S. public and private sectors.

Much of the discussion in the Biden Administration, on Capitol Hill, and throughout corporate boardrooms has revolved around improving U.S. cyber defenses. There is plenty of work to do on that front. Government and the private sector alike should improve cybersecurity awareness of their employees, employ multifactor authentication and zero-trust architecture, and improve public–private partnerships and information sharing. Congress, for its part, should impose breach notification requirements[4] and help establish additional baseline cybersecurity protocols for critical infrastructure systems. All these steps are necessary, but they will not be sufficient. Cyber defenders must stop every possible attack, while attackers only need to find a single vulnerability to exploit. Given the breadth of U.S. critical infrastructure—including more than 10,000 power plants,[5] 153,000 public drinking water systems, 16,000 publicly owned wastewater treatment facilities,[6] and 6,000 health care facilities[7]—a determined attacker will always find a way through network defenses.

Current Efforts Are Insufficient

The Biden Administration has attempted to use diplomacy, sanctions, and law enforcement actions to fight ransomware. This strategy is not new, and it is unlikely to succeed. Adversaries such as Russia are indifferent to sternly worded press releases and shrug off diplomatic efforts. In June, President Biden warned Russian President Vladimir Putin that attacks on 16 U.S. critical infrastructure sectors were off-limits;[8] it took only a few weeks for Russian hackers to launch another round of ransomware attacks.[9] More recently, Russia's foreign intelligence service, the SVR, appears to have continued an espionage campaign against thousands of U.S. government, corporate, and nonprofit networks.[10]

Economic sanctions can also be important tools, but for many nation-states and criminals, they have reached the limits of their effectiveness. Many adversaries have reduced their reliance on the U.S. financial system,[11] and many of the logical targets have already been targeted. Another layer of sanctions on Russian intelligence services, for example, is unlikely to change Moscow's decision-making.[12]

Targeted sanctions also take a significant amount of time to develop. For example, the Department of the Treasury designated the North Korean state-sponsored "Lazarus Group" for sanctions in September 2019—nearly

two years after the group launched the WannaCry 2.0 ransomware attack and five years after it hacked the Sony Pictures film studio.[13] There must be evidence of the sanctions target's nefarious behavior that could be used in a court proceeding if the target challenges the designation. Thus, the U.S. Intelligence Community is frequently hesitant to allow its best intelligence sources and methods to be used to support a designation. As a result, sanctions are too little, too late to deter cyberattacks.

Law enforcement efforts are similarly unlikely to deter cyberattacks. Attackers should, of course, be prosecuted when possible. Cybercrime investigations, however, often require cooperation from foreign adversaries who are unlikely to provide it. And even when there is enough evidence to indict cybercriminals, government-sponsored hackers can escape justice simply by remaining in their home countries, safely out of the reach of U.S. law enforcement. The Department of Justice has brought charges against numerous Chinese and Russian hackers over the past decade, but only a token few have ever appeared inside American courtrooms.[14]

Some commentators have proposed bolstering private-sector capabilities for "active cyber defense." This approach, sometimes called "hacking back," would encourage the U.S. private sector to go beyond protective software, firewalls, and other passive screening methods and deceive, identify, disable, or otherwise retaliate against hackers.[15] Private-sector hacking-back presents various challenges under both domestic and international law, especially the prohibition in the 1986 Computer Fraud and Abuse Act (CFAA) on accessing a computer system without authorization. Uncoordinated actions by the private sector also risk interfering with U.S. foreign policy interests and ongoing U.S. military and intelligence operations. Even so, recently some U.S. companies have attempted to work within the scope of CFAA to take action against cyber attackers.[16]

In short, although U.S. diplomats, sanctions enforcement officials, prosecutors, and law enforcement agents are engaged in noble efforts, their actions alone will not deter the most significant cyberattacks. The United States should continue to use these diplomatic, economic, and investigative tools, but unless its adversaries pay a price, cyberattacks will only continue to escalate.[17]

