The U.S. Playbook for Digital Warfare: Economic Sanctions, Criminal Prosecutions, and Diplomacy

William I. Friedman*

ABSTRACT

This article charts the emergence and maturation of the United States' cyber-related sanctions regime as a central pillar of twenty-first-century national security strategy. It traces the regime's origins to the U.S. response to North Korea's 2014 cyberattack on Sony Pictures Entertainment, arguing that this episode marked a doctrinal inflection point in the evolution of digital warfare. The Sony incident catalyzed the development of a proactive, whole-of-government architecture that integrates economic sanctions, criminal prosecutions, and diplomatic engagement in ways that complement, and increasingly operate in tandem with, the Department of Defense's Defend Forward *doctrine.*

Through case studies of North Korea, Russia, Iran, and China, the article demonstrates how sanctions designations and criminal indictments have become

* William I. Friedman served as Section Chief in the Policy Division of the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury (2024-2025) and as a federal prosecutor in the Money Laundering and Asset Recovery Section of the U.S. Department of Justice's Criminal Division (2018–2023), including a detail as a Special Assistant U.S. Attorney in the U.S. Attorney's Office for the Eastern District of Virginia (2020–2021). Before entering federal service, Mr. Friedman practiced as Special Counsel at Schulte Roth & Zabel LLP (2005–2012). He subsequently joined Sullivan & CromwellLLP where he practiced as a senior attorney (2012–2018). Earlier in his career, he worked in the New York Stock Exchange's Enforcement Division (2004-2005) and Market Surveillance Division (1996-2000), and clerked for Justice Bernard J. Fried in the Criminal Division of the Supreme Court of New York County (2001–2003).

Mr. Friedman is the author of *Starving the Bear; Sanctions, Power, and the Battle for Ukraine*, forthcoming in the *Annual Review of Banking & Financial Law* (Summer 2026). His earlier scholarship includes *The Fourteenth Amendment's Public/Private Distinction Among Securities Regulators in the U.S. Marketplace—Revisited* (*Annual Review of Banking Law*, 2004); *One Country, Two Systems: The Inherent Conflict Between China's Communist Politics and Capitalist Securities Market* (*Brooklyn Journal of International Law*, 2002); and *China's One Country, Two-System Paradigm Extends Itself Beyond the Mainland's Borders to the Southern Provincial Government of Hong Kong* (*Transnational Law & Policy*, 2001).

Mr. Friedman has also co-authored white papers on the Bank Secrecy Act of 1970, the USA PATRIOT Act of 2001, the Foreign Corrupt Practices Act of 1977 (as amended), the Export Administration Act, the International Emergency Economic Powers Act, the Trading with the Enemy Act, and the National Emergencies Act, while at Sullivan & Cromwell LLP and Schulte Roth & Zabel LLP. These works have been featured in the *Harvard Law School Forum on Corporate Governance*, the *Financial Fraud Law Report*, and other publications. He also co-authored regulatory guidance for The Clearing House Association, the Managed Funds Association, and the Securities Industry and Financial Markets Association, industry leading trade organizations representing the banking, securities, and asset-management sectors.

Mr. Friedman holds degrees from the University of Chicago (M.A., 2024), Georgetown University Law Center (LL.M., 2021), Brooklyn Law School (J.D., 2001), Baruch College/City University of New York, Zicklin School of Business (M.B.A., 1997), and Brandeis University (B.A., 1992).

mutually reinforcing tools for cost imposition, attribution, accountability, disruption, and norm-building. Although these measures do not necessarily produce deterrence in the strict sense of halting adversary cyber operations, they contribute to the broader foundations of cumulative cyber deterrence by raising costs, exposing malign actors, constraining illicit networks, and extending U.S. cyber statecraft beyond traditional military mechanisms.

The article situates these developments within the broader statutory and administrative framework governing presidential emergency powers, examining the executive orders and legislation that collectively authorize the Executive Branch to respond to foreign malicious cyber activity. Consistent with the 2025 National Security Strategy, it argues that sanctions and prosecutions now operate as core instruments of U.S. national power rather than episodic responses to discrete cyber incidents.

It further analyzes the deepening operational partnership among the Departments of the Treasury, Justice, and State, now a defining feature of the United States' modern integrated cyber governance model, and their role in shaping international norms of responsible state behavior in cyberspace. At the same time, it identifies emerging policy divergences under the second Trump Administration. Drawing on the Cyberspace Solarium Commission's 2025 Annual Report, it highlights the federal government's first measurable regression in cyber-governance capacity since 2019, revealing structural vulnerabilities in an architecture dependent on robust interagency coordination and sustained diplomatic engagement.

The article concludes that as cyber operations converge with artificial intelligence and other emerging technologies, preserving U.S. security, credibility, and global leadership will require an adaptive, fully integrated fusion of economic, legal, diplomatic, and military tools, supported by the institutional infrastructure necessary to employ them coherently and at scale. Together, they form a modernized playbook for digital statecraft that will be essential to meeting the strategic demands of the next decade.

I. INTRODUCTION

The 2014 cyberattack on Sony Pictures Entertainment ("SPE" or "Sony") by North Korean-sponsored hackers was far more than an assault on a private corporation; it marked a pivotal moment in the evolution of modern conflict, exposing the profound vulnerabilities of global enterprises to state-sponsored digital coercion, and signaling that cyberspace had become an arena for geopolitical competition. Triggered by the planned release of the satirical film *The Interview*, the unprecedented attack crippled Sony's operations, destroyed roughly 70 percent of its computer systems, and exposed vast quantities of proprietary and personally identifiable information, sending shockwaves throughout government and industry. As the Obama Administration confronted this crisis, it was forced to grapple

with unprecedented questions about the federal government's authority, strategic responsibility, and the proper scope of government intervention when a foreign government targets a private entity. These questions, in turn, forced policymakers to confront the broader implications such threats posed to U.S. national security, the constitutional framework governing the executive's emergency powers, and international legal norms regulating state behavior in cyberspace.

In the decade since the Sony attack, the United States has operated in an increasingly contested, volatile, and hostile digital environment. This environment has been shaped not only by the persistent threat of a catastrophic, high-impact cyberattack, but also by the gradual erosion of digital security caused by continuous foreign intrusions targeting industry, critical infrastructure, and democratic institutions. In an era of renewed great-power competition, both state and non-state actors, most prominently China, Russia, Iran, and North Korea, have exploited the gray zone of cyberspace to contest U.S. influence, undermine democratic institutions, steal sensitive commercial and personal data, disrupt critical infrastructure, and destabilize the liberal democratic rules based international order, all while remaining below the threshold of armed conflict.[1] This contested environment is now reflected at the highest level of U.S. strategy, as the 2025 National Security Strategy expressly situates cyber capabilities as central instruments of national power in long-term competition with peer adversaries.[2] Russia's interference in the 2016 presidential election[3] and China's 2015 theft of the personal information of more than 22 million people from the U.S. government's Office of Personnel Management[4] and 2017 theft of trade secrets and the

1. U.S. CYBERSPACE SOLARIUM COMM'N, 2020 US CYBERSPACE SOLARIUM COMMISSION REPORT 2 (2020), https://perma.cc/652F-EW8N [hereinafter 2020 CSC REPORT]; *see* JIWON MA, CSC 2.0: 2025 ANNUAL REPORT ON IMPLEMENTATION (2025), https://perma.cc/NDJ7-BEDQ [hereinafter 2025 CSC REPORT].

2. WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE U.S. 18–19 (2025), https://perma.cc/NV3D-P9LL [hereinafter NSS].

3. *See* Indictment at 3, U.S. v. Netyksho et al., No. 18-cr-215-ABJ (D.D.C. July 13, 2018), https://perma.cc/V9YQ-LJF4 (alleging Russian military intelligence officers engaged in a hacking and influence campaign targeting the 2016 U.S. elections).

4. Mike Levine & Jack Date, *22 Million Affected by OPM Hack, Official Says*, ABC NEWS (July 9, 2015), https://perma.cc/8PEJ-TSRP (reporting that ". . . more than 22 million people inside and outside government likely had their personal information stolen . . .," including applicants for security clearances who had their Social Security numbers and other personal information stolen and relatives and other associates also had information taken, according to OPM. That includes 3.6 million of the current and former government employees. "If an individual underwent a background investigation through OPM in 2000 or afterwards . . . it is highly likely that the individual is impacted by this cyber breach."); *see* Indictment at 45, U.S. v. Dong et al., No. 14-118 (W.D. Pa. May 1, 2014), https://perma.cc/G352-TF7V (charging Chinese military personnel with economic-espionage-motivated intrusions into U.S. firms); *see also* Press Release, U.S. DEP'T OF JUST., U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://perma.cc/CTA8-NEKA (indicting five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries, alleging the defendants stole trade secrets and other sensitive information beneficial to Chinese companies).

personal data of nearly 150 million Americans from Equifax,[5] underscored the inadequacy of a reactive cyber posture that imposed few meaningful costs on America's foreign adversaries.[6]

These developments catalyzed a fundamental shift in U.S. cybersecurity strategy, evolving from a purely Department of Defense military doctrine, known as *Defend Forward*,[7] into a broader whole-of-government cyber framework, consistent with the recommendations of the Cyberspace Solarium Commission. Complementing the Department of Defense, this model integrates the full spectrum of U.S. national power: the Department of the Treasury deploys targeted economic sanctions to isolate and financially constrict foreign cyber actors and their facilitators; the Department of Justice employs criminal indictments to attribute attacks, dismantle operational networks, and impose accountability; and the Department of State advances diplomatic initiatives to reinforce emerging norms of responsible state behavior in cyberspace.[8] These non-kinetic tools no longer operate in separate institutional silos. Instead, sanctions designations,

5. Indictment at 2, U.S. v. Wu Zhiyong et al. (No. under seal) (N.D. Ga. Jan. 20, 2020), https://perma.cc/5UXE-82K4 (alleging four members of China's People's Liberation Army for the 2017 Equifax breach, stealing sensitive personal information of nearly 150 million Americans); Press Release, U.S. DEP'T OF JUST., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://perma.cc/2LSY-BXG8.

6. *See* Ben Buchanan, *The Implications of Defending Forward in the New Pentagon Cyber Strategy*, COUNCIL ON FOREIGN RELS. (Sep. 25, 2018), https://perma.cc/VUP2-6Z3R [hereinafter *Defending Forward Implications*] (analyzing how the *Defend Forward* concept reshapes U.S. cyber operations).

7. The Department of Defense's Defend Forward doctrine represents a strategic shift from reactive cyber defense toward proactive, "persistent engagement," with foreign adversaries in cyberspace. The doctrine rests on the premise that malicious cyber activity against the United States is continuous rather than episodic and that effective defense therefore requires sustained operations to observe, pursue, and counter adversary campaigns at their source, often within foreign networks, before those operations reach U.S. systems. *See Hearing Before the Subcomm. on Intelligence and Emerging Threats and Capabilities of the H. Comm. on Armed Servs.*, 116th Cong. 2 (2020) (statement of Kenneth Rapuano); *see also Cyber Strategy Summary*, U.S. DEP'T OF DEFENSE (Sep. 18, 2018), https://perma.cc/GED6-ZWVK; U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR U.S. CYBER COMMAND 5–7 (2018), https://perma.cc/T399-PJV9. Operationalized under General Paul M. Nakasone's leadership at U.S. Cyber Command, *Defend Forward* authorizes continuous cyber operations designed to disrupt adversary infrastructure and degrade hostile capabilities while remaining below the threshold of armed conflict. *See* 2020 CSC REPORT, *supra* note 1, at 24, 33, 110. Scholars have emphasized that persistent engagement also serves a normative function, shaping state behavior through repeated interaction and reinforcing emerging norms of responsible conduct in cyberspace. *See* MICHAEL P. FISCHERKELLER, INST. FOR DEF. ANALYSES, PERSISTENT ENGAGEMENT AND TACIT BARGAINING: A STRATEGIC FRAMEWORK FOR NORMS DEVELOPMENT IN CYBERSPACE'S AGREED COMPETITION 16 (2018), https://perma.cc/9XLK-7RLB; *see also* JACK GOLDSMITH, THE UNITED STATES DEFEND FORWARD CYBER STRATEGY: A COMPREHENSIVE LEGAL ASSESSMENT 11 (2022). Congress codified this doctrinal shift in Section 1642 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which authorizes the Department of Defense, subject to National Command Authority approval, to conduct "appropriate and proportional action in foreign cyberspace" in response to ongoing cyber campaigns by Russia, China, Iran, or North Korea. Pub. L. No. 115-232, § 1642, 132 Stat. 1636, 2148–49 (2018). For discussion of the interaction between this authority and pre-existing constitutional and statutory war powers, *see* Robert Chesney, *The Domestic Legal Framework for U.S. Military Cyber Operations*, HOOVER INST. 1–6 (July 29, 2020), https://perma.cc/EP5W-YN2S.

8. *See* 2020 CSC REPORT, *supra* note 1, at 23–24, 29, 33.

criminal indictments, and diplomatic engagement now operate as mutually reinforcing instruments of attribution, accountability, disruption, cost imposition, and norm-building, together complementing the Department of Defense's *Defend Forward* posture as components of a unified architecture for countering foreign cyber threats.

The Biden Administration carried this model to maturity. In January 2025, days before leaving office, President Biden issued Executive Order 14,144, an expansive modernization of the cyber-sanctions framework first established in Executive Order 13,694. Yet the early trajectory of the second Trump administration reveals a more complex picture, defined by doctrinal continuity but institutional fragility. While the core playbook of integrated sanctions, prosecutions, diplomacy, and persistent engagement has remained intact, the Administration has simultaneously weakened key components of the federal cyber-governance infrastructure. The Cyberspace Solarium Commission's 2025 Annual Report documents the first measurable regression in whole-of-government cyber capacity since 2019, driven by reduced federal resourcing, bureaucratic downgrades, and the dismantling of interagency coordination mechanisms.[9] These developments pose structural risks to an otherwise durable bipartisan consensus on countering foreign cyber adversaries.

Against this backdrop, this article examines the legal and strategic architecture that emerged from the federal government's response to the Sony attack and ultimately matured into the modern U.S. cyber-sanction regime. It traces the evolution of economic sanctions as a central instrument of national cyber strategy; analyzes the deepening operational partnership among the Departments of Treasury, Justice, and State; and explores the interplay between executive power and statutory authority in targeting global cyber actors as part of a coherent framework for detecting, disrupting, imposing costs on, and laying the groundwork for cumulative deterrence against malicious cyber activity while shaping evolving norms of state responsibility in cyberspace. It further assesses the Biden Administration's final reforms, including Executive Order 14,144, and evaluates key areas of continuity and divergence under the second Trump Administration.

This article proceeds in six parts. Part II reconstructs the 2014 North Korean cyberattack on Sony Pictures Entertainment and the Obama Administration's unprecedented legal and strategic response, which together laid the foundation for the modern U.S. cyber-sanctions regime. Part III traces the subsequent evolution of that regime from the Obama Administration's foundational executive orders through the major statutory developments, most notably the Countering America's Adversaries Through Sanctions Act ("CAATSA") of 2017, which transformed cyber sanctions from a tool of executive discretion into a legislatively mandated policy. Part IV examines the deepening operational partnership between the Departments of the Treasury and Justice, detailing how coordinated sanctions designations and criminal prosecutions have become mutually reinforcing

9. *See id.*

tools for attributing, disrupting, and dismantling transnational cybercrime networks. Part V analyzes the Biden Administration's final cyber initiatives, including Executive Order 14,144, while Part VI assesses the emerging doctrinal continuity, divergence, and structural fragility of the U.S. cyber deterrence architecture under the second Trump Administration. In conclusion, Part VII evaluates the strategic significance and long-term resilience of the United States' integrated sanctions–prosecutions–diplomacy–military model amid accelerating technological change, AI-enabled cyber operations, and intensifying great-power competition in the digital domain.

Ultimately, this article argues that the U.S. response to the Sony attack ushered in a new era of cyber governance: one defined by interagency coordination, proactive defense, and the fusion of economic, legal, diplomatic, and military instruments into a unified architecture of persistent cyber statecraft that imposes costs, disrupts malicious networks, reinforces attribution, and strengthens international norms of responsible state behavior in cyberspace. As cyber operations grow increasingly sophisticated with artificial intelligence and other emerging technologies, sustaining and strengthening this whole-of-government framework will be essential to preserving U.S. security, global stability, and the rules-based international order in the digital age.