Trump Streamlined U.S. Offensive Cyber Operations

Given the insufficiency of other policy tools, the U.S. government should increase its use of offensive cyber operations, sometimes called cyber effects operations, to degrade adversaries' capabilities and create strategic

deterrence.[18] Under the Obama Administration's policies, offensive cyber operations were destined for failure. President Obama's 2012 Presidential Policy Directive 20 (PPD-20) stressed that the U.S. government would "undertake the least action necessary to mitigate threats" and expressly prioritized "network defense and law enforcement as preferred courses of action."[19] Before the U.S. government could carry out an offensive cyber operation, PPD-20 required an interagency policy coordination process chaired by the National Security Council—at least three levels of meetings, allowing "anyone to stop the process at any point." As a result, "much of the authority [was] held at the presidential level,"[20] making the PPD-20 process too "slow and cumbersome" to enable timely or meaningful cyber operations.[21]

President Trump's replacement directive, National Security Presidential Memorandum (NSPM)-13, established a process to delegate authorities to operating agencies, including to the Department of Defense, to conduct "time-sensitive military operations in cyberspace."[22] Although much of the substance of the order and operations remains classified, the U.S. government has publicly disclosed a few operations that occurred under the NSPM-13 framework. General Paul Nakasone, commander of U.S. Cyber Command (USCYBERCOM) and director of the National Security Agency (NSA), has described efforts to "Defend Forward" and maintain "persistent engagement" against adversaries.[23] In March 2021, Nakasone testified that USCYBERCOM had conducted "more than two dozen operations to get ahead of foreign threats before they interfered or influenced our elections in 2020."[24] This number included 11 "hunt-forward" operations, where USCYBERCOM partnered with allies to counter or halt malicious cyber activity, in nine different countries as part of election-security efforts.[25] In addition, an October 2020 USCYBERCOM operation disrupted the Russia-based Trickbot botnet, a malicious malware that had previously damaged a health care provider and was viewed as a possible threat to the 2020 election cycle.[26]

Congress has also helped clarify the legal landscape for offensive cyber operations. The Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) recommended that the "United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests"[27] and provided statutory authorization for certain offensive cyber operations, including those that would "significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government)."[28] The FY2019 NDAA also settled a long-running

question as to whether a cyber operation constitutes covert action if it obscures U.S. involvement in the operation.[29] By affirmatively stating that such operations are "traditional military activities," the NDAA opened the door for deniable cyber operations without a covert action finding.[30]

Foreign Governments Engage in Offensive Cyber Operations

When the recission of PPD-20 was reported, many commentators feared hostile reactions from allies and a cycle of escalation with adversaries.[31] Neither fear has been borne out. Worries of offensive operations impairing intelligence-collection efforts have also not come to fruition. In fact, many allies have sought U.S. leadership and cooperation to deter mutual adversaries. The United Kingdom, for instance, took a forward-leaning view of international law that permitted it to conduct offensive cyber operations well before the shift in U.S. policy.[32] And last year, the U.K. established a National Cyber Force, a unified command staffed by personnel from the Secret Intelligence Service (MI6), the Government Communications Headquarters (GCHQ), and the Ministry of Defense to conduct offensive cyber operations.[33] GCHQ Director Sir Jeremy Fleming recently stated the desire and capability to deploy civilian personnel from the National Cyber Force to "go after" ransomware gangs, and where groups were outside the reach of prosecutors and police, they would face "the pointy end of the spear."[34]

China, Russia, and other adversaries regularly engage in offensive cyber operations. The Office of the Director of National Intelligence's 2021 Annual Threat Assessment noted that Russian cyber operations "target critical infrastructure, including underwater cables and industrial control systems" and that Russia considers "cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[35] Similarly, China is "a prolific and effective cyber-espionage threat" that "possesses substantial cyber-attack capabilities" and can "launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[36] Rather than cede the debate over international norms to Russia and China through inaction, the United States should join its allies to create the norms it desires through state practice.[37]

The Biden Administration's Approach

So far, it is not clear what approach the Biden Administration has taken with respect to offensive cyber operations. Earlier this year, following the

SolarWinds intrusion, as well as a spate of ransomware attacks emanating from Russian territory, news reports indicated the Biden Administration prepared a "series of clandestine actions across Russian networks that are intended to be evident to President Vladimir V. Putin and his intelligence services and military but not to the wider world."[38] And according to recent press reports, a multi-country operation successfully forced REvil, a Russia-based ransomware group, offline.[39] REvil was involved in several prominent cyberattacks this year, including the Colonial Pipeline and JBS meatpacking attacks.