II. THE SONY HACK: A CASE STUDY IN CYBER WARFARE AND THE U.S. RESPONSE

A. The Hack Heard Around the World: North Korea's Cyberattack on Sony that Sparked a Global Security Crisis

In 2014, Sony Pictures Entertainment ("SPE" or "Sony") became the target of one of the most consequential cyber incidents in modern history, constituting a global incident that redefined the parameters of state-sponsored cyber warfare. The immediate catalyst was *The Interview*,[10] a satirical film depicting two journalists enlisted to assassinate North Korea's young new leader, Kim Jong-Un.[11] Despite Pyongyang's vehement objections, Sony proceeded with its release of the movie until a far more sinister reprisal emerged.[12]

In November 2014, a team of North Korean state-sponsored hackers, acting under government orders, launched a devastating cyberattack against Sony in retaliation for the film.[13] Armed with sophisticated malware, the hackers infiltrated Sony's internal network, seizing control of company systems.[14] Consequently, on November 24, SPE employees arrived at work to find their computer systems

10. THE INTERVIEW (Sony Pictures Ent. 2014).

11. David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More.*, N.Y. TIMES (Oct. 15, 2017), https://perma.cc/M2DQ-JVG4.

12. *Id.*

13. Press Release, FED. BUREAU OF INVESTIGATION, Update on Sony Investigation (Dec. 19, 2014), https://perma.cc/6EBB-NHL4 [hereinafter FBI Press Release on Sony Investigation].

14. Criminal Complaint & Affidavit at 3, ¶ 7, United States v. Park Jin Hyok, No. 18-MJ-1479 (C.D. Cal. June 8, 2018) [hereinafter Park Criminal Complaint] (detailing the North Korean hacker's role in the Sony attack, the WannaCry ransomware campaign, and other global intrusions); Press Release, U.S. DEP'T OF JUST., North Korean Regime-Backed Programmer Charged in Conspiracy to Conduct Multiple

hijacked by the chilling sight of a red skeleton and a menacing message from the "Guardians of Peace":

> We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data . . . to the world. Determine what will you do till November 24th, 11:00 PM (GMT).[15]

The attack crippled Sony's operations. The malware destroyed approximately 70 percent of the company's computers, rendering them inoperable, and forcing Sony to shut down its entire corporate network.[16] Employees were left scrambling to communicate, resorting to pen, paper, and phones.[17] Consequently, the company's business operations were significantly disrupted by the malware. The hackers stole vast quantities of proprietary data, confidential communications, and employees' personally identifiable information ("PII") before erasing Sony's hard drives and leaking embarrassing internal emails online.[18] The attack, which began as corporate sabotage, quickly became personal, as Sony executives, employees, and even theater owners who distributed its movies received direct threats of violence and more attacks should *The Interview* be released.[19]

Under mounting pressure, Sony canceled its planned theatrical debut of the film in movie theaters, opting for a limited digital distribution instead.[20] The Sony hack was more than an assault on a single corporation; it was a bold geopolitical statement that marked North Korea's emergence as a capable cyber power, signaling to the international community that the digital battleground was now a frontline in global conflict. It served as a stark wake-up call about the escalating nature of cyber threats that nations face in an increasingly interconnected, digital world, where cyberattacks now function as instruments of coercion and warfare, blurring the boundaries between espionage, sabotage, and armed conflict in the digital age.

B. The Obama Administration's Dilemma: Whether the U.S. Government Should Intervene in a Private Company's Defense Against North Korea's Cyberattack

The Federal Bureau of Investigation ("FBI") described North Korea's state-sponsored cyberattack on Sony Pictures Entertainment as deeply troubling in light of its destructive nature and its profound impact on both the company and

---

Cyberattacks and Intrusions (Sep. 6, 2018), https://perma.cc/B7R5-TT9C [hereinafter Park Press Release].

15. Park Criminal Complaint, *supra* note 14, ¶ 64.

16. Sanger et al., *supra* note 11; *see* FBI Press Release on Sony Investigation, *supra* note 13.

17. Sanger et al., *supra* note 11; *see* FBI Press Release on Sony Investigation, *supra* note 13.

18. *See* FBI Press Release on Sony Investigation, *supra* note 13; *see, e.g.*, Complaint at 26, Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at 1 (C.D. Cal. June 15, 2015), https://perma.cc/W79R-6Q48 (discussing a class action suit by eight Sony employees alleging that Sony failed to reasonably protect their personally identifiable information ("PII"), resulting in at least 15,000 current and former Sony employees' PII being compromised).

19. Sanger et al., *supra* note 11; *see* FBI Press Release on Sony Investigation, *supra* note 13.

20. *See* Sanger et al., *supra* note 11.

its employees.[21] The Sony intrusion was not merely another cyber incident; it constituted one of the most devastating acts of cyber warfare ever perpetrated by a foreign government against a U.S. corporation.[22] Although the FBI had encountered an increasing number and variety of cyber intrusions, what distinguished the Sony attack was not simply the scale of the damage but its coercive purpose: to inflict significant harm on an American business and suppress Americans' constitutional right to free expression.[23] Such acts of intimidation violate established international norms of acceptable state behavior and threaten the economic and social fabric of the United States.[24] North Korea's assault on SPE reaffirmed that malicious cyber activity represents one of the most serious and evolving national security threats confronting the nation.[25]

As news emerged that North Korean hackers had infiltrated Sony Pictures Entertainment, the Obama Administration confronted a genuinely unprecedented policy dilemma: whether the United States government should intervene to defend a private corporation from a state-sponsored cyberattack. Within the White House and across the national security agencies, this question likely triggered a vigorous debate. One camp would have likely emphasized Sony's inadequate cybersecurity posture as rendering any government intervention inappropriate and unwarranted. From this perspective, deploying federal resources to assist a company raised serious concerns. The company had failed to take basic measures to safeguard its own systems. Providing government assistance under those circumstances risked weakening incentives for private companies to invest in their own cybersecurity defenses. It could also establish a precedent that might obligate future administrations to respond whenever a private entity suffers a cyber intrusion by a foreign actor.[26] The opposing view would have likely framed this incident in fundamentally different terms: not as a routine commercial misfortune but as a deliberate act of state-sponsored coercion against a U.S. corporation. Under this conception, the attack implicated national security interests extending far beyond Sony itself. Thus, a forceful government response would be necessary to defend the broader norms governing responsible state behavior in cyberspace, deter future foreign aggression, and signal that foreign coercive cyber operations targeting American companies would not go unanswered.

The initial internal debate would have quickly converged on a more nuanced legal question: whether Sony qualified as part of the nation's "critical infrastructure" under Presidential Policy Directive-21 ("PPD-21"), which incorporated the

21. *See* FBI Press Release on Sony Investigation, *supra* note 13.
22. *See id.*
23. *See id.*
24. *See id.*
25. *See id.*
26. *See* James Andrew Lewis, *Sony and North Korea: Making the Case*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 5, 2014), https://perma.cc/4DVJ-VKLZ.

"critical infrastructure" definition set forth in the USA PATRIOT Act.[27] This inquiry required Administration officials to assess whether Sony fell within the scope of any of the sixteen designated "critical infrastructure" sectors, such as communications, commercial facilities, and information technology, whose incapacitation would have a "debilitating impact" on national security, the economy, or public health and safety.[28] Although Sony undeniably operated within the communications and information-technology arenas, Administration officials would likely have concluded that it did not meet the "critical infrastructure" threshold under PPD-21. Its disruption, however consequential for the company and its employees, would not, on its own, singularly cripple the U.S. economy or meaningfully compromise national security. As a result, Sony could not be treated as "critical infrastructure" for purposes of triggering any special federal protection obligation.

Although the Administration would have determined that Sony did not fall within the Directive's "critical infrastructure" definition, the stakes would have continued to rise for officials as another nuanced legal question loomed: whether the North Korean intrusion constituted an "unusual and extraordinary threat" to the national security, foreign policy, or economy of the United States, sufficient to justify invoking national emergency powers under the International Emergency Economic Powers Act ("IEEPA")[29] and the National Emergencies Act ("NEA").[30] Making such a determination would have transformed a corporate breach into a national security emergency, authorizing the President to deploy the full arsenal of nonmilitary tools against its foreign adversary, North Korea. Yet even if the statutory threshold could be met, employing national emergency powers in response to a private-sector cyber incident risked establishing a precedent that would effectively obligate the federal government to intervene whenever an American corporation was targeted by foreign actors. The Administration thus found itself navigating a delicate balance: deterring and punishing state-sponsored aggression while avoiding the creation of expansive, and potentially unsustainable, expectations of federal protection for private-sector victims of foreign cyber operations.

Despite these institutional concerns, the Obama Administration ultimately recognized that the implications of the Sony attack extended far beyond a single corporation. It was about establishing a deterrent framework for addressing state-sponsored cyberattacks and signaling to America's adversaries, such as North Korea, that malicious cyber activity targeting the United States would carry consequences. On the other hand, a failure to act risked signaling to North Korea and others that the United States lacked either the capacity or the will to impose costs for state-sponsored cyber aggression. Such inaction, in the Administration's

27. *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, WHITE HOUSE (Feb. 12, 2013), https://perma.cc/93HP-54N4 [hereinafter *Presidential Policy Directive 21*].

28. *Id.*; Park Press Release, *supra* note 14.

29. International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1710 [hereinafter IEEPA].

30. National Emergencies Act, 50 U.S.C. §§ 1601–1651 [hereinafter NEA].

view, would have emboldened hostile states to escalate their operations against U.S. targets, thereby increasing long-term dangers to U.S. national security. The Sony attack arguably did not meet IEEPA's statutory requirement of an "unusual and extraordinary threat." Nevertheless, the Administration concluded that the incident warranted a more expansive interpretation of its authorities and forceful response. Its objective was not only to address the immediate harm caused by the attack, but also to establish a framework for imposing consequences, signaling red lines, and laying the groundwork for a more credible long-term deterrence posture against future cyber intrusions. By invoking the flexible, and at times deliberately ambiguous language of IEEPA and NEA, the Executive Branch exercised its discretionary emergency authority to impose economic costs on North Korea and to signal a clear red line against state-sponsored cyber coercion to safeguard the nation's broader security interests. While IEEPA's text suggests some limitations on that authority, neither Congress nor the courts challenged the President's determination of a national emergency in the Sony context, reinforcing the President's considerable latitude in defining the scope of national emergencies in the cyber domain.

The Administration's concerns would prove well-founded. The 2014 Sony hack, which was North Korea's retaliatory response for the film *The Interview*, involved massive data breaches and the destruction of Sony's internal systems, capturing worldwide headlines and illustrating the vulnerability of private corporations to state-sponsored cyber aggression. Yet this incident was merely the opening act. In the years that followed the Sony attack, Pyongyang dramatically escalated its cyber operations, executing increasingly sophisticated, high-profile, and financially profitable attacks across the globe. For example, in February 2016, North Korean state-sponsored hackers orchestrated the Bangladesh Bank heist, attempting to steal over $1 billion from financial institutions worldwide and ultimately succeeding in siphoning $81 million from the bank.[31] According to court filings, the conspirators in the Bangladesh Bank heist infiltrated the bank's network through spear-phishing campaigns targeting bank employees, and ultimately gaining access to the computer terminals connected to the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") network.[32] Once inside, they transmitted fraudulent SWIFT messages instructing the Federal Reserve Bank of New York to transfer funds from the bank's reserve account to accounts under the conspirators' control.[33] The operation revealed North Korea's growing capacity to exploit systemic vulnerabilities in the international financial system.

---

31. Press Release, U.S. DEP'T OF JUST., DOJ Criminal Complaint of a North Korean Regime-Backed Programmer (Sep. 6, 2018), https://perma.cc/2QXH-NB7X [hereinafter North Korean Programmer Complaint]; *see* U.S. DEP'TS OF STATE, TREASURY, HOMELAND SEC. & JUST., DPRK CYBER THREAT ADVISORY GUIDANCE ON THE NORTH KOREAN CYBER THREAT (2020), https://perma.cc/PL7V-GUF8 [hereinafter DPRK CYBER THREAT ADVISORY].

32. *See* North Korean Programmer Complaint, *supra* note 31; DPRK CYBER THREAT ADVISORY, *supra* note 31.

33. *See* North Korean Programmer Complaint, *supra* note 31; DPRK CYBER THREAT ADVISORY, *supra* note 31.

A year later, in May 2017, North Korean state-sponsored cyber operatives unleashed the ransomware "WannaCry 2.0," which encrypted victims' data on hundreds of thousands of computers across more than 150 countries and demanded ransom payment in Bitcoin digital currency in exchange for their decryption keys.[34] The attack paralyzed hospitals, schools, transportation networks, and businesses worldwide, causing hundreds of millions, if not billions, of dollars in economic losses.[35] In response, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") designated a North Korean computer programmer involved in the Sony, Bangladesh Bank, and WannaCry 2.0 operations and the organization employing him as Specially Designated Nationals and Blocked Persons ("SDNs").[36] As a legal consequence of these actions, all property and interests in property[37] of these designated persons that come within the possession or control of U.S. persons[38] or that are otherwise subject to U.S. jurisdiction must be blocked (or frozen).[39] U.S. persons generally are prohibited from engaging in any transactions or dealings with the designated individuals or entities absent a specific license authorization from OFAC. These measures effectively severed the designees' access to the U.S. financial system. More broadly, these OFAC designations marked not only a response to the growing threat posed by North Korea's cyber apparatus but also a significant evolution in U.S. cyber statecraft. They reflected the integration of economic sanctions not merely as a punitive measure, but as a core element of an emerging cyber-deterrence strategy in the United States, designed to impose costs on state-sponsored malicious cyber activity while shaping adversary behavior in the digital domain.[40]

---

34. *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, WHITE HOUSE (Dec. 19, 2017), https://perma.cc/C5DL-BVEM [hereinafter *White House WannaCry Attribution*]; DPRK CYBER THREAT ADVISORY, *supra* note 31; *see* North Korean Programmer Complaint, *supra* note 31.

35. Park Press Release, *supra* note 14; Park Criminal Complaint, *supra* note 14; *see* FBI Press Release on Sony Investigation, *supra* note 13.

36. Press Release, U.S. Dep't of the Treasury, Treasury Targets North Korea for Multiple Cyber-Attacks (Sep. 6, 2018), https://perma.cc/CM6D-QE93 [hereinafter Treasury Targets DPRK Cyber-Attacks]; *see* DPRK CYBER THREAT ADVISORY, *supra* note 31.

37. Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015), https://perma.cc/R3ZH-LEQT; 31 C.F.R. § 578.309 (2024) (defining "interests in property" as anything tangible or intangible, including money, trade, checks, contracts, goods, real property, contingent rights or obligations).

38. Pursuant to the Cyber-Related Sanctions Regulations, 31 C.F.R. § 578.314, a "U.S. person" is any U.S. citizen, permanent resident alien, entity organized under U.S. law (including foreign branches), or any person in the United States; and, under certain sanctions programs like the Cuba Sanctions Regulations, 31 C.F.R. § 515.329, U.S. controlled foreign subsidiaries.

39. *See, e.g.*, Trading with the Enemy Act, 50 U.S.C. §§ 4301–4341; IEEPA, *supra* note 29, 50 U.S.C. §§ 1702, 1708– 1710; Exec. Order No. 13,694, *supra* note 37, §§ 1(a), (b), 3, 5; 31 C.F.R. § 578.201; U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 3 (2020), https://perma.cc/SN3P-TG8J [hereinafter RANSOMWARE ADVISORY]. *See generally* U.S. DEP'T OF THE TREASURY, OFAC CYBER-RELATED SANCTIONS PROGRAM OVERVIEW 4 (July 3, 2017), https://perma.cc/C4BQ-MLXN [hereinafter SANCTIONS OVERVIEW].

40. Treasury Targets DPRK Cyber-Attacks, *supra* note 36; *see* DPRK CYBER THREAT ADVISORY, *supra* note 31.

Once ridiculed for its technologically unsophisticated cyber capabilities, North Korea has established itself as a formidable player in the domain of digital warfare, capable of disrupting global markets and inflicting substantial economic harm.[41] The Sony incident marked a pivotal moment in the evolution of U.S. cyber policy, revealing the vulnerabilities of private industry to state-sponsored cyber aggression and the government's response, integrating economic sanctions into the United States' broader digital warfare and deterrence strategy.

C. Obama Strikes Back with Sanctions and Criminal Charges

1. Treasury Hits North Korea with Additional Sanctions.

Against this backdrop, the U.S. government responded swiftly and unequivocally to North Korea's cyberattack on Sony Pictures Entertainment, marking a pivotal shift in the United States approach to foreign cyber threats. In the wake of this unprecedented breach, the Obama Administration adopted a series of measures designed to signal to the world that cyber aggression by hostile states would not be tolerated. Central to this response was the deployment of economic sanctions, tools intended not only to punish North Korea for its destructive conduct but also to deter future malicious cyber operations and reinforce international norms of responsible state behavior in cyberspace.