News reports also indicate National Security Advisor Jake Sullivan—who has no legal authority to direct departments or agencies—reportedly issued guidance to notify the National Security Council (NSC) of large-scale operations and allow for a review and adjustment of those operations through the policy coordination channels.[40] As has been reported for other critical national security issues,[41] this guidance may signal a return to the Obama Administration's byzantine procedural requirements that prevent a timely response to cyber threats.[42]

Recommendations

Congress should:

- **Provide additional statutory authorities to USCYBERCOM.** Congress should further clarify that the FY 2019 NDAA authorities extend beyond election interference and extend statutory authorization to a wide range of cyber operations that can deter or degrade adversaries' ability to attack U.S. critical infrastructure. Although the President has constitutional authority to carry out offensive cyber operations,[43] additional statutory authority will help bolster the President's power[44] and send a clear signal to U.S. allies and adversaries of political support for offensive cyber operations.

The Administration should:

- **Continue to delegate authority to operating agencies.** Rather than restoring the Obama Administration's paralysis by analysis, President Biden and his NSC should retain the former Administration's approach and drive operating agencies to establish deterrence below the threshold of an armed conflict. Siloed infighting among competing agencies and discussions of intelligence-collection gains

and loss analysis should not be allowed to dominate considerations of proper and necessary responses. Additionally, policymakers should be clear-eyed on the time, resources, and potential technical capability loss needed to plan and execute offensive cyber operations as well as the level of their impact and time for an adversary to reconstitute. This framework should rely on metrics to properly evaluate risk and reward as well as the effect of actions and their long-term impacts.

- **Publicly announce the threshold for offensive cyber operations.** Just as the U.S. nuclear "declaratory" policy helps establish deterrence,[45] a publicly announced policy on U.S. offensive cyber operations will force adversaries to consider the likely U.S. reaction before they launch cyberattacks. Furthermore, a clear declaratory policy can help the U.S. government understand, attribute, and prioritize actions against nation-state cyber actors, even when they enter a complicit "gray-zone" or "blind eye" by work with criminal actors. A publicly announced threshold for offensive cyber operations need not exclude more traditional tools—such as diplomacy, sanctions, and prosecutions—when adversaries' actions fall short of cyber redlines.

- **Disclose the results of cyber operations.** The U.S. government should also proactively disclose more of its offensive cyber operations. Deterrence works only if adversaries understand—and fear—U.S. capabilities. Just as the U.S. military ensures that adversaries understand the consequences of crossing U.S. redlines, limited disclosures of successful U.S. cyber operations may cause prospective cyber attackers to reconsider. For example, the press attributed the recent success against REvil to "private sector cyber experts working with the United States and one former official," but there was no official U.S. government statement on the operation.[46] If executed properly, such disclosures would also be unlikely to jeopardize USCYBERCOM's techniques or intelligence sources and methods.

- **Identify additional domestic law enforcement authorities and capabilities.** The Department of Justice, including the Federal Bureau of Investigation, should review additional capabilities or authorities needed to target and disrupt known ransomware and, when possible, recover illicit gains from criminals' financial networks.

The Administration and Congress should:

- **Explore further structural changes to interagency cyber operations and collaboration.** During the Obama Administration, then-Secretary of Defense Robert Gates proposed appointing a Department of Homeland Security (DHS) official to concurrently serve as a deputy director of the NSA with the power to task NSA resources under DHS authorities.[47] This proposal would have brought the vast and well-established capabilities of the NSA to bear against cyberattacks originating within the United States while following the more stringent privacy and civil liberties regulations of DHS. Gates believes DHS possesses many of the authorities to protect the homeland from cyber threats, but it has little capability to exercise those authorities without duplicating the substantial human and technical resources of the NSA. Despite allegedly receiving the approval of President Obama, this proposal "came to naught" because of "bureaucratic foot-dragging and resistance."[48] Bureaucracy and conflicting messages should not slow down the U.S. approach to necessary cyber responses.