On January 2, 2015, President Obama issued Executive Order 13,687, imposing sweeping sanctions on the Government of North Korea and the Workers' Party of North Korea for their role in the cyberattack against Sony Pictures Entertainment.[42] Citing Pyongyang's "destructive, coercive cyber-related actions," the order authorized OFAC to designate three North Korean-controlled entities and ten senior government officials as SDNs, effectively severing these entities' and officials' access to the U.S. financial system.[43] Despite these measures and subsequent designations targeting additional North Korean individuals and entities, Pyongyang appeared largely unmoved, underscoring the limitations of sanctions when directed against an already isolated regime.[44] The Sony incident nonetheless served as a wake-up call for Washington, prompting the United States to adopt a more coordinated and aggressive "whole-of-government" cyber strategy that combined sanctions, criminal prosecutions, and diplomatic engagement in ways that complemented the Department of Defense's *Defend Forward* posture.[45] This approach extended beyond North Korea to encompass other state adversaries, including Iran, Russia, and China, whose cyber activities posed significant threats to U.S. national security and the global digital economy.[46]

41. Sanger et al., *supra* note 11.
42. *See* Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015).
43. *Id.*
44. Sanger et al., *supra* note 11.
45. Naomi Aoki, Melvin Tay & Stuti Rawat, *Whole-of-Government and Joined-Up Government: A Systematic Literature Review*, 102 PUB. ADMIN. 733, 734 (2023), https://perma.cc/6AEW-F8XX.
46. *Id.*

2. The U.S. Justice Department Criminally Charges North Korea's Cybercrime Syndicate

In a landmark enforcement action reflecting this "whole-of-government" approach, the U.S. Department of Justice unsealed a detailed criminal complaint in September 2019, exposing the inner workings of a North Korean state-sponsored cybercrime network.[47] The complaint charged Park Jin Hyok, a programmer affiliated with the Lazarus Group, which was a cyber unit operating under North Korea's primary intelligence organization, the Reconnaissance General Bureau, with conspiracy to commit computer fraud and wire fraud.[48] Park was identified as a principal architect of several of the most destructive cyberattacks in modern history, including the 2014 SPE intrusion, the 2016 Bangladesh Bank heist, and the 2017 WannaCry 2.0 ransomware campaign.[49] On the same day, OFAC designated Park as an SDN under Executive Order 13,722, part of the broader North Korea Sanctions Program, for his role in malicious cyber activities.[50] OFAC simultaneously designated the Lazarus Group and its subgroups, Bluenoroff and Andariel, each controlled by North Korea's Reconnaissance General Bureau, as SDNs.[51]

Together, these measures signaled that North Korea's cyber operations would be met with the full range of legal and financial tools available to the United States. This coordinated action by the Treasury and Justice Departments illustrated the new U.S. cyber strategy: the integration of economic sanctions and criminal prosecutions as complementary instruments to deter future cyberattacks and redefine what constitutes acceptable responsible norms of behavior in cyberspace on a global scale.[52]

III. U.S. WHOLE-OF-GOVERNMENT APPROACH OF ECONOMIC SANCTIONS, CRIMINAL ENFORCEMENT, & DIPLOMACY TO COMBAT MALICIOUS CYBER ACTORS

A. The Role of the U.S. Department of the Treasury in the New Era of Cyber Threats

1. Hackers Beware: Obama's Sanctions Redrew the Battle Lines in Cyber Warfare with Executive Orders 13,694 and 13,757

In the wake of the Sony Pictures Entertainment cyberattack, the U.S. government reacted in a way that reshaped the digital battlefield.[53] April 1, 2015, marked

47. Park Press Release, *supra* note 14; Park Criminal Complaint, *supra* note 14.

48. Park Press Release, *supra* note 14; Park Criminal Complaint, *supra* note 14.

49. Park Press Release, *supra* note 14; Park Criminal Complaint, *supra* note 14.

50. Treasury Targets DPRK Cyber-Attacks, *supra* note 36.

51. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sep. 13, 2019), https://perma.cc/9DHH-3EC8.

52. President Barack Obama, *A New Tool Against Cyber Threats*, MEDIUM (Apr. 1, 2015), https://perma.cc/2NU5-BE8F [hereinafter *New Tool Against Cyber Threats*]; *see also* 2020 CSC REPORT, *supra* note 1.

53. *See* U.S. DEP'T OF THE TREASURY, Sanctions Related to Significant Malicious Cyber-Enabled Activities (Dec. 18, 2020), https://perma.cc/4APE-24QM.

the official birth of the U.S. cyber-related sanctions regime, as President Obama, wielding the powers granted by IEEPA[54] and NEA,[55] issued Executive Order 13,694.[56] Declaring a "national emergency," President Obama framed the "increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States" as an "unusual and extraordinary threat" to national security, foreign policy, and the economy.[57] This was no small maneuver. Rather, this was the first time sanctions were tailored specifically to combat digital threats, with "targeted sanctions against individuals or entities whose actions in cyberspace result in significant threats to the national security, foreign policy, economic health, or financial stability of the United States."[58] These sanctions were aimed at punishing cybercriminals and changing the rules of the global cybersecurity game.

The Executive Order was not just a slap on the wrists of those who engaged in malicious cyber activity. Rather, it was about financially isolating those who thought they could lurk in the dark corners of the Internet, committing malicious cyber activity without any repercussions. President Obama's message was clear: the worst offenders, especially those targeting U.S. infrastructure, companies, and citizens, would face economic exile from the U.S. financial system. Treasury's OFAC was handed the reins as the primary agency entrusted with administering and enforcing these sanctions, which included identifying and sanctioning cybercriminals, freezing their assets, and cutting them off from the U.S. financial system.[59] President Obama promised to use these sanctions "judiciously," targeting only the most severe threats by "go[ing] after the worst of the worst,"[60] such as "[t]hose whose cyber activities – whether directed against our critical infrastructure, our companies, or our citizens – could threaten the national security, foreign policy, economic health, or financial stability of the United States."[61] The Treasury Secretary reminded the world that the Executive Order allowed it "to expose and financially isolate those who hide in the shadows of the Internet to conduct malicious cyber activities."[62]

---

54. IEEPA, *supra* note 29.

55. NEA, *supra* note 30.

56. Exec. Order No. 13,694, *supra* note 37 (representing a pivotal expansion of U.S. efforts to combat significant malicious cyber-enabled activities, with a particular focus on addressing the misuse of U.S. Infrastructure as a Service ("IaaS") products by foreign actors).

57. *Id.* (noting that Exec. Order No. 13,694, like other similar Executive Orders signed by the President under IEEPA and NEA, was issued without public notice; consequently, the public did not have an opportunity to provide comments concerning the Order). *See generally* SANCTIONS OVERVIEW, *supra* note 39, at 3–4.

58. *New Tool Against Cyber Threats*, *supra* note 52.

59. Exec. Order No. 13,694, *supra* note 37.

60. *Id.*

61. Michael Daniel, *Our Latest Tool to Combat Cyber Attacks: What You Need to Know*, WHITE HOUSE BLOG (Apr. 1, 2015), https://perma.cc/SV6V-G3NR [hereinafter *What You Need to Know*].

62. *Id.*

Russia's interference in the 2016 U.S. presidential election raised the stakes considerably and prompted a further expansion of these authorities. On December 28, 2016, President Obama released Executive Order 13,757, which was an expansion of Executive Order 13,694, targeting anyone who dared meddle with U.S. elections.[63] Specifically, Executive Order 13,694, as amended by Executive Order 13,757, authorizes the blocking (or freezing) of the property and interests in property[64] of persons or entities determined by the Treasury Secretary, in consultation with the Attorney General and the Secretary of State, "to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[65] Under the Order, cyber-enabled activities that meet this threshold must have the specified purpose or effect of:

> (A) harming, or otherwise significantly compromising the provision of services by a computer or network of computers that support one or more entities in a critical infrastructure sector;
>
> (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
>
> (C) causing a significant disruption to the availability of a computer or network of computers;
>
> (D) causing a significant misappropriation[66] of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or
>
> (E) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.[67]

---

63. Exec. Order No. 13,757, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, 82 Fed. Reg. 1 (Dec. 28, 2016), https://perma.cc/A4RH-QPBR. *See generally* SANCTIONS OVERVIEW, *supra* note 39, at 3–4.

64. Exec. Order No. 13,694, *supra* note 37, §1 (a)(ii); 31 C.F.R. § 578.309 (2024).

65. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i).

66. The Executive Order defines "misappropriation" as "the taking or obtaining [of information] by improper means, without permission or consent, or under false pretenses." *Frequently Asked Questions 489*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Dec. 29, 2016), https://perma.cc/DNY6-P9MM.

67. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i)(A)-(D), amended by Exec. Order No. 13,757, *supra* note 63, § 1(a)(ii)(E) (emphasizing that subparagraphs (A)-(D) were included in the original Executive Order 13,694 in April 2015, until it was subsequently amended by Executive Order 13,757 in December 2016, which added subparagraph (E) in light of Russia's interference in the 2016 U.S. presidential election).

The individual provisions of this Executive Order cast a wide net over cyber-enabled activities. Subparagraphs (A) and (C), for instance, target not just massive cyberattacks that harm, compromise, or disrupt a network of computers, but even actions that compromise a single computer.[68] Subparagraphs (A) and (B) focus on critical infrastructure, as defined by Presidential Policy Directive 21.[69] Subparagraph (C) goes even further, sanctioning any significant disruption to a computer network, with no requirement that the computer involve a critical infrastructure sector[70]; this provision was designed in part to tackle Iran's distributed denial-of-service ("DDoS") attacks on U.S. financial institutions between 2011 and 2013.[71] Moving to Subparagraph (D), this provision zeroes in on state-sponsored intellectual property theft, with China being a prime suspect here.[72] And lastly, subparagraph (E), which was added by Executive Order 13,757 in December 2016, introduces a critical update in the wake of Russia's meddling in the 2016 U.S. elections, creating the legal framework to sanction future election interference and disinformation campaigns designed to undermine American democracy.[73]

Executive Order 13,694 does not stop there. It authorizes sanctions blocking (or freezing) the property or interests in property against any party receiving stolen trade secrets through cyber means, so long as there is knowledge the trade secrets were stolen, and the theft is "reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[74] This clause acts as a deterrent, targeting companies that "knowingly use stolen trade secrets to undermine the nation's economic health."[75] This order also authorizes blocking sanctions against those who knowingly benefit from these malicious cyber activities, namely, both the hackers and their customers.[76] This two-pronged approach is a rare maneuver in U.S. sanctions programs, striking at both the supply and demand sides of cybercrime.[77]

Moreover, the Order empowers the U.S. to freeze the assets of anyone who materially assists, sponsors, or supports these cyber-enabled activities.[78] These

68. *Id.*

69. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i)(A)-(B); *see Presidential Policy Directive 21*, *supra* note 27.

70. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i)(C).

71. Press Release, FED. BUREAU OF INVESTIGATION, International Cyber Crime: Iranians Charged With Hacking U.S. Financial Sector (Mar. 24, 2016), https://perma.cc/6KK6-AEG6; *see* Kristen Eichensehr, *The Cyber Sanctions Executive Order: What Will It Do and Will It Work*, JUST SEC. (Apr. 2, 2015), https://perma.cc/W5KA-KXMT [hereinafter *Cyber Order: What Will It Do and Will It Work*].

72. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i)(D); *see Cyber Order: What Will It Do and Will It Work*, *supra* note 71.

73. Exec. Order No. 13,694, *supra* note 37, § 1(a)(i)(E), amended by, Exec. Order No. 13,757, *supra* note 63, § 1(a)(ii)(E).

74. Exec. Order 13,694, *supra* note 37, § 1(a)(ii)(A).

75. *Id.*

76. *Id.*

77. *New Tool Against Cyber Threats*, *supra* note 52.

78. Exec. Order 13,694, *supra* note 37, § 1(a)(ii)(B)-(C).

sanctions further apply to any party owned or controlled by or acting for or on behalf of any party designated under the Order.[79] Like all other Executive Orders, entry into the U.S. is denied to any parties designated under this Order.[80] In short, this Executive Order represents a significant impediment to cybercriminals and their enablers, whose activities threaten the security or economy of the United States by damaging critical infrastructure, disrupting or hijacking computer networks, and stealing trade secrets for commercial gain. The Order empowers the government with robust authorities to respond to these threats, including the ability to block access to the U.S. financial system and freeze assets, restricting offenders' ability to conduct business with U.S. companies and thus limiting their ability to profit from their illicit cyber activities.[81]

In sum, President Obama's groundbreaking sanctions did not stop at just targeting hackers; they went after anyone benefiting from stolen data, too.[82] The sanctions program now extends to companies knowingly using stolen trade secrets, flipping the script by taking aim at the demand side of cybercrime.[83] Whether you bankrolled a hacker or conveniently turned a blind eye while cashing in on stolen data, the U.S. was coming for you. Armed with a powerful arsenal of sanctions and an ironclad legal framework administering and enforcing these sanctions, the U.S. was ready to flex its economic muscle to block bad actors from reaping the rewards of their misdeeds, reshaping the norms of cyberspace in the process and sending a clear message that in this new digital battleground, no one is untouchable or outside the scope of the U.S. government's sanctions regime.

2. OFAC Unleashes Sanctions Regulations Under Executive Authority in the Digital Battlefield

Building on this expanding executive authority, the Treasury Department moved to operationalize the new cyber sanctions regime through comprehensive regulations. On December 31, 2015, OFAC, an arm of the Treasury responsible for administering and enforcing U.S. trade and economic sanctions, issued Cyber-Related Sanctions Regulations (31 C.F.R. Part 578).[84] These regulations implemented the broad authorities granted by Executive Orders 13,694, as amended. In doing so, they converted the broad Executive Order's policy objectives into enforceable regulatory measures. The regulations target malicious cyber actors and their financial enablers by authorizing their designation on OFAC's SDN List under the "[CYBER]" designation.[85] Moreover, any company even partially owned by one or more blocked individuals or entities in aggregate

79. *Id.*
80. *Id.* § 4.
81. *New Tool Against Cyber Threats*, *supra* note 52.
82. *Id.*
83. *Id. See also What You Need to Know*, *supra* note 61.
84. Cyber-Related Sanctions Regulations, 31 C.F.R. Part 578 (Sep. 6, 2022).
85. 31 C.F.R. § 578.201 (2024).

faces the same fate as an SDN under OFAC's 50% Rule, even if such a company is not explicitly included on OFAC's SDN List.[86] Consequently, U.S. persons are strictly prohibited from doing business with these cyber bad actors, essentially cutting them off from the U.S. financial system entirely.[87] Unlike the rules issued by the Financial Crimes Enforcement Network ("FinCEN"), OFAC's counterpart in rulemaking at the Treasury Department, OFAC's Cyber-Related Sanctions Regulations became immediately effective, without "notice and comment," giving OFAC full power to crack down on cybercrime without delay.[88]

Neither the White House nor the Department of the Treasury has explicitly defined the term malicious "cyber-enabled" activities in the Executive Order or its implementing Regulations. OFAC, however, has issued guidance clarifying the conduct covered by the sanctions program. According to OFAC's guidance, the sanctions target individuals and entities responsible for deliberate activities conducted through unauthorized access to computer systems.[89] Such activities include hacking, bypassing security measures, and compromising hardware or software.[90] Moreover, these sanctions "target those actors whose malicious cyber-enabled conduct is reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[91] These sanctions are designed to punish the worst offenders who wreak havoc on critical infrastructure, launch denial-of-service attacks, and steal sensitive information like trade secrets and personal financial data.[92] OFAC has, however, reassured the public that legitimate cyber activities,[93] and innocent victims, caught in the crossfire are not the focus here.[94]

---

86. 31 C.F.R. § 578.406 (2024).

87. 31 C.F.R. § 578.201 (2024).

88. Cyber-Related Sanctions Regulations, 80 Fed. Reg. 81,752, 81,753 (Dec. 31, 2015) (explaining that the OFAC Cyber-Related Sanctions Regulations were issued by OFAC in the Federal Register on the same date they were set to become effective, December 31, 2015, consequently without public notice; therefore, the public did not have an opportunity to provide comments concerning the regulations).

89. *Frequently Asked Questions 447*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Apr. 1, 2015), https://perma.cc/77A4-Q8ZU.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Frequently Asked Questions 448*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Apr. 1, 2015), https://perma.cc/HU42-6AWF (explaining that the Order is not designed to prevent or interfere with legitimate cyber-enabled academic, business, or non-profit activities; noting that the U.S. government supports efforts by researchers, cybersecurity experts, and network defense specialists to identify, respond to, and repair vulnerabilities that could be exploited by malicious actors; and clarifying that the Order does not target persons engaged in legitimate activities that ensure and promote the security of information systems (including penetration testing, academic research, commercial innovation, or "good faith" security-oriented events") nor does it restrict routine network defense or maintenance activities performed on authorized system); *Frequently Asked Questions 449*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Apr. 1, 2015), https://perma.cc/7CEW-ZC3C.

94. *Frequently Asked Questions 450*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Apr. 1, 2015), https://perma.cc/2UVV-WCX3.

The Cyber-Related Sanctions Regulations, implementing the executive orders, marked a decisive step in the U.S. government's strategy to hit malicious actors where it hurts: their wallets. With this regulatory framework, OFAC made it clear to bad actors worldwide that the days of hiding behind a computer screen while wreaking havoc on the digital world were over. These regulations created the practical enforcement machinery necessary to give the executive orders real-world force, ensuring that designations translated into concrete financial consequences across the global economy. But sanctions regulations alone were not enough. As cyber threats escalated, particularly from Russia, Iran, and North Korea, Congress found itself needing to intervene to further strengthen the regime.

3. Congress Forces Trump's Hand with CAATSA to Enforce Global Cyber Sanctions on Russia

By 2017, amid doubts about the incoming Trump Administration's willingness to hold Russia accountable for its malicious cyber activities, Congress took decisive bipartisan action. With a resounding vote of 419 to 3 in the House of Representatives and 98 to 2 in the Senate, lawmakers enacted the Countering America's Adversaries Through Sanctions Act, effectively forcing President Trump's hand by transforming cyber sanctions from an executive policy choice into a statutory mandate.[95] Unable to veto the bill, on August 2, 2017, the President signed into law one of the most comprehensive sanctions packages in U.S. history,[96] targeting not just Russia for its cyber meddling, but also Iran and North Korea.[97]

CAATSA did not just codify existing sanctions like Executive Order 13,694, Section 224(a)(1) of the Act mandated that the President bar entry to the U.S. and impose asset-blocking sanctions on any individual or entity involved in "significant activities undermining cybersecurity" or any entity owned or controlled by or acting for or on behalf of such person.[98] The Act defines "significant activities undermining cybersecurity" as including:

> (1) significant efforts (A) to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or (B) to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of— (i) conducting influence operations; or (ii) causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for

95. Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, 131 Stat. 886 (2017) [hereinafter CAATSA].

96. Emily Tamkin, *Trump Finally Signs Sanctions Bill, Then Adds Bizarre Statements*, FOREIGN POL'Y (Aug. 2, 2017) (quoting that "President Donald Trump may have felt forced to sign the new sanctions legislation into law").

97. CAATSA, *supra* note 95, §§ 112, 216, 224(a)(1), 224(a)(2), 224(d), 228 (amending 22 U.S.C. § 8901 *et seq.*), 235, 236.

98. *Id.* § 224(a)(1).

> commercial or competitive advantage or private financial gain; (2) significant destructive malware attacks; and (3) significant denial of service activities.[99]

Whether disrupting networks, stealing sensitive information, or degrading communications systems, these bad actors were in the crosshairs of the U.S. government.

The U.S. government's crackdown on malicious cyber activities did not stop there. Section 224(a)(2) of the Act extended beyond U.S. borders, extraterritorially imposing "secondary" sanctions on any foreign individual or entity who "knowingly materially assists, sponsors, or provides financial, material, or technological support for, or goods or services in support of," a significant activity undermining cybersecurity.[100] Section 228 went even further, requiring the President to impose "secondary" sanctions on any foreign individual or entity who knowingly materially violates, attempts to violate, conspires to violate or causes a violation of Executive Order 13,694, as amended, or facilitates a significant transaction for or on behalf of any person subject to sanctions imposed by the United States with respect to Russia, or any child, spouse, parent or sibling of such sanctioned person.[101]

Secondary sanctions included: (1) the denial of export-import bank assistance in connection with any exports of goods or services to a sanctioned person; (2) the prohibition against a U.S. financial institution's loans to sanctioned persons; (3) the prohibition against the U.S. government procuring goods or services from a sanctioned person; (4) the prohibition against any banking or property transactions in which a sanctioned person has an interest; (5) a ban on investments in the equity or debt of a sanctioned person; (6) the exclusion from the United States of a corporate officer, principal or shareholder with a controlling interest in a sanctioned person; and (7) the imposition of any of these secondary sanctions on the principal executive officer of a sanctioned person.[102] The punishment potentially included anything from freezing assets to denying access to loans and contracts, prohibiting investments, and banning entry into the U.S. by key executives.

CAATSA gave the U.S. government a long arm of justice with an extraterritorial reach to its cyber sanctions regime. Unlike "primary" sanctions, which apply to U.S. persons or transactions with a U.S. nexus,[103] these penalties forced non-U.S. companies and citizens to avoid dealings with sanctioned individuals and entities or engaging in sanctionable conduct described under Section 224(a)(2) or Section 228 of CAATSA or risk being sanctioned themselves, even though neither the person nor the transaction may be subject to U.S. jurisdiction.[104] The U.S. was effectively flexing its economic muscle far beyond its own borders,

99. *Id.* § 224(d).
100. *Id.* §§ 224(a)(2), 235.
101. *Id.* § 228 (amending 22 U.S.C. 8901 *et seq.*).
102. *Id.* § 235.
103. *Id.*
104. *Id.* §§ 224(a)(2), 228.

forcing foreign actors to rethink their business dealings or face severe financial and legal repercussions. The rules of engagement had thus shifted: foreign actors, once free to engage in cyber sabotage without major consequences, now had to contend with the full force of U.S. sanctions, even when operating completely offshore without any nexus to the United States.

Despite President Trump's view that CAATSA overstepped Article II constitutional boundaries, the President signed it into law rather than challenge Congress in court.[105] This decision was likely influenced by the statute's inclusion of limited presidential waiver authority on sanctions, *albeit* under heightened congressional oversight.[106] Even with that concession, CAATSA hardened the United States' posture on cyber-related sanctions by reinforcing Executive Order 13,694's measures and significantly expanding the reach of the U.S. government's sanctions authority far beyond its borders.[107] Foreign actors, who were once free to engage in cyber sabotage without major consequences, now had to think twice before doing business with sanctioned individuals and companies, lest they find themselves swept up in the U.S. sanctions net and having to contend with the full force of U.S. secondary sanctions. CAATSA thus strengthened the cyber sanctions framework on two fronts. First, it codified existing executive authorities, reducing their susceptibility to future political reversal, and second, it introduced powerful new "secondary" sanctions with genuine extraterritorial force. This expansion raised a critical question: how would these increasingly robust sanctions be enforced?

4. OFAC's Enforcement Guidelines and Penalties: A Wake-Up Call for Sanctions Violators

With both executive and legislative authorities now firmly in place, this article turns to the topic of enforcement, the defining driving force behind the U.S. cyber sanctions regime. The penalties for sanctions violators can be quite severe, adding to the deterrent effect of the U.S. sanctions program against foreign actors who dare to engage in malicious cyber activities and any U.S. persons who transact with them.

These penalties range from civil to criminal, depending on the nature of the violation. Criminal violations of cyber-related sanctions fall within the jurisdiction of the Department of Justice, which may impose penalties of up to $1,000,000 and, for natural persons, prison sentences of up to 20 years for willful breaches.[108] On the civil side, OFAC may levy penalties not to exceed the greater of $377,700 per violation or an amount that is twice the amount of the underlying transaction for a cyber-related sanctions violation under IEEPA.[109] These authorities are not theoretical: over the past decade, both U.S. and non-U.S. persons

105. Statement on Signing the Countering America's Adversaries Through Sanctions Act, 2017 DAILY COMP. PRES. DOC. 00559 (Aug. 2, 2017).

106. CAATSA, *supra* note 95, §§ 112, 216, 236.

107. *Id.*

108. IEEPA, *supra* note 29, § 1705(c); 31 C.F.R. § 578.701(a)(3) (2024).

109. IEEPA, *supra* note 29, § 1705(b); 31 C.F.R. § 578.701(a)(2) (2024).

have faced unprecedented sanctions penalties. For instance, France's largest bank, BNP Paribas, paid a record-setting $8.9 billion fine in 2014 for sanctions violations, while HSBC, the world's largest U.S. dollar clearing bank, incurred approximately $1.3 billion in penalties in 2012.[110] These outcomes demonstrate the sheer force of U.S. sanctions enforcement and the high stakes for entities that fail to comply with cyber-related restrictions.

To avert these potentially crippling penalties, many companies have invested heavily in robust sanctions compliance programs incorporating enhanced due diligence tools, most notably Know Your Customer ("KYC") and Know Your Customer's Customer ("KYCC") procedures.[111] Yet even the most sophisticated compliance framework cannot insulate a company from civil exposure. Because U.S. sanctions operate under a strict-liability regime, a company may be held liable for a prohibited transaction regardless of its intent, knowledge, or awareness of the underlying violation.[112]

To provide some measure of predictability, OFAC has issued detailed Economic Sanctions Enforcement Guidelines outlining the factors it weighs when assessing penalties for sanctions violations.[113] These guidelines encourage organizations to adopt risk-based, tailored compliance programs and emphasize the value of voluntary self-disclosure, prompt remediation, and full cooperation with investigators.[114] A company's robust sanctions compliance efforts can meaningfully mitigate the severity of an enforcement action.[115] In some cases, it can mean the difference between a substantial civil penalty and a cautionary letter or no-action determination.[116]

The prospect of severe penalties serves as a powerful deterrent, discouraging U.S. and non-U.S. businesses and individuals from facilitating malicious cyber activity. At the same time, it incentivizes companies to proactively take steps to ensure their compliance by building a compliance framework that far exceeds minimum legal requirements. For companies operating in high-risk sectors like technology and finance, having a robust sanctions compliance program is not just a best practice; it is essential to avoid catastrophic financial and legal consequences. OFAC's enforcement guidelines function as both "stick" and "carrot," punishing those who violate sanctions while incentivizing those who prioritize compliance by building mature, well-documented compliance programs.[117] This dual approach reinforces sanctions as a core instrument of the U.S. cyber strategy

110. *The Seven Largest Sanctions-Related Fines Against Banks*, AM. BANKER (last updated Jan. 16, 2017), https://perma.cc/GZ4T-FGR6.

111. *Customer Due Diligence (CDD) and Know Your Customer (KYC) Explained*, COMPFIDUS (Sep. 24, 2024), https://perma.cc/6YG2-V4KS.

112. RANSOMWARE ADVISORY, *supra* note 39, at 3.

113. Economic Sanctions Enforcement Guidelines, 74 Fed. Reg. 57593 (Nov. 9, 2009) [hereinafter Economic Sanctions Enforcement Guidelines].

114. *Id.* at 57602.

115. *Id.*

116. U.S. DEP'T OF THE TREASURY, OFF. OF FOREIGN ASSET CONTROL, A FRAMEWORK FOR OFAC COMPLIANCE COMMITMENTS (2019), https://ofac.treasury.gov/media/16331/download?inline.

117. Eric A. Sohn, *Carrots and Sticks. . .and Sanctions*, ACAMS TODAY (Sep. 19, 2017), https://perma.cc/J2UF-GCPS.

and strengthens the integrity of the international financial system. To ensure that both public- and private-sectors remain apprised of evolving threats, Treasury supplemented its regulatory and enforcement network with targeted advisories designed to communicate real-time, sector-specific cyber and sanctions risks.

B. Treasury Issues Multiple Cyber-Related Sanctions Advisories

1. Treasury's Initial Ransomware Payments Advisory Unmasking How U.S. Sanctions Target Hackers and Their Accomplices

As ransomware and other forms of cybercrime have surged in scale, sophistication, and geopolitical impact, Treasury has recognized that an effective sanctions regime requires proactive guidance, and not merely punitive action. Treasury therefore issued its first ransomware payments advisory, alerting financial institutions (including depository institutions and money service businesses), insurers, and digital forensics and incident response firms to the sanctions' risks associated with facilitating ransom payments to malicious cyber actors.[118] The scope of U.S. cyber-related sanctions extends well beyond the perpetrators themselves to ensnare those who assist, enable, or derive benefit from their operations.[119] The advisory further clarifies that sanctions liability is not confined to direct dealings. Rather, it also includes any transaction by a non-U.S. person that "causes" a U.S. person to violate sanctions; consequently, the assets of non-U.S. persons are on the hook too.[120] For example, a non-U.S. person facilitating a payment through the U.S. financial system to a sanctioned party might find itself under fire from OFAC enforcement as well.[121]

However, per the advisory, the regulations do not stop there. Beyond these baseline prohibitions, OFAC's facilitation doctrine sharply limits the activities of U.S. persons operating abroad. Under this doctrine, U.S. persons, wherever they are located, are prohibited from facilitating actions of non-U.S. persons in activities that would otherwise be prohibited for U.S. actors under U.S. sanctions.[122] Therefore, U.S. persons may not approve, finance, guarantee, or otherwise support transactions by non-U.S. persons that U.S. persons themselves could not

118. RANSOMWARE ADVISORY, *supra* note 39.

119. *See, e.g.*, Jason Bartlett & Megan Ophel, *Sanctions by the Numbers: Spotlight on Cyber Sanctions*, CTR. FOR A NEW AM. SEC. (May 4, 2021), https://perma.cc/3ZHA-WHTF; *Cyber Related Sanctions*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL, https://perma.cc/9CPX-PN59; TWEA, *supra* note 39; IEEPA, *supra* note 29; Exec. Order No. 13,694, *supra* note 37, §§ 1(a)-(b), 3, 5; 31 C.F.R. § 578.201; RANSOMWARE ADVISORY, *supra* note 39; SANCTIONS OVERVIEW, *supra* note 39, at 4.

120. *Frequently Asked Questions 9*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Sep. 10, 2002), https://perma.cc/A5XD-9FXP.

121. *Frequently Asked Questions 980*, U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL (Feb. 24, 2022), https://perma.cc/6QEG-ZKHH.

122. RANSOMWARE ADVISORY, *supra* note 39, at 3; *see* Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.208 ("Except as otherwise authorized pursuant to this part . . . no United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited by this part if performed by a United States person or within the United States.").

lawfully undertake.[123] This is particularly significant in the ransomware context, where intermediaries such as financial institutions, insurers, digital forensics teams, and incident response firms may become enforcement targets themselves for violating U.S. sanctions when they enable ransom payments to sanctioned cyber actors.[124] Thus, the advisory warned that even financial service companies such as depository institutions and money service businesses that may be involved in processing ransomware payments to sanctioned cyber actors could face strict liability exposure under U.S. sanctions.[125]

The advisory further states that U.S. cyber sanctions do not only focus on hackers; they also target those who knowingly *benefit from* stolen trade secrets or other cyber-derived assets.[126] A sanctions designation not only freezes assets of sanctioned parties but also serves as a powerful market warning to U.S. persons and businesses that have not been designated by OFAC, putting them on notice that they should not transact with any parties named under Executive Order 13,694.[127] This produces a chilling effect far beyond the designated actor, prompting businesses to reevaluate their supply chains and business relationships, fearing that the unknown risk of a potential misstep of transacting with a sanctions target could land them in OFAC's crosshairs. The uncertainty itself is a weapon of sanctions itself: companies may avoid wide swaths of suppliers or potential partners, even preemptively severing ties with entire sectors or certain jurisdictions, choosing to avoid the risk of becoming entangled with a person or company who may be the target of U.S. sanctions, and thus a potential sanctions enforcement action. This tactic is more popularly known as "derisking":

> [The] Order may cause businesses to more closely examine their supply chains for entities that benefit from stolen trade secrets and to avoid relationships with entities that are or even might become subject to U.S. sanctions. In fact, ambiguity about how exactly the Order will be applied could contribute to its deterrent effect if the uncertainty causes businesses to avoid large swaths of suppliers as a prophylactic measure than they would if they could confidently predict who would be sanctioned. If the Order makes business more difficult and less profitable for entities that benefit from stolen intellectual property, it will have accomplished at least part of its goal of decreasing the rewards of crime.[128]

123. Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.208.

124. RANSOMWARE ADVISORY, *supra* note 39, at 3–4.

125. *Id.*

126. Exec. Order No. 13,694, *supra* note 37, § 1(a)(ii)(A).

127. *On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"*, WHITE HOUSE (Apr. 1, 2015), https://perma.cc/ZBT9-PDH2.

128. *See Cyber Order: What Will It Do and Will It Work*, *supra* note 71.

Consequently, where firms cannot confidently predict which actors may become sanctioned, they often withdraw from entire sectors or regions as a prophylactic measure.

This broad-reaching impact delivers a powerful deterrent. The advisory thus crystallized a core tenet of U.S. cyber strategy: sanctions are aimed not only at the hackers themselves, but at the financial, logistical, and commercial networks that sustain them, including anyone who enables, facilitates, or profits from their operations.

The accelerating pace, severity, and sophistication of ransomware attacks revealed that this initial advisory, while groundbreaking, was insufficient. Treasury thus needed to issue more targeted, sector-specific, and forceful guidance to keep pace with the evolving threat landscape, which it did in the following years.

2. Treasury's Updated Ransomware Payments Advisory

Treasury's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments ("Updated Advisory"), released by OFAC on September 21, 2021, builds on the foundations of the initial advisory regarding the legal and financial risks associated with ransomware payments.[129] It was issued amid a dramatic escalation in ransomware attacks, particularly during the COVID-19 pandemic, that targeted critical infrastructure, health systems, financial institutions, and government agencies.[130] These attacks typically involve malicious actors encrypting data and demanding payments, often in virtual currency, in exchange for restoring access.