- **Consider ending the NSA and USCYBERCOM "dual-hat" relationship.** Currently, the NSA director is a four-star military officer who serves concurrently as the commander of USCYBERCOM. This arrangement was necessary in the infancy of USCYBERCOM, when it relied on the NSA for its capabilities, but there has long been an intent to end the relationship once USCYBERCOM reaches maturity. President Trump elevated USCYBERCOM to an independent unified command in 2018, and the committee-passed Intelligence Authorization Act for Fiscal Year 2022 sets a road map for the termination of the dual-hat arrangement.[49] Congress should continue its oversight efforts while working in conjunction with the Administration, NSA, and USCYBERCOM to evaluate whether the dual-hat relationship should be ended.[50] The dual-hat role is an enormous job for a single person, and a separate seat at the table for USCYBERCOM would help prevent intelligence gain-loss considerations from dominating discussions of offensive cyber operations. Separating the two organizations, may, however, lead to overlapping capabilities. If the dual-hat arrangement ends, there is little reason why the director of the NSA—like the directors of the National Geospatial-Intelligence Agency and the National Reconnaissance Office—could not be a civilian official.

Conclusion

In short, although the Administration should continue to make use of diplomacy, sanctions, and law enforcement actions to reduce the threat of cyberattacks, these efforts are not sufficient. Similarly, efforts to improve the cybersecurity of U.S. critical infrastructure are likely to fall short in the face of attacks sponsored by nation-states. The Administration and Congress should instead continue and expand President Trump's approach by using offensive cyber operations to degrade adversaries' capabilities and create credible deterrence. The Administration should disclose more information about these operations to discourage adversaries from attacking, and Congress should consider structural changes to improve the efficiency and effectiveness of U.S. offensive cyber operations.

Dustin Carmack is Research Fellow in Technology Policy in the Center for Technology Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. **Michael Ellis** is Visiting Fellow for Technology and Law in the Edwin J. Meese Center III for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation.

Endnotes

1. Matt Stieb, "What's Driving the Surge in Ransomware Attacks?," *Intelligencer*, September 7, 2021, https://nymag.com/intelligencer/article/ransomware-attacks-2021.html (accessed October 20, 2021).
2. Between July 2020 and June 2021, Microsoft attributed 58 percent of all cyberattacks to Russia while noting that China-based actors carry out more robust operations targeting critical infrastructure sectors. Tom Burt, "Russian Cyberattacks Pose Greater Risk to Governments and Other Insights from Our Annual Report," *Microsoft on the Issues*, October 7, 2021, https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/ (accessed October 20, 2021). See also Microsoft, *Digital Defense Report*, October 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi (accessed October 20, 2021).
3. Dustin Volz and Aruna Viswanatha, "Biden Administration Blames Hackers Tied to China for Microsoft Cyberattack Spree," *Wall Street Journal*, July 19, 2021, https://www.wsj.com/articles/biden-administration-to-blame-hackers-tied-to-china-for-microsoft-cyberattack-spree-11626692401 (accessed October 21, 2021).
4. Michael Ellis, "Time for a National Cyber Incident Disclosure Requirement," Heritage Foundation *Issue Brief* No. 6081, May 26, 2021, https://www.heritage.org/technology/report/time-national-cyber-incident-disclosure-requirement.
5. U.S. Energy Information Administration, "How Many Power Plants Are There in the United States?," November 18, 2020, https://www.eia.gov/tools/faqs/faq.php?id=65&t=2#:~:text=As%20of%20December%2031%2C%202019,least%201%20megawatt%20(MW) (accessed October 18, 2021).
6. Cybersecurity and Infrastructure Security Agency, "Water and Wastewater Systems Sector," https://www.cisa.gov/water-and-wastewater-systems-sector (accessed October 18, 2021).
7. American Hospital Association, "Fast Facts on U.S. Hospitals, 2021," January 2021, https://www.aha.org/statistics/fast-facts-us-hospitals (accessed October 18, 2021).
8. Vladimir Soldatkin and Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off Limits,'" Reuters, June 16, 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/ (accessed October 19, 2021).
9. Dustin Volz and Robert McMillan, "Software Firm at Center of Ransomware Attack Was Warned of Cyber Flaw in April," *Wall Street Journal*, July 7, 2021, https://www.wsj.com/articles/software-firm-at-center-of-ransomware-attack-was-warned-of-cyber-flaw-in-april-11625673291?mod=article_inline (accessed October 19, 2021).
10. David E. Sanger, "Ignoring Sanctions, Russia Renews Broad Cybersurveillance Operation," *New York Times*, October 25, 2021, https://www.nytimes.com/2021/10/25/us/politics/russia-cybersurveillance-biden.html (accessed October 26, 2021).
11. See U.S. Department of the Treasury, "The Treasury 2021 Sanctions Review," p. 2, https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf (accessed October 14, 2021).
12. Russia's Federal Security Service and Main Intelligence Directorate, for example, were sanctioned in 2016 for interfering in U.S. elections, in 2018 for malicious cyber activities, and in 2021 for activities related to the proliferation of weapons of mass destruction. See news release, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," U.S. Department of the Treasury, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127 (accessed October 20, 2021).
13. News release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," U.S. Department of the Treasury, September 13, 2019, https://home.treasury.gov/news/press-releases/sm774 (accessed October 20, 2021).
14. Between 2013 and May 2019, the Department of Justice brought charges against 93 foreign nationals for state-linked hacking activity and foreign online influence operations. Under the Trump Administration, that pace quickened—16 of the 24 cases were charged after January 2017 to May 2019. See Garrett Hinck and Tim Maurer, "What's the Point of Charging Foreign State-Linked Hackers?," *Lawfare*, May 24, 2019, https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers (accessed November 8, 2021) and https://docs.google.com/document/d/1sipdsjWkDlT9xmbbQQ3wKfanmETS-N_4VD60H2ssfgQ/edit (accessed October 18, 2021); Jack Goldsmith and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," *Lawfare*, December 28, 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy (accessed October 18, 2021); and Robert D. Williams, "America's Hopelessly Anemic Response to One of the Largest Personal-Data Breaches Ever," *The Atlantic*, February 12, 2020, https://www.theatlantic.com/ideas/archive/2020/02/whats-behind-the-indictment-of-the-equifax-hackers/606466/ (accessed October 18, 2021).
15. Paul Rosenzweig, Steven P. Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Heritage Foundation *Backgrounder* No. 3188, May 5, 2017, https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense.
16. James Rundle, "Cyber Private Eyes Go After Hackers, Without Counterattacking," *Wall Street Journal*, October 18, 2021, https://www.wsj.com/articles/cyber-private-eyes-go-after-hackers-without-counterattacking-11634549400 (accessed October 22, 2021).
17. David Inserra, "Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace," Heritage Foundation *Backgrounder* No. 3223, July 14, 2017, https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors.