The Updated Advisory reiterates OFAC's longstanding position that facilitating ransomware payments, including through financial institutions, cyber insurers, and incident-response firms such as digital forensics providers, may violate U.S. sanctions when such payments involve sanctioned actors, jurisdictions, or virtual-currency intermediaries.[131] In this Updated Advisory, the U.S. government strongly discourages the payment of ransom, underscoring that such payments not only embolden criminal organizations but may also finance other illicit activities posing acute national security risks and result in severe penalties.[132] The advisory names several sanctioned ransomware facilitators, including North Korea's Lazarus Group which was responsible for the WannaCry attack, Russia-based Evil Corp. which was behind the Dridex malware attack, and the virtual currency exchange SUEX OTC which laundered ransomware proceeds, as emblematic threats.[133]

---

129. RANSOMWARE ADVISORY, *supra* note 39.

130. *Id.*

131. *Id.*

132. *Id.*

133. *See, e.g.*, Press Release, U.S. DEP'T OF THE TREASURY, Treasury Takes Robust Actions to Counter Ransomware (Sep. 21, 2021), https://perma.cc/SRK8-QCSK.

The Updated Advisory further reiterates OFAC's enforcement of sanctions violations under a strict liability standard, in which companies may face severe significant civil or criminal penalties even absent knowledge that a transaction involved a sanctioned person.[134] The advisory therefore places renewed emphasis on companies' implementation of comprehensive, risk-based sanctions compliance programs.[135] Such programs include enhanced cybersecurity defenses; offline data backups; rehearsed incident response plans; and timely self-reporting ransomware incidents to OFAC, FBI, Cybersecurity and Infrastructure Security Agency ("CISA"), and other relevant agencies.[136] In the advisory, OFAC emphasizes that cooperation, prompt reporting, and demonstrable compliance efforts may function as mitigating factors in potential enforcement actions.[137]

The Updated Advisory also adopts a restrictive posture toward licenses for ransomware payments, noting that license applications are generally reviewed with a presumption of denial given the strong public-policy interest in deterring future attacks.[138] This advisory serves as a critical reminder that ransomware payments implicate not only private financial risk but also U.S. national security, particularly when they enable adversaries engaged in nefarious activities such as weapons development, terrorism, or other broader destabilizing activities.[139] It is therefore essential that companies prioritize their cybersecurity resilience and sanctions compliance which are mutually reinforcing obligations that companies must integrate into their operational risk frameworks to safeguard both their financial interests and U.S. national security.[140] This sharpened, sanctions-forward approach to ransomware set the stage for Treasury's broader international efforts to address state-sponsored cyber threats, nowhere more urgently than in the case of North Korea.

3. Treasury's North Korea Cyber Threat Advisory: A Global Call to Action

North Korea's malicious cyber activities, intensifying in the years following the Sony attack, have evolved into one of the most significant and destabilizing threats to the international financial system. Recognizing that Pyongyang's cyber capabilities had rapidly matured into a core instrument of state power, the U.S. Departments of State, Treasury, and Homeland Security, together with the FBI, issued an unprecedented joint advisory in April 2020, detailing the existential threat posed by North Korea's rapidly advancing malicious cyber capabilities.[141] The advisory functioned not only as a comprehensive assessment of North

134. RANSOMWARE ADVISORY, *supra* note 39.
135. *Id.*
136. *Id.*
137. *See* Economic Sanctions Enforcement Guidelines, *supra* note 113.
138. RANSOMWARE ADVISORY, *supra* note 39, at 4.
139. *Id.*
140. *Id.*
141. *See generally* DPRK CYBER THREAT ADVISORY, *supra* note 31.

Korea's rapidly maturing cyber apparatus but also as a strategic roadmap for a coordinated global response to counter the North Korean cyber threat.[142]

The advisory outlines North Korea's deployment of increasingly sophisticated tactics, executed by teams of hackers, cryptologists, and software developers, to generate illicit revenue for the regime in defiance of U.S. and U.N. sanctions.[143] These operations include:

- **Cyber-enabled financial theft and money laundering**, including attempted thefts totaling an estimated $2 billion, documented by the U.N. 1718 Panel of Experts, and cryptocurrency heists described in DOJ filings[144];
- **Ransomware campaigns**, in which North Korean actors both extort victims and masquerade as "consultants" selling pseudo-protection services[145]; and
- **Cryptojacking**, using malware to hijack computing resources to mine cryptocurrency covertly.[146]

The advisory notes that under sustained international pressure, Pyongyang has turned to cybercrime as a principal means of funding its weapons of mass destruction and ballistic missile programs.[147] Referring to these operations collectively as HIDDEN COBRA, the U.S. government has warned that they target financial institutions and cryptocurrency exchanges worldwide, threatening the stability of both the U.S. and international financial system.[148] North Korea's actions have also blatantly disregarded core international norms, positioning itself as a rogue state actor in stark opposition to the rules-based international order of acceptable responsible state behavior in cyberspace.[149]

The advisory cites the condemnation of North Korea's destabilizing cyber activities by a coalition of U.S. allies, including the United Kingdom, Australia,

142. *Id.* at 1.

143. *Id.*

144. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 2; Mid-Term Rep. of the 1718 Comm. Panel of Experts on the Democratic People's Republic of Korea, ¶ 57, U.N. Doc. S/2019/691 (Aug. 30, 2019), https://perma.cc/DLU2-KXV4 [hereinafter 2019 U.N. POE Report] (describing how North Korean state sponsored hackers targeted global financial institutions and laundered stolen funds through complex international networks; reporting the Panel's estimate that the DPRK attempted to steal as much as $2 billion through illicit cyber operations; and corroborating these findings with a 2020 Department of Justice complaint detailing the theft of hundreds of millions of dollars in cryptocurrency stolen and laundered from multiple exchanges through several jurisdictions).

145. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 2 (describing DPRK ransomware campaigns against third country victims, including extortion schemes demanding payments to restore compromised systems; in some cases, involving fraudulent consulting services purportedly guaranteeing protection from future attacks).

146. *Id.*

147. *Id.* at 1.

148. *Id.*

149. *Id.*

Canada, New Zealand, Denmark, and Japan, which attributed the WannaCry 2.0 ransomware attack to North Korea.[150] The joint attribution, one of the most significant multilateral responses to a state-sponsored cyberattack, underscored both the scale of the threat and the necessity of collective action. It also marked a critical step toward collective international norm-setting in cyberspace, signaling a willingness among like-minded states to publicly call out Pyongyang's cyber aggression and hold North Korea accountable.[151]

Recognizing that North Korea's cyber activities represent a global threat with implications extending beyond the United States, the advisory urges governments, private industry, and civil society to adopt concrete measures to:

- Raise awareness of the North Korea cyber threat and strengthen preventative and risk mitigation strategies.[152]
- Promote international exchanges of cyber tactics, threat intelligence, and best practices.[153]
- Implement robust cybersecurity measures, including network segmentation, regular data backups, and cyber incident response plans.[154]
- Enhance anti-money laundering, countering the financing of terrorism, and counter-proliferation financing controls.[155]

150. *Id.*; *see also White House WannaCry Attribution*, *supra* note 34.

151. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 1; *White House WannaCry Attribution*, *supra* note 34.

152. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 5.

153. *Id.* at 9 (noting that the advisory references CISA, which permits non-federal entities to share cyber threat indicators and defensive measures related to HIDDEN COBRA with both federal and non-federal entities); Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 [hereinafter CISA].

154. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 5, Annex I (U.S. government resources for countering the DPRK cyber threat); *see also Cybersecurity Capability Maturity Model (C2M2)*, U.S. DEP'T OF ENERGY, https://perma.cc/UR9D-D29P; *Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH., https://perma.cc/YMN5-A7QB (providing guidance on developing and implementing robust cybersecurity practices). *See also* CYBERSECURITY INFRASTRUCTURE SEC. AGENCY, https://perma.cc/4DRS-MH5V (providing technical alerts, malware analysis reports, and other resources to enable network defenders to identify and reduce exposure to malicious cyber activities).

155. CISA, *supra* note 153; *see* FINANCIAL ACTION TASK FORCE, THE FATF RECOMMENDATIONS (2025), https://perma.cc/GZ73-9D3M; *High-Risk Jurisdictions Subject to a Call for Action*, FINANCIAL ACTION TASK FORCE (Feb. 21, 2025), https://perma.cc/HR2S-8V63; DPRK CYBER THREAT ADVISORY, *supra* note 31, at 6 (recommending that U.S. financial institutions and other covered businesses and persons comply with the Bank Secrecy Act, as amended by the USA PATRIOT Act, and implementing regulations, by "developing and maintaining effective anti-money laundering programs designed to prevent the money service business from being used to facilitate money laundering and the financing of terrorist activities, as well as identifying and reporting suspicious transactions, including those conducted, affected, or facilitated by cyber events or illicit finance involving digital assets, in suspicious activity reporting to FinCEN.").

- Promptly report suspected North Korean cyber activity to law enforcement.[156]

Consistent with U.N. Security Council resolutions such as Resolution 2270, the advisory further encourages states to repatriate North Korean IT workers, terminate North Korean-affiliated ventures, and restrict the global access of North Korean banks.[157] It also emphasizes the severe consequences awaiting individuals and entities that enable or benefit from Pyongyang's cybercriminal networks.[158] The advisory emphasizes that violators risk asset freezes, travel bans, exclusion from U.S. financial systems, and potentially substantial fines and imprisonment.[159]

Ultimately, the advisory makes unmistakably clear that countering North Korea's malicious cyber operations requires coordinated action across nations, industries, and individuals.[160] High-profile international denunciations, such as the resounding global condemnation of the WannaCry attack, illustrate the growing international consensus that Pyongyang's cyber activities represent a systemic destabilizing threat requiring unified action by the global community.[161]

The advisory thus functions as both a warning and a call to action, urging the U.S. and international community to take concrete, actionable steps to defend against North Korean cyber threat.[162] The advisory also serves as an operational guide, compiling extensive U.S. government resources detailing North Korea's cyber activities and practical strategies for mitigating such risks.[163] It further directs the public to the U.N. 1718 Sanctions Committee's Panel of Experts reports, which provide in-depth analysis of North Korea's illicit activities and recommendations for strengthening global compliance.[164] Together, these materials equip governments, industries, and individuals with essential tools for understanding and managing the risks posed by North Korea's increasingly aggressive cyber strategy. They reaffirm that confronting Pyongyang's cyber activity transcends national boundaries and has therefore become a global priority.

156. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 5–6.

157. *Id.*; *see also* U.N. Doc. S/RES/2270, ¶ 14 (Mar. 2, 2016), https://perma.cc/AL4E-75MQ (describing Resolution 2270's repatriation mandates for North Korean nationals earning income abroad); *id.* ¶ 33 (noting the required closure of existing branches, subsidiaries, and representative offices of North Korean banks and the termination of correspondent relationships with North Korean banks).

158. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 7–8; *see* 2019 U.N. POE Report, *supra* note 144, at 4; U.N. Doc. S/RES/1718, ¶¶ 8(d), 11, 32 (Oct. 14, 2006), https://perma.cc/FAL2-ZPKM.

159. DPRK CYBER THREAT ADVISORY, *supra* note 31, at 7 (noting that foreign financial institutions that knowingly conduct or facilitate significant trade with North Korea or transactions on behalf of a person designated under a North Korea-related Executive Order risk losing their ability to maintain a correspondent or payable-through account in the United States).

160. *Id.* at 1.

161. *See, e.g.*, Gordon Corera, *Cyber-Attack: US and UK Blame North Korea for WannaCry*, BBC (Dec. 19, 2017), https://perma.cc/5M3T-WQDN.

162. DPRK CYBER THREAT ADVISORY, *supra* note 31.

163. *Id.* at 9.

164. 2019 U.N. POE Report, *supra* note 144, at 33.

IV. PRESENTING A UNITED FRONT AGAINST CYBER THREATS THROUGH A TREASURY-JUSTICE PARTNERSHIP

A. Treasury-Justice Alliance: Integrating Economic Statecraft and Criminal Enforcement

The modern fight against malicious cyber activity has revealed that no single agency possesses the statutory authorities, technical capabilities, visibility, or operational reach to respond effectively in isolation. The Treasury and Justice Departments have emerged as a powerful duo, each playing a vital role in detecting, deterring, and disrupting cyber threats. Treasury's OFAC brings unparalleled capacity to impose immediate economic costs, freeze assets, and isolate malicious actors from the global financial system. The Justice Department, by contrast, wields investigative tools, criminal enforcement powers, and norm-shaping prosecutorial strategies that expose, attribute, and penalize cybercriminals worldwide. Together, they form a critical frontline defense against the escalating wave of cyber threats, combining their strengths to deliver a potent and coordinated response.

Although undertheorized in legal scholarship, the Treasury-Justice partnership has become one of the most consequential developments in modern cyber governance. Together, the two agencies have developed one of the most powerful deterrent architectures in contemporary national security practice. When coordinated, DOJ's indictments provide a public evidentiary record that supports OFAC designations,[165] and OFAC's sanctions deprive adversaries of access to the financial networks that make cyber operations possible.[166]The result is a mutually reinforcing system that not only neutralizes immediate threats but also signals to foreign governments that state-linked cyber activity will trigger escalating and multi-dimensional costs.

High-profile enforcement actions, such as those involving BNP Paribas[167] and HSBC,[168] have demonstrated the potential of this powerful partnership. Yet the

165. Indictment, United States v. Besciokov, No. 1:25-CR-0039 (E.D. Va. Feb. 27, 2025), https://perma.cc/7BAH-UADT [hereinafter Besciokov Indictment]; Press Release, U.S. DEP'T OF JUST., Garantex Cryptocurrency Exchange Disrupted in International Operation (Mar. 7, 2025), https://perma.cc/2PNL-QR7L [hereinafter Garantex Press Release]; Treasury sanctions related to Salt Typhoon, *supra note* 165; Treasury sanctions related to Lazarus Group supra note 165; Indictment, U.S. v. Guan Tianfeng, No. 24-cr-00088 (N.D. Ind. Sep. 19, 2024) [hereinafter Tianfeng Indictment]; Indictment, U. S. v. Yin Kecheng and Zhou Shuai, No. 18-cr-00126 (D.D.C. Mar. 28, 2023) [hereinafter Kecheng and Zhou Inditment].

166. Besciokov Indictment, *supra note* 165; Garantex Press Release, *supra note* 165; Treasury sanctions related to Salt Typhoon, *supra note* 165; Treasury sanctions related to Lazarus Group supra note 165; Indictment, Guan Tianfeng Indictment, *supra* note 165; Kecheng and Zhou Indictment, *supra* note 165.

167. Press Release, U.S. DEP'T OF JUST., BNP Paribas Agrees to Plead Guilty and to Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to U.S. Economic Sanctions (June 30, 2014), https://perma.cc/9YB4-BWAN.

168. Press Release, U.S. DEP'T OF JUST., HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement (Dec. 11, 2012), https://perma.cc/7KPX-ZY8M.

partnership is not without limits: the Treasury Department has, for unknown reasons, declined to sanction all persons or entities indicted by the Justice Department for cybercrimes.[169] This divergence raises broader questions about evidentiary burdens, diplomatic considerations, and the Executive Branch's strategic approach toward malicious cyber activity, particularly, for instance, Chinese cyber-enabled theft.

By 2016, the Justice Department had explicitly embraced criminal prosecutions as a central deterrent tool against cyber actors and deepened its collaboration with OFAC to reinforce norms of responsible behavior in cyberspace.[170] The DOJ's 2018 Cyber Digital Task Force further underscored sanctions as a critical pillar of the U.S. cyber response. Working closely with Treasury, the Justice Department helped orchestrate targeted sanctions designations based on intelligence derived from its investigations, ensuring that cybercriminals face both the reputational and legal consequences of criminal charges and the financial incapacitation imposed by OFAC designations.[171] This framework has been deployed against a range of adversaries, including Russian cybercriminal syndicates, Iranian state-sponsored hackers, North Korean money launderers, and China-linked facilitators. In each instance, joint action has struck malign actors "where it hurts most."[172]

The following examples highlight how coordinated Treasury–Justice actions have disrupted cyber-enabled threats orchestrated by proxies of hostile foreign governments: Beginning in 2015, the Russian cybercrime syndicate Evil Corp. deployed Dridex malware to harvest banking login credentials from hundreds of financial institutions in more than forty countries, resulting in over $100 million in stolen funds and millions more in damages to U.S. and global financial institutions and their customers.[173] OFAC responded in December 2019 by designating Evil Corp. and its leader, Maksim Yakubets, as an SDN,[174] while the Justice Department simultaneously unsealed charges against Yakubets and another Evil Corp. member for conspiracy, bank fraud, wire fraud, and computer damage.[175] The combined actions ensured this Russian cybercrime ring faced legal and financial consequences on multiple fronts.

---

169. Indictment, U.S. v. Wang, No. 19-cr-00153 (E.D. Va. May 7, 2019) [hereinafter Wang Indictment]; Press Release, U.S. DEP'T OF JUSTICE, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), https://perma.cc/45MS-PDEH.

170. Benjamin Wittes, *John Carlin on "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats"*, LAWFARE (June 21, 2016), https://perma.cc/3KGX-S9U6.

171. U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 74 (July 2, 2018), https://perma.cc/27BH-DG77.

172. *Id.*

173. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Evil Corp, The Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), https://perma.cc/FZ5W-R5YS.

174. *Id.*

175. Press Release, U.S. DEP'T OF JUST., Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware (Dec. 5, 2019), https://perma.cc/NST7-D3DJ.

In a high-profile case involving Iran, in March 2018, the Justice Department charged nine Iranian nationals tied to Iran's Mabna Institute for a massive hacking campaign targeting more than 300 universities worldwide and stealing an estimated 31 terabytes of proprietary data.[176] The charges alone effectively curtailed the defendants' travel outside Iran without risking arrest. That same day, Treasury's OFAC, capitalizing on the DOJ's actions, sanctioned the Institute and its members for "engaging in malicious cyber-enabled activities related to the significant misappropriation of economic resources or personal identifiers for private financial gain," under Executive Order 13,694.[177] Once again, this synchronized legal and financial crackdown sent a powerful message about the consequences of state-backed cyber espionage.

In another scheme involving Iran in November 2018, a federal grand jury indicted two Iranian nationals for deploying the SamSam ransomware over a 34-month period that extorted more than $6 million from hospitals, municipalities, and public institutions and caused over $30 million in losses.[178] The scheme relied on Bitcoin payments laundered through Iranian entities, illustrating how state-linked cyber actors increasingly exploit virtual currencies to obscure their financial footprints. Concurrently, OFAC took the first virtual asset–related action under its cyber sanctions authorities, Executive Order 13,694, as amended by Executive Order 13,757, by designating the two individuals as SDNs for providing material support to malicious cyber activities.[179] OFAC traced Bitcoin addresses linked to the two individuals that were associated with more than 7,000 transactions worth millions of dollars, marking a significant moment in Treasury's efforts to penetrate anonymized digital currency networks.[180] Through this action, OFAC signaled that it would "aggressively pursue Iran and other

176. Indictment, U.S. v. Rafatnejad, No. 18-CR-94 (Mar. 23, 2018); Press Release, U.S. DEP'T OF JUST., Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps (Mar. 23, 2018), https://perma.cc/XV7M-XTAK; Press Release, U.S. DEP'T OF JUST., Deputy Assistant Attorney General Adam Hickey of the National Security Division Delivers Remarks at CyberNext DC (Oct. 4, 2018), https://perma.cc/5FQX-MT5G.

177. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities (Mar. 23, 2018), https://perma.cc/Z47N-ZBLG.

178. Indictment, U.S. v. Savandi & Mansouri, 18-CR-704 (BRM) (Nov. 26, 2018), https://perma.cc/25Q7-J6TP; Press Release, U.S. DEP'T OF JUST., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://perma.cc/K2JG-YY8Q; Press Release, U.S. DEP'T OF THE TREASURY, Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://perma.cc/4EB4-RBCK (describing the U.S. Department of Justice's charges against the two Iranian nationals for conspiracy, wire fraud, and intentional damage to protected computers arising from the SamSam ransomware campaign); *see also SamSam Ransomware*, CYBERSECURITY INFRASTRUCTURE SEC. AGENCY (Dec. 3, 2018), https://perma.cc/4JF4-5B8F; FED. BUREAU OF INVESTIGATION, *Ransomware Suspects Indicted: Iranian Men Charged with Deploying Damaging SamSam Ransomware* (Nov. 28, 2018), https://perma.cc/JHD8-E8PB.

179. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), https://perma.cc/6SXQ-VJU6.

180. *Id.*

rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards," while urging exchanges, peer-to-peer platforms, and other virtual asset service providers to strengthen their compliance controls.[181] Taken together, these enforcement actions underscored the strength of the coordinated U.S. government response by DOJ and OFAC to counter state-sponsored cybercrime and the exploitation of digital currencies for illicit financial activities. They also signaled that the use of virtual currencies would not shield cybercriminals from U.S. enforcement.

And finally in a joint Treasury–Justice action, in March 2020, OFAC sanctioned two Chinese nationals for laundering more than $100 million in cryptocurrency stolen by North Korean operatives as part of Pyongyang's broader cyber-heist program.[182] The Justice Department simultaneously announced criminal charges against these two Chinese nationals for money laundering and operating an unlicensed money-transmitting business and later pursued forfeiture of 280 virtual currency accounts tied to the scheme.[183] These actions illustrated the agility of joint enforcement in the rapidly evolving digital-assets ecosystem.

B. Fault Lines in Chinese Enforcement: When DOJ Indicts, But Treasury Declines to Sanction

Despite the benefits of this coordinated enforcement effort, the Treasury–Justice partnership has not functioned seamlessly across all geopolitical contexts. Notably, OFAC has, for reasons not publicly known, declined to impose sanctions in certain circumstances, even when the Justice Department has pursued criminal charges and the factual record appeared sufficient to support designation under Executive Order 13,694. For example, in 2019, the Justice Department indicted a member of a Chinese hacking group responsible for stealing the personal data of 78 million Americans from health insurer, Anthem, Inc., and other companies, yet in that scenario OFAC did not issue parallel sanctions.[184] Similarly, in July 2020, the Justice Department charged Chinese nationals, Li Xiaoyu and Dong Jiazhi, for a decade-long hacking campaign, including intrusions targeting COVID-19 vaccine research, but yet again OFAC did not sanction these individuals.[185] Assistant Attorney General John C. Demers publicly warned

181. *Id.*

182. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), https://perma.cc/VB3H-8NCV.

183. Press Release, U.S. DEP'T OF JUST., Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack (Mar. 2, 2020), https://perma.cc/Q2YK-G2CG.

184. *See* Wang Indictment, *supra* note 169; Press Release, U.S. DEP'T OF JUST., Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), https://perma.cc/E9X5-GH93.

185. Indictment, U.S. v. Xiaoyu, No. 20-cr-06019 (E.D. Wash. July 7, 2020) [hereinafter Two Chinese Hackers 2020 Indictment]; Press Release, U.S. DEP'T OF JUST., Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 20, 2020), https://perma.cc/5QPJ-E8XW [hereinafter Two Chinese Hackers 2020 Press Release]; Brian

that China had joined Russia, Iran, and North Korea as a "safe haven" for cybercriminals—nonetheless, Treasury remained silent in these scenarios.[186]

This pattern echoes OFAC's earlier refusal to sanction the Chinese hackers responsible for the Equifax breach affecting nearly 150 million Americans, even though the Justice Department had unsealed indictments related to the breach.[187] While the reasons may be speculatively rooted in diplomatic sensitivity, evidentiary considerations, or broader strategic calculation, the gap between DOJ prosecutions and Treasury sanctions in these particular Chinese-related cases raises questions about the coherence and credibility of the U.S. cyber deterrence framework.

Notwithstanding these limitations, the growing cooperation between the Treasury and Justice Departments in tackling cyber threats represents one of the most significant developments in the evolution of U.S. cyber statecraft. Their coordinated use of sanctions and criminal prosecutions has produced a robust model for attributing cyber operations, imposing real costs on state-sponsored and criminal networks, disrupting financial and technical infrastructure, and shaping international norms of responsible behavior in cyberspace. Whether that model can mature into effective deterrence will depend on its consistency, severity, and sustained application across adversaries. As cyber threats increase in sophistication and complexity, the effectiveness of this partnership and its ability to operate consistently across all adversaries will remain central to the United States' broader strategy for defending the digital domain.

Taken together, these developments underscore both the promise and the fragility of the Treasury–Justice enforcement model. The question that follows is how this architecture has fared amid the transition from the Biden Administration to the second Trump Administration, particularly as each administration reshaped the legal authorities, institutional structures, and strategic priorities governing U.S. cyber sanctions.

V. THE BIDEN FAREWELL EXECUTIVE ORDERS DEFENDING THE UNITED STATES AGAINST CYBER THREATS

In the final days of his presidency, on January 16, 2025, President Biden issued Executive Order 14,144, Strengthening and Promoting Innovation in the Nation's Cybersecurity.[188] The Order represents President Biden's effort to reinforce the federal cyber sanctions architecture first established a decade earlier in Executive Order 13,694 (2015), and subsequently expanded through Executive Orders

Barrett, *How China's Elite APT10 Hackers Stole the World's Secrets*, WIRED (Dec. 20, 2018), https://perma.cc/EM3X-4WJE.

186. *See* Two Chinese Hackers 2020 Indictment, *supra* note 185; Two Chinese Hackers 2020 Press Release, *supra* note 185.

187. Press Release, U.S. DEP'T OF JUST., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage, and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://perma.cc/EN29-HJKW.

188. Exec. Order No. 14,144, 90 Fed. Reg. 6755 (Jan. 17, 2025) [hereinafter Exec. Order No. 14,144].

13,757 (2016) and 13,984 (2021).[189] Those foundational Orders declared that foreign malicious cyber-enabled activities constitute an "unusual and extraordinary threat" to the national security, foreign policy, and economic stability of the United States, thus activating the President's emergency authorities under IEEPA.

Building upon this foundation, President Biden's Executive Order 14,144 modernizes and significantly expands the federal government's ability to disrupt, penalize, and impose costs on foreign-directed cyber operations, while strengthening the institutional foundation for long-term cyber deterrence. The Order broadens the categories of sanctionable conduct under Executive Order 13,694, as amended by Executive Order 13,757, while strengthening the Treasury Department's authority under IEEPA to impose costs on malicious cyber actors.[190] It expressly targets ransomware campaigns, unauthorized access to critical infrastructure, cyber-enabled espionage, data theft, sanctions evasion, and other malicious cyber activities conducted by, for, or on behalf of foreign governments and their proxies against the United States and its allies.[191] In doing so, the Order updates the cyber sanctions framework to reflect the modern threat landscape and the national security challenges of the digital era.

To address these evolving threats, Executive Order 14,144 substantially enhances Treasury's authority under IEEPA by authorizing the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose blocking sanctions on any foreign person determined to be "responsible for or complicit in," or to have "engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States," where those activities are "reasonably likely to result in, or have materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States."[192]

The Order also materially expands the scope of sanctionable conduct established under Executive Order 13,694. Most notably, it creates new categories of sanctionable conduct addressing ransomware attacks and unauthorized computer intrusions while replacing the former reference to the theft of "trade secret" with a significantly broader description of misappropriated assets. These revisions recognize that modern cyber operations increasingly target a wide range of valuable digital assets, including financial information, personal identifiers, proprietary

189. Exec. Order No. 13,984, Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 86 Fed. Reg. 6837 (Jan. 25, 2021) (explaining that the order expands the framework established in Executive Order No. 13,694, as amended, by requiring U.S. IaaS providers to implement enhanced identity-verification and record-keeping measures for foreign users; authorizing the Secretary of Commerce to impose special measures on high-risk foreign jurisdictions and actors using U.S. infrastructure for malicious cyber activity; and encouraging voluntary information sharing between the IaaS sector and federal agencies to strengthen national cybersecurity and mitigate foreign cyber threats).

190. Exec. Order No. 14,144, *supra* note 188.

191. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(ii).

192. *Id.*

business information, and intellectual property, rather than traditional trade secrets alone.

Under the Executive Order 14,144, the following categories of cyber-enabled activity are sanctionable when undertaken with the specified purpose or effect of:

> (A) harming, or otherwise compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
>
> (B) compromising the provision of services by one or more entities in a critical infrastructure sector;
>
> (C) disrupting the availability of a computer or network of computers or *compromising the integrity of the information stored on a computer or network of computers*; [193]
>
> (D) causing a misappropriation of *funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information* for commercial or competitive advantage or private financial gain;[194]
>
> (E) tampering with, altering, or causing a misappropriation of information with the purpose of or that involves interfering with or undermining election processes or institutions; or
>
> (F) *engaging in a ransomware attack, such as extortion through malicious use of code, encryption, or other activity to affect the confidentiality, integrity, or availability of data or a computer or network of computers, against a United States person, the United States, a United States ally or partner or a citizen, national, or entity organized under the laws thereof.*[195]

These amendments reflect a fundamental evolution in the federal government's understanding of the cyber threat environment. Subparagraph (C) expands the sanctions framework beyond attacks on critical infrastructure by reaching unauthorized computer intrusions that disrupt system availability or compromise data integrity, thereby capturing a broader range of malicious cyber operations that may not immediately affect critical infrastructure but nonetheless threaten national security. Subparagraph (D) similarly modernizes the framework by replacing the narrow reference to "trade secrets" with a comprehensive description of stolen digital assets, recognizing that contemporary cyber actors increasingly target financial information, personal identifiers, proprietary business

193. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(ii)(C) (*emphasis added*).
194. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(ii)(D) (*emphasis added*).
195. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(ii)(F) (*emphasis added*).

information, and other valuable data rather than traditional industrial secrets alone. The addition of subparagraph (F) expressly incorporates ransomware into the cyber sanctions regime for the first time, reflecting the Administration's recognition that ransomware has evolved from a predominantly criminal enterprise into a significant national security threat capable of disrupting hospitals, energy infrastructure, financial institutions, and government services. Collectively, these amendments shift the focus of Executive Order 13,694 from combating discrete acts of cyber-enabled economic espionage toward addressing the broader ecosystem of malicious cyber activity, including ransomware, destructive intrusions, and the theft of a wide range of digital assets.

Executive Order 14,144 also expands secondary forms of sanctionable conduct by authorizing sanctions against any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, "to be responsible for or complicit in, or to have engaged in, directly or indirectly," in:

> (A) the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of *funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information* misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such *funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information*,[196] or
>
> *(B) activities related to gaining or attempting to gain unauthorized access to a computer or network of computers of a United States person, the United States, a United States ally or partner or a citizen, national, or entity organized under the laws thereof, where such efforts originate from or are directed by persons located, in whole or substantial part, outside the United States,*[197]

provided that such activities are "reasonably likely to result in, or have materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States."[198]

These additional provisions are equally significant because they extend sanctions liability beyond the perpetrators of cyber intrusions to encompass those who knowingly benefit from or facilitate cyber-enabled theft. Subparagraph (A) targets individuals and entities that knowingly receive or exploit misappropriated information or assets for commercial or financial advantage, thereby disrupting the economic incentives that sustain cyber-enabled espionage and theft.

196. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(iii)(A) (*emphasis added*).
197. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(iii)(B) (*emphasis added*).
198. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(iii)(A-B).

Subparagraph (B) likewise authorizes sanctions against those responsible for unauthorized computer intrusions themselves, even before stolen information is exploited commercially. By authorizing sanctions throughout this ecosystem, Executive Order 14,144 substantially increases Treasury's ability to impose economic costs not only on the individuals conducting cyber operations, but also on those who knowingly profit from their illicit activities.

Collectively, these amendments substantially broaden the scope of sanctionable cyber-enabled conduct. Rather than focusing primarily on cyber-enabled economic espionage and the theft of trade secrets, the revised framework encompasses ransomware operations, unauthorized computer intrusions, a broader range of stolen digital assets, and those who knowingly exploit the proceeds of cyber-enabled theft.[199] The amendments reflect a more comprehensive sanctions regime capable of targeting the full ecosystem of malicious cyber activities, from the perpetrators of cyber intrusion to the individuals and entities that knowingly facilitate or profit from them.

Moreover, Executive Order 14,144 expands secondary sanctions exposure. It allows Treasury to designate individuals or entities that materially assist, sponsor, or provide financial, technological, or other support for malicious cyber activities, including those who own or control, or are acting for or on behalf of, a designated person.[200] It also expressly extends potential liability to leaders, officials, senior executives, and board members of designated entities.[201] By expanding the class of sanctionable actors in this manner, the Order strengthens the deterrent reach of the cyber-sanctions framework by targeting the organizational and governance structures that enable or facilitate state-sponsored and transnational cyber operations, and not merely the direct perpetrators. As a result, Executive Order 14,144 strengthens the U.S. government's ability to impose meaningful costs on, not only the direct perpetrators of cybercrimes, but those foreign actors supporting or profiting from the cyber-enabled attacks, reinforcing the national security and economic stability of the U.S. and its allies.[202]

By modernizing the sanctions regime to reflect current threats, the Order reaffirms the United States' commitment to defending its national and global interests in an increasingly contested and hostile digital landscape. It also positions an updated, more expansive, and strategically calibrated sanctions regime as an enduring pillar of U.S. cyber statecraft at a moment of transition between administrations.

199. *Id.*
200. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(iii)(C–E).
201. *Id.* § 9, amending Exec. Order No. 13694 § (1)(a)(iii)(F).
202. *Id.* § 9.