18. The Department of Defense defines *offensive cyber operations* as "missions intended to project power in and through cyberspace." See Joint Publication 3-12, "Cyberspace Operations," June 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed October 20, 2021).
19. Office of the White House Press Secretary, "Presidential Policy Directive 20 [Fact Sheet]," Homeland Security Digital Library, January 2013, https://www.hsdl.org/?abstract&did=814897 (accessed October 20, 2021).
20. Sydney J. Freedberg Jr., "Trump Eases Cyber Ops, but Safeguards Remain: Joint Staff," *Breaking Defense*, September 17, 2018, https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/ (accessed October 20, 2021).
21. Gary P. Corn, "National Security Decision-Making in the Age of Technology: Delivering Outcomes On Time and On Target," *Journal of National Security Law and Policy*, Vol. 12, No. 61 (November 2021), p. 69, https://jnslp.com/wp-content/uploads/2021/09/National-Security-Decision-Making-in-the-Age-of-Technology.pdf (accessed October 20, 2021).
22. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," remarks by Paul C. Ney Jr., U.S. Department of Defense, March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ (accessed October 21, 2021).
23. Brad D. Williams, "CYBERCOM Plays 'Key Role' as SolarWinds Unfolds: Gen. Nakasone," *Breaking Defense*, March 5, 2021, https://breakingdefense.com/2021/03/cybercom-plays-key-role-as-solarwinds-unfolds-gen-nakasone/ (accessed October 20, 2021), and JFQ, "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, Vol. 92 (January/February/March 2019), p. 4-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf (accessed October 20, 2021).
24. Christopher P. Maier, General Richard D. Clarke, and General Paul M. Nakasone, "To Receive Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2022 and the Future Years Defense Program," testimony before the Committee on Armed Services, U.S. Senate, March 25, 2021, https://www.armed-services.senate.gov/imo/media/doc/21-17_03-25-20212.pdf (accessed October 20, 2021).
25. Olivia Gazis, "U.S. Launched 'More Than 2 Dozen' Cyber Operations to Protect Election, Top Official Says," CBS News, March 25, 2021, https://www.cbsnews.com/news/election-interference-us-cyber-command-nsa-nakasone/ (accessed October 20, 2021).
26. Ellen Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html (accessed October 20, 2021).
27. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115–232.
28. Ibid.
29. Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare*, July 26, 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa (accessed October 20, 2021).
30. Robert Chesney, "Covert Military Information Operations and the New NDAA: The Law of the Gray Zone Evolves," *Lawfare*, December 10, 2019, https://www.lawfareblog.com/covert-military-information-operations-and-new-ndaa-law-gray-zone-evolves (accessed October 20, 2021).
31. See, for example, Mack DeGeurin, "U.S. Silently Enters New Age of Cyberwarfare," *New York Intelligencer*, September 11, 2018, https://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html (accessed October 20, 2021), and Herb Lin and Max Smeets, "What Is Absent from the U.S. Cyber Command 'Vision,'" *Lawfare*, May 3, 2018, https://www.lawfareblog.com/what-absent-us-cyber-command-vision (accessed October 20, 2021).
32. U.K. Attorney General's Office, "Cyber and International Law in the 21st Century," May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed October 20, 2021).
33. Ministry of Defence, Cabinet Office, The Rt Hon Steve Barclay MP, and The Rt Hon Ben Wallace MP, "Permanent Location of National Cyber Force Campus Announced," Gov.uk, October 4, 2021, https://www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced (accessed October 21, 2021).
34. Helen Warrell, "GCHQ to Use New Cyber Force to Hunt Ransomware Gangs," *Financial Times*, October 25, 2021, https://www.ft.com/content/2e391872-428d-44bf-8910-23f123c8aaa6 (accessed October 25, 2021).
35. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf (accessed October 21, 2021).
36. Ibid.
37. David Ignatius, "How Russia and China Are Attempting to Rewrite Cyberworld Order," *The Washington Post*, March 30, 2021, https://www.washingtonpost.com/opinions/global-opinions/how-russia-and-china-are-attempting-to-rewrite-cyberworld-order/2021/03/30/16030226-9190-11eb-a74e-1f4cf89fd948_story.html (accessed October 20, 2021).
38. David E. Sanger, Julian E. Barnes, and Nicole Perlroth, "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China," *New York Times*, September 9, 2021, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html (accessed October 21, 2021).