VI. TRUMP 2.0: CONTINUITY, DIVERGENCE, AND THE STRUCTURAL FRAGILITY OF THE U.S. CYBER DETERRENCE ARCHITECTURE

The first year of the second Trump Administration presents a complex, and in several respects contradictory picture of U.S. cyber statecraft. On one hand, the Administration has preserved the core operational elements of the integrated sanctions–prosecutions–diplomacy framework that emerged after the Sony Pictures Entertainment attack and matured during the Biden Administration. On the other hand, it has simultaneously weakened the institutional infrastructure necessary to sustain that framework, prompting what the Cyberspace Solarium Commission ("CSC or Commission") describes as the first measurable regression in the nation's whole-of-government cyber architecture since Congress established the Commission in 2019.[203] This tension is particularly striking because the Administration's 2025 National Security Strategy expressly embraces the strategic importance of cyber capabilities,[204] while, as this Part demonstrates, many of the institutional mechanisms needed to implement that strategy have been diminished in practice. This has resulted in a cyber strategy characterized by operational continuity but institutional erosion, the long-term strategic consequences of which remain uncertain.

A. A Bipartisan Consensus on Cyber Statecraft: Continuity Across the Biden and Trump Administrations in Countering Transnational Cyber-Criminal Networks

Successive administrations have converged on a shared premise: transnational cyber-criminal networks pose a national security threat that demands an integrated sanctions–prosecutions–diplomatic strategy. This continuity is unmistakably evident when examining the closing months of the Biden Administration and the opening phase of President Trump's second term. The handoff between administrations did not disrupt U.S. cyber-sanctions policy; rather, it reinforced it. As the Biden team exited and the Trump Administration took office, both pursued a consistent strategic approach to malicious cyber actors, particularly those tied to the People's Republic of China. This continuity mirrors the assessment of the Office of the Director of National Intelligence's 2024 Annual Threat Assessment, which identified Chinese state-sponsored cyber activity among the most consequential threats to U.S. national security.[205] In practice, the final months of the Biden Administration and the early months of Trump's second term featured a series of harmonized sanctions designations, criminal indictments, and joint diplomatic actions aimed at disrupting foreign cyber operations.

---

203. *See* 2025 CSC REPORT, *supra* note 1.

204. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 21–22 (2025) ("[T]he U.S. Government's critical relationships with the American private sector help maintain surveillance of persistent threats to U.S. networks . . . enabl[ing] the U.S. Government's ability to conduct real-time discovery, attribution, and response (i.e., network defense and offensive cyber operations)").

205. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2024), https://perma.cc/Z3WX-X9ZC [hereinafter ODNI THREAT ASSESSMENT].

Rather than a shift in direction, the transition revealed a bipartisan consensus: countering global cyber threats requires persistent, mutually reinforcing use of economic statecraft, federal law enforcement authorities, and diplomatic engagement.

Nearing the end of the Biden Administration, in December 2024, the Department of Justice unsealed criminal charges against Guan Tianfeng, an employee of Sichuan Silence Information Technology Co. Ltd. ("Sichuan Silence"), a Chinese state-linked cybersecurity contractor.[206] The charges allege that Guan exploited a previously unknown "zero-day" vulnerability[207] in firewall devices developed by the UK-based cybersecurity firm Sophos Ltd. in 2020.[208] The intrusion compromised more than 81,000 systems worldwide, including those of a U.S. government agency.[209] On that same day, Treasury's OFAC imposed sanctions against Sichuan Silence and Guan for their roles in the 2020 compromise of tens of thousands of firewall devices worldwide under Executive Order 13,694, as amended. Many of the victims of this attack were U.S. critical infrastructure firms, highlighting the systemic risk posed by Chinese cyber operations.[210] These coordinated actions exemplify the integrated sanctions-and-prosecutions model described in Part IV of this Article.

The Trump Administration reinforced this continuity in U.S. cyber posture shortly after taking office.[211] In March 2025, Treasury's OFAC imposed sanctions against Zhou Shuai, a Shanghai-based cyber actor and data broker, along with his firm, Shanghai Heiying Information Technology Company, Limited ("Shanghai Heiying"), under Executive Order 13,694, as amended by Executive Order 14,144.[212] OFAC found that Zhou, who was working in concert with previously designated Yin Kecheng,[213] a Chinese state-sponsored cyber operative and

206. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Cybersecurity Company Involved in Compromise of Firewall Products and Attempted Ransomware Attacks (Dec. 10, 2024), https://perma.cc/QE86-PPPY.

207. What is a zero-day exploit? IBM, https://perma.cc/H2QZ-9JLT (The unknown or unaddressed vulnerability is referred to as a zero-day vulnerability or zero-day threat. "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.)

208. Indictment, U.S. v. Guan Tianfeng, No. 24-cr-00088 (N.D. Ind. Sep. 19, 2024); Press Release, U.S. DEP'T OF JUST., China-Based Hacker Charged for Conspiring to Develop and Deploy Malware that Exploited Tens of Thousands of Firewalls Worldwide (Dec. 10, 2024), https://perma.cc/77S6-9EVA.

209. I*d.*

210. *Id.*

211. *See* 2025 CSC REPORT, *supra* note 1, at 10; Press Release, U.S. DEP'T OF JUST., Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns (Mar. 5, 2025), https://perma.cc/JR4L-7A8A; Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks (Mar. 5, 2025), https://perma.cc/8VNT-LP7C [hereinafter China Based Hacker 2025 Press Release].

212. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks (Mar. 5, 2025), https://perma.cc/8VNT-LP7C; Press Statement, U.S. DEP'T OF STATE, Sanctions on China-Based Hacker and Data Broker (Mar. 5, 2025), https://perma.cc/F4YC-HTCL [hereinafter Sanctions on China-Based Hacker/Data Broker].

213. Yin Kecheng had previously been sanctioned by OFAC in January 2025 for his role in the compromise of the U.S. Treasury Department's network. Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise (Jan. 17, 2025), https://perma.cc/WY9C-3GKQ (announcing sanctions against Sichuan

former Shanghai Heiying employee, had illegally acquired, brokered, and sold sensitive stolen data from U.S. critical infrastructure networks across the technology, communications, defense, healthcare, and government sectors.[214] In a coordinated action, the Department of Justice simultaneously unsealed parallel indictments charging Zhou Shuai, Yin Kecheng, employees of the Chinese firm i-Soon, and two Chinese Ministry of Public Security officers with a series of hacking offenses targeting U.S. critical infrastructure sectors.[215] Consistent with the government's broader cyber deterrence strategy, the State Department and FBI also announced substantial financial rewards for information leading to the apprehension of these individuals. Taken together, these coordinated sanctions, indictments, and rewards reinforced Washington's commitment across administrations to disrupting state-linked foreign cyber threats through a unified economic and law enforcement posture.[216]

More recently, in October 2025, OFAC imposed sweeping sanctions on 146 targets within the Prince Group Transnational Criminal Organization ("Prince Group TCO"), a Cambodia-based network led by Chen Zhi that operates online investment scams targeting Americans and other victims worldwide.[217] The U.S. Department of Justice simultaneously unsealed an indictment in the Eastern District of New York charging Chen with running "pig butchering" cryptocurrency investment fraud schemes that generated billions of dollars in illicit proceeds from victims in the United States and around the world.[218] The DOJ also filed a civil forfeiture complaint seeking to seize approximately 127,271 bitcoin,

---

Juxinhe Network Technology Co., Ltd., a Sichuan-based cybersecurity company involved in the Salt Typhoon cyber group, which compromised the network infrastructure of several major U.S. telecommunication and internet service providers); Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Technology Company for Support to Malicious Cyber Group (Jan. 3, 2025), https://perma.cc/A836-MW3P (announcing sanctions against Integrity Technology Group, a Beijing-based cybersecurity company implicated in multiple computer intrusions publicly attributed to Flax Typhoon, a Chinese state-sponsored hacking group active since at least 2021 and targeting U.S. critical infrastructure sectors).

214. China Based Hacker 2025 Press Release, *supra* note 211.

215. Indictment, U. S. v. Yin Kecheng and Zhou Shuai, No. 18-cr-00126 (D.D.C. Mar. 28, 2023); Press Release, U.S. DEP'T OF JUST., Chinese Nationals with Ties to the PRC Government and "APT27" Charged in a Computer Hacking Campaign for Profit, Targeting Numerous U.S. Companies, Institutions, and Municipalities (Mar. 5, 2025), https://perma.cc/B4QE-PZ9H.

216. Sanctions on China-Based Hacker/Data Broker, *supra* note 212 (The Diplomatic Security Service's Rewards for Justice Program is offering up to $10 million for information on i-Soon, its employees, and the MPS officers engaged in the malicious cyber activities highlighted in the indictments. The State Department has also offered up to $2 million each for information leading to the arrests or convictions of Zhou Shuai and Yin Kecheng).

217. Press Release, U.S. DEP'T OF THE TREASURY, U.S. and UK Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia (Oct. 14, 2025), https://perma.cc/PK8Y-NG9E [hereinafter US/UK Action Targeting Southeast Asia Cybercriminal Networks]; Press Release, UK Foreign, Commonwealth, and Dev. Off., UK and US Take Joint Action to Disrupt Major Online Fraud Network (Oct. 14, 2025), https://perma.cc/JU7K-HL5Z (these measures were taken in close coordination with the United Kingdom's Foreign, Commonwealth, and Development Office ("FCDO"), which concurrently imposed sanctions on Prince Holding Group, Chen Zhi, and key associates).

218. Indictment, U.S. v. Chen Zhi, No. 25-cr-00312 (E.D.N.Y. Oct. 8, 2025) [hereinafter Chen Zhi Indictment]; Press Release, U.S. DEP'T OF JUST., Chairman of Prince Group Indicted for Operating

worth roughly $15 billion, that are proceeds and instrumentalities of the defendant's fraud and money laundering schemes, marking the largest forfeiture action in U.S. history.[219]

Complementing these actions, the U.S. Department of the Treasury's FinCEN[220] issued a final rule under section 311 of the USA PATRIOT Act severing Huione Group, Cambodia-based financial conglomerate, from the U.S. financial system.[221] FinCEN identified Huione Group as a "financial institution of primary money-laundering concern" for facilitating the laundering of proceeds from DPRK cyber heists and Southeast Asia TCO-linked virtual currency investment scams.[222] According to FinCEN's findings, between August 2021 and January 2025, Huione Group laundered at least $4 billion in illicit proceeds, including $37 million from DPRK cyber heists, $36 million from virtual currency investment scams, and $300 million from other cyber schemes.[223] As a result of its Section 311 designation, U.S. financial institutions are now prohibited from opening or maintaining correspondent accounts for or on behalf of Huione Group.[224] They are also required to take reasonable steps to ensure they do not process transactions through the correspondent accounts of foreign banking institutions in the United States that involve Huione Group.[225] Collectively, these restrictions effectively deny Huione Group indirect access to the U.S. financial system.[226]

These actions illustrate the U.S. government's sustained, coordinated, and multi-agency approach to countering cyber threats, employing a whole-of-government strategy that integrates sanctions, criminal enforcement, and financial incentives to safeguard U.S. national security, protect sensitive personal data, and defend critical infrastructure against China-based cyber actors. The Trump Administration has signaled its intent to continue utilizing all available policy tools, including economic, law enforcement, and diplomatic measures, to address the evolving cyber threat landscape posed by China and other hostile actors. Rather than signaling a shift in policy, the continuity of cyber sanctions and enforcement actions across the Biden and Trump administrations reflects a

Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes (Oct. 14, 2025), https://perma.cc/P6KQ-F65P [hereinafter Chen Zhi Indictment Press Release].

219. Chen Zhi Indictment, *supra* note 218; Chen Zhi Indictment Press Release, *supra* note 218.

220. *Mission*, U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, https://perma.cc/BY6V-YF3Q (FinCEN's mission is "to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.").

221. Press Release, U.S. DEP'T OF THE TREASURY, FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System (Oct. 15, 2025), https://perma.cc/LG3S-DUN7; *see* US/UK Action Targeting Southeast Asia Cybercriminal Networks, *supra* note 217.

222. US/UK Action Targeting Southeast Asia Cybercriminal Networks, *supra* note 217; *see* Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 48295 (Oct. 16, 2025).

223. US/UK Action Targeting Southeast Asia Cybercriminal Networks, *supra* note 217.

224. 31 C.F.R. § 1010.664 (2024).

225. *Id.*

226. *Id.*

bipartisan consensus on the use of economic statecraft, criminal enforcement, and diplomacy, to address cyber threats emanating from China and Southeast Asia in general.

B. Emerging Divergences in U.S. Cyber Statecraft: From Biden to Trump

1. Scaling Back Executive Order 13,694 and Shifting U.S. Posture to Russia

Despite substantial continuity in operations, meaningful divergences have emerged in U.S. cyber statecraft between the Biden and Trump Administrations. The most consequential legal change concerns the narrowing of the United States' primary cyber-sanctions authority, Executive Order 13,694. On June 6, 2025, President Trump issued Executive Order 14,306, amending Executive Order 13,694, to restrict its scope exclusively to "foreign persons."[227] Under the Obama- and Biden-era framework, cyber sanctions could be imposed on "any person," including U.S. persons who materially supported foreign malicious cyber activity.[228] The new restriction formally precludes sanctions use against domestic actors and purports to "clarify" that the order cannot be applied to election-related activities.[229] This change, while framed as a clarification, substantively narrows the U.S. government's sanctions toolkit and eliminates an authority used sparingly but effectively to disrupt American enablers of foreign cyber operations.

A second point of divergence lies in the Administration's posture toward Russia. Disregarding the Office of the Director of National Intelligence's 2024 Annual Threat Assessment, which identified Moscow as a persistent cyber threat to U.S. national security,[230] the Trump Administration has taken decisive steps to recalibrate U.S. policy toward Russia. Most prominently, on March 1, 2025, Secretary of Defense Pete Hegseth reportedly ordered U.S. Cyber Command to halt offensive cyber operations against Russian networks, a directive that would mark a departure from longstanding U.S. practice.[231] Although the Pentagon has

227. Exec. Order No. 14,306, 90 Fed. Reg. 24723 (June 11, 2025) [hereinafter Exec. Order No. 14,306]; *see* Benjamin A. Powell, Barry J. Hurewitz, Joshua A. Geltzer, Arianna Evers, Shervin Z. Taheran & Maria I. Kanevsky, *New Executive Order Modifies Cybersecurity Requirements to Be Imposed on Federal Contractors and Subcontractors*, WILMERHALE (June 13, 2025), https://perma.cc/K3HQ-QRU8 [hereinafter *WilmerHale Client Alert on EO 14,306*].

228. Exec. Order No. 14,306, *supra* note 227, § 3; *WilmerHale Client Alert on EO 14,306*, *supra* note 227.

229. *Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America*, WHITE HOUSE (June 6, 2025), https://perma.cc/JRM6-WYYY.

230. ODNI THREAT ASSESSMENT, *supra* note 205.

231. Ellan Nakashima & Joseph Menn, *As Trump Warms to Putin, U.S. Halts Offensive Cyber Operations Against Moscow*, WASH. POST (Mar. 1, 2025), https://perma.cc/Q8TB-GK59; Julian E. Barnes, David E. Sanger & Helen Cooper, *Hegseth Orders Pentagon to Stop Offensive Cyberoperations Against Russia*, N.Y. TIMES (Mar. 2, 2025), https://perma.cc/5EEL-HNTY; Colin Ahern & Mark Montgomery, *U.S. Digital Disarmament Gives Russia Free Rein in Cyberspace. Bad Idea*, WASH. POST (Mar. 3, 2025), https://perma.cc/4G9W-EN34; Jim Sciutto & Sean Lyngaas, *US Suspends Offensive Cyber Operations Against Russia, Senior US Official Says*, CNN (Mar. 3, 2025), https://perma.cc/324W-NCZZ; *US Vetoes Canada's G7 Proposal to Form a Task Force to Counter Russia's Shadow Fleet. Here's Why*, FIRSTPOST (Mar. 9, 2025), https://perma.cc/V3VJ-XSZA (The Trump Administration

publicly denied these reports,[232] the Administration's early signals suggest an unwillingness to treat Russia as a strategic cyber threat,[233] a shift that could undermine U.S. deterrence.[234] These developments place the Administration at odds with the prior U.S. policy, the broader U.S. intelligence community, and key allies, including Ukraine, all of whom continue to view Russian cyber operations as one of the foremost threats to national security, signaling a potential reorientation of U.S. cyber posture toward Russia. Notwithstanding these reports, the United States has continued to issue indictments and sanctions targeting Russian criminal networks.[235]

2. Gaps in America's Whole-of-Government Approach to Cyber Threats Under Trump, As Identified in the 2025 Solarium Commission Report

Although Congress and prior administrations have materially strengthened U.S. cyber resilience, the Cyberspace Solarium Commission's 2025 Annual Report offers a sobering conclusion that the federal whole-of-government architecture combatting malicious cyber activity has experienced its first measurable regression since the Commission's establishment in 2019, marking "a substantial reversal of the advances made in previous years."[236] This reversal suggests that institutional reform in cyberspace remains susceptible to underinvestment, budgetary reductions, personnel turnover, and shifting executive branch priorities.[237]

The Commission highlights significant deterioration in cyber diplomacy. The State Department's Bureau of Cyberspace and Digital Policy ("CDP"), whose central mission is to strengthen cyber-defense capacity among foreign partners and advance U.S. cyber norms abroad, has faced staff reductions, canceled foreign

---

vetoed a Canadian proposal at the G7 meeting to create a task force targeting Russia's "shadow fleet" of oil tankers used to evade sanctions.); Scott Lucas, *Ukraine War, Day 1,110: Trump Administration Vetoes G7 Proposal v. Russia's "Shadow Fleet"*, EA WORLDVIEW (Mar. 9, 2025), https://perma.cc/6DQS-LTPE; Jennifer Hansler, *US Joins Russia to Vote Against UN Resolution Condemning Russia's War Against Ukraine*, CNN (Feb. 24, 2025), https://perma.cc/P7F5-TTPJ (On the third anniversary of Russia's full-scale invasion of Ukraine, the United States voted with Russia at the UN General Assembly against a resolution condemning Moscow's aggression against Ukraine, instead co-sponsoring a U.S-drafted resolution calling for a "swift end to the conflict" and "lasting peace between Ukraine and Russia," omitting references to Ukrainian territorial integrity or Russia's culpability.).