39. Joseph Menn and Christopher Bing, "EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline," Reuters, October 21, 2021, https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/ (accessed October 22, 2021).
40. Ibid.
41. Charlie Savage and Eric Schmitt, "Biden Secretly Limits Counterterrorism Drone Strikes Away from War Zones," *New York Times*, March 3, 2021, https://www.nytimes.com/2021/03/03/us/politics/biden-drones.html (accessed October 20, 2021).
42. See, for example, Committee on Intelligence, U.S. Senate, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 116th Cong., 2nd. Sess., Vol. 3, minority views of Senators Risch, Rubio, Cotton, Cornyn, and Sasse, at p. 48, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf (accessed October 14, 2021).
43. Chesney, "The Law of Military Cyber Operations and the New NDAA."
44. See *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 636-37 (1952) (Jackson, J., concurring).
45. U.S. Department of Defense, *Nuclear Posture Review, February 2018*, 2018, p. 45, https://www.documentcloud.org/documents/4365530-2018-Nuclear-Posture-Review-Final-Report.html (accessed October 20, 2021).
46. Menn and Bing, "EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline."
47. Robert M. Gates, "The United States Has a Major Hole in Its Cyberdefense. Here's How to Fix It," *Washington Post*, March 28, 2021, https://www.washingtonpost.com/opinions/2021/03/28/united-states-has-major-hole-its-cyberdefense-heres-how-fix-it/ (accessed October 13, 2021).
48. Ibid.
49. Intelligence Authorization Act for Fiscal Year 2022, H.R. 5412, 117th Cong.
50. James Di Pane, "Should Cyber Command and the NSA Have Separate Leadership? How to Decide," Heritage Foundation *Backgrounder* No. 3403, May 2, 2019, https://www.heritage.org/defense/report/should-cyber-command-and-the-nsa-have-separate-leadership-how-decide.