232. DoD Rapid Response (@DODResponse), X (Mar. 4, 2025), https://perma.cc/37KV-G4DU.

233. Stephanie Kirchgaessner, *Trump Administration Retreats in Fight Against Russian Cyber Threats*, GUARDIAN (Mar. 1, 2025), https://perma.cc/U8XR-KA23.

234. *See* 2025 CSC REPORT, *supra* note 1, at 9.

235. Press Release, U.S. Dep't of Just., Botnet Dismantled in International Operation, Russian and Kazakhstani Administrators Indicted (May 9, 2025), https://perma.cc/R8FP-MDWZ [hereinafter DOJ Botnet Press Release]. *See* 2025 CSC REPORT, *supra* note 1, at 18 (announcing the DOJ's dismantlement and indictment of separate groups of Russian and Kazakhstani hackers for deploying malware to build and monetize networks of compromised devices, noting the subsequent July 23, 2025 victim assistance order directing federal authorities to issue notify affected victims).

236. *See* 2025 CSC REPORT, *supra* note 1, at 4.

237. *See id.*

assistance programs, and extended leadership vacancies.[238] These setbacks have markedly degraded U.S. cyber diplomacy as adversaries, principally China, Russia, Iran, and North Korea, seek to expand their digital influence and shape international cyber norms.[239] Because the federal government's whole-of-government architecture relies on sustained diplomatic engagement to mobilize allied support in order to reinforce deterrence, the weakening of this foreign-policy pillar leaves the U.S. cyber framework strategically imbalanced.[240]

These vulnerabilities, which have been compounded by broader budgetary contractions affecting the National Institute of Standards and Technology ("NIST"), CDP, and CISA,[241] alongside the Trump Administration's stated intent to dismantle the CHIPS and Science Act,[242] risk undermining U.S. leadership in key international standard forums.[243] For instance, CISA, which is the nation's primary civilian cyber defense agency, responsible for national incident response, threat advisories, and critical-infrastructure protection, has lost nearly one-third of its workforce, significantly impairing its ability to engage industry and coordinate domestic cyber defense.[244] A resource-constrained CISA weakens deterrence by denial and erodes confidence in the United States' ability to withstand and recover from major cyber incidents. The Trump Administration also eliminated the Critical Infrastructure Partnership Advisory Council ("CIPAC"), which provided the legal framework for information sharing between government and

238. *See id.* at 6; James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 3898 (codifying the State Department's Cyberspace and Digital Policy Bureau ("CDP") under the Cyber Diplomacy Act of 2022, whose mission is to strengthen capacity and resilience among allies and partners).

239. *See* 2025 CSC REPORT, *supra* note 1, at 6.

240. *See id.* at 11.

241. Alexandra Kelley & Eric Katz, *NIST Fires Over 70 Probationary Employees*, NEXTGOV/FCW (Mar. 4, 2025), https://perma.cc/47HD-XACK; David Dimolfetta, *State Department Cuts Hit Cyber Diplomats Doing International Engagements*, NEXTGOV/FCW (July 15, 2025), https://perma.cc/3A9E-L3FU; Eric Geller, *Trump Proposes Major Cut to CISA's Budget, Citing False "Censorship" Claims*, CYBERSECURITY DIVE (May 2, 2025), https://perma.cc/MR8S-WMDX.

242. Blake Ledbetter & Drew Clark, *Trump Says Tariff Threat Drove U.S. Investments, Blasts Biden on Energy*, BROADBAND & BREAKFAST (Mar. 5, 2025), https://perma.cc/8UPW-2UBZ.

243. *See* 2025 CSC REPORT, *supra* note 1, at 11.

244. *See id.* at 6, 10, 19 (noting that the Trump administration's FY 2026 budget proposed a nearly seventeen percent cut to CISA's budget); Press Release, HOUSE APPROPRIATIONS COMM., Ranking Member Henry Cuellar Statement at the Fiscal Year 2025 Budget Request Hearing for the Cybersecurity and Infrastructure Security Agency (Apr. 30, 2024); Sam Sabin, *Exclusive: One-Third of Top U.S. Cyber Force Has Left Since Trump Took Office*, AXIOS (June 3, 2025), https://perma.cc/VC2G-F2NB (reporting that the White House has proposed cutting roughly one-third of CISA's workforce); Tim Starks, *Contract Lapse Leaves Critical Infrastructure Cybersecurity Sensor Data Unanalyzed at National Lab*, CYBERSCOOP (July 22, 2025), https://perma.cc/QQE5-YJHR (reporting that DHS allowed key contracts to lapse, shrinking CISA's technical and outreach capacity); Eric Geller, *"Suspended Animation": US Government Upheaval Has Frayed Partnerships with Critical Infrastructure*, CYBERSECURITY DIVE (June 25, 2025), https://perma.cc/EQ3K-BWRE (CISA has reduced capabilities at a time when its mission is more critical than ever); HOUSE APPROPRIATIONS COMM., 119TH CONG., HOMELAND SEC. APPROPRIATIONS ACT, 2026 6 (Comm. Print 2025), https://perma.cc/LZY7-QZ54 (reflecting a $2.7 billion CISA budget, representing an approximately five percent cut).

industry.[245] This was compounded by the cancellation of more than 83 percent of USAID foreign assistance contracts, including more than $175 million in cyber-related assistance programs,[246] reducing U.S. efforts to secure global digital infrastructure and strengthen partner defenses.

The most consequential setback has been the closure of the Cyber Threat Intelligence Integration Center ("CTIIC") under the "ODNI 2.0" restructuring plan, which also involved a 40-percent reduction in ODNI personnel.[247] CTIIC's elimination removed the government's central node for integrating cyber intelligence and delivering monthly classified briefings to critical-infrastructure operators.[248] Combined with workforce reductions at CISA's Joint Cyber Defense Collaborative ("JCDC"),[249] these changes fractured real-time cyber intelligence sharing between government and industry at a moment of escalating foreign cyber activity.[250]

Some areas nonetheless have showed progress: The National Cyber Investigative Joint Task Force ("NCIJTF"), which is the federal government's lead center for coordinated cyber threat response,[251] conducted more than thirty ransomware-related disruption operations in 2024[252] and has coordinated election-related counterintelligence efforts with CISA and the NSA.[253] The FBI has expanded its overseas cyber presence, including opening a new attaché office in New Zealand, and increasing its network of cyber-focused assistant legal attachés to more than twenty-two key embassies to strengthen its coordination with

245. *See* 2025 CSC REPORT, *supra* note 1, at 7 (noting that, in CIPAC's absence, federal-government engagement with the private sector has measurably declined).

246. Marco Rubio (@marcorubio), X (Mar. 10, 2020), https://perma.cc/9XAF-QH8G; Sam Mednick, Wilson McMakin & Monika Pronczuk, *USAID Cuts Are Already Hitting Countries Around the World. Here Are 20 Projects that Have Closed*, AP NEWS (Mar. 1, 2025), https://perma.cc/EQ8P-2BTA; *see* 2025 CSC REPORT, *supra* note 1, at 11–12.

247. Press Release, OFF. OF THE DIR. OF NAT'L INTEL., DNI Gabbard Launches ODNI 2.0: Reduce Bloat By Over 40% and Save Taxpayers $700+ Million Per Year (Aug. 20, 2025); OFF. OF THE DIR. OF NAT'L INTEL., FACT SHEET: ODNI 2.0 LAUNCH 3 (2025), https://perma.cc/W7KQ-RHTL; *see* 2025 CSC REPORT, *supra* note 1, at 10.

248. *Critical Infrastructure Intelligence Initiative*, OFF. OF THE DIR. OF NAT'L INTEL., NAT'L COUNTERTERRORISM CTR. (Jan. 27, 2025), https://perma.cc/H8M6-L4CT; *see* 2025 CSC REPORT, *supra* note 1, at 10.

249. Eric Geller, *People Are Scared: Inside CISA as It Reels from Trump's Purge*, WIRED (Mar. 13, 2025), https://perma.cc/38K3-35L3; *see* 2025 CSC REPORT, *supra* note 1, at 20.

250. Eric Geller, *CISA's Joint Cyber Defense Collaborative Takes Major Personnel Hit*, CYBERSECURITY DIVE (July 30, 2025), https://perma.cc/4W3Z-6FJA; *see* 2025 CSC REPORT, *supra* note 1, at 10, 20.

251. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CYBER STORM IX: AFTER-ACTION REPORT 16 (2024), https://perma.cc/YQ2W-9D7T; U.S. DEP'T OF HOMELAND SEC., PUBLIC-PRIVATE ANALYTIC EXCH. PROGRAM, IMPACT OF ARTIFICIAL INTELLIGENCE ON CRIMINAL AND ILLICIT ACTIVITIES 39–40 (2024), https://perma.cc/3JRL-A27G; 2025 CSC REPORT, *supra* note 1, at 10. *See generally* Leo S. F. Lin, *Organizational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud*, 14 LAWS 46 (2025).

252. Christian Vasquez, *FBI Has Conducted More Than 30 Disruption Operations in 2024*, CYBERSCOOP (Oct. 30, 2024), https://perma.cc/UQ92-9XCP; *see* 2025 CSC REPORT, *supra* note 1, at 10.

253. Press Release, FED. BUREAU OF INVESTIGATION, Joint ODNI, FBI, and CISA Statement (Nov. 4, 2024); *see* 2025 CSC REPORT, *supra* note 1, at 10.

allies.[254] Yet these gains are threatened by proposed budget cuts and a reduction of 1,830 FBI personnel, which risk undermining its operational ability to respond to cyber threats.[255]

Even amid these institutional constraints, federal agencies have continued major joint operations against Chinese- and Russian-linked botnets through sanctions, indictments, and victim-notification orders.[256] These operations reflect the continued vitality of the Treasury–Justice–DoD coordination and the effectiveness of the integrated sanctions-and-prosecutions model first institutionalized during the Obama Administration.[257] Nevertheless, adversary cyber activity continues at scale, indicating that, although the model has increased the costs of malicious cyber operations, those costs have not yet become sufficiently severe to deter or materially alter adversary behavior.[258] Taken together, the first year of Trump's second term reveals a mixed pattern: operational continuity in using sanctions, law enforcement, and diplomatic tools developed under prior administrations to confront China and transnational cyber-criminal networks, but institutional regression in its diplomacy, domestic cyber defense, and strategic approach to Russia. That divergence is difficult to reconcile with the Administration's own 2025 National Security Strategy, which formally commits the United States to sustained capabilities in cyberspace, requiring precisely the institutional capacity that the Solarium Commission identifies as eroding.[259] The long-term risk is that the United States may retain the tools of cyber statecraft but lose the institutional infrastructure required to use them effectively, raising questions about the future trajectory of U.S. cyber deterrence that has guided the nation's response to foreign cyber threats.

VII. CONCLUSION

The past decade marks a decisive reorientation of U.S. national security strategy toward an integrated, non-kinetic, whole-of-government model for responding to

254. Press Release, FED. BUREAU OF INVESTIGATION, FBI Opens Standalone Office in New Zealand (July 31, 2025); *see* 2025 CSC REPORT, *supra* note 1, at 12.

255. U.S. DEP'T OF JUST., JUST. MGMT. DIV., FISCAL YEAR 2026 BUDGET AND PERFORMANCE 133 (2025), https://perma.cc/B6TR-N5AY; *see* 2025 CSC REPORT, *supra* note 1, at 12.

256. U.S. DEP'T OF HOMELAND SEC., CRITICAL INFRASTRUCTURE AND SEC. AGENCY, PEOPLE'S REPUBLIC OF CHINA-LINKED ACTORS COMPROMISE ROUTERS AND IOT DEVICES FOR BOTNET OPERATIONS 1–3 (Sep. 28, 2024), https://perma.cc/9TTT-J3YE. Press Release, U.S. DEP'T OF STATE, Sanctioning PRC Cyber Company Involved in Malicious Botnet Operations (Jan. 3, 2025), https://perma.cc/5K39-NQ8Z; DOJ Botnet Press Release, *supra* note 235; *see* 2025 CSC REPORT, *supra* note 1, at 18 (In September 2024, U.S. and allied authorities exposed and issued mitigation guidance regarding a PRC-linked botnet comprising more than 1.2 million compromised devices worldwide, including 385, 000 in the United States. Treasury subsequently sanctioned Integrity Technology Group, a cybersecurity company linked to the Chinese Ministry of State Security, on January 3, 2025. The Justice Department followed with coordinated indictments and dismantlement actions targeting Russian and Kazakhstani malware networks in May 2025, accompanied by a July 23 victim assistance order directing the federal government to issue notices to these victims.).

257. *See* 2025 CSC REPORT, *supra* note 1, at 5.

258. *See id.*

259. *See* NSS, *supra* note 2.

malicious cyber activity.[260] Anchored in statutory authorities such as IEEPA, the NEA, and CAATSA,[261] and operationalized through a succession of targeted, cyber-focused executive orders,[262] this model fuses economic sanctions, criminal prosecutions, diplomatic engagement, and persistent military operations into a unified framework for imposing costs, attributing responsibility, disrupting illicit networks, and shaping adversary behavior in the digital domain. The deepening partnership between the Departments of the Treasury and Justice has been especially consequential, producing a hybrid enforcement model that exposes state-sponsored hackers and transnational cybercriminal syndicates, constrains their access to the international financial system, and strengthens emerging norms of responsible state behavior in cyberspace.[263]

Properly understood, however, the central achievement of this sanctions-and-prosecutions model is not that it has produced deterrence in the strict sense of eliminating, or even substantially halting, adversary cyber operations. State-sponsored and criminal cyber activity by Russia, China, Iran, North Korea, and transnational cybercriminal networks persists at significant scale.[264] But that reality does not render the U.S. playbook ineffective. Rather, it clarifies what the evidence supports: sanctions, indictments, forfeiture actions, diplomatic attribution, and military cyber operations have functioned most clearly as instruments of cost imposition, public attribution, financial disruption, accountability, and norm-building.[265] These functions are not substitutes for deterrence; they are the necessary foundations for it. Deterrence in cyberspace is likely to be cumulative, partial, and contested rather than absolute. It depends not on any single designation, indictment, or diplomatic statement, but on whether those tools are sequenced and sustained in ways that increase the expected costs of malicious activity, reduce its operational benefits, and reinforce international expectations of responsible state behavior.

Yet this integrated model now faces growing strain. As the Cyberspace Solarium Commission's 2025 Annual Report warns, federal cyber capacity is beginning to erode, threatening the strategic coherence and institutional resilience

260. *See* WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023), https://perma.cc/ZTK4-ZHJ9; U.S. CYBER COMMAND, *Cyber 101 – Defend Forward and Persistent Engagement* (Oct. 25, 2022), https://perma.cc/ASB8-SWHC; U.S DEP'T OF DEFENSE, *Summary 2023 Cyber Strategy of the Department of Defense* (Sept. 12, 2023), https://perma.cc/X5KF-QU2F.

261. IEEPA, *supra* note 29; NEA, supra note 30; CAATSA, *supra* note 95.

262. Exec. Order No. 13,694, *supra* note 37; Exec. Order No. 13,984.

263. Besciokov Indictment *supra note* 165; Garantex Press Release *supra note* 165; Treasury sanctions related to Salt Typhoon, *supra note* 165; Treasury sanctions related to Lazarus Group supra note 165; Indictment, U.S. v. Guan Tianfeng, No. 24-cr-00088 (N.D. Ind. Sep. 19, 2024); Indictment, U. S. v. Yin Kecheng and Zhou Shuai, No. 18-cr-00126 (D.D.C. Mar. 28, 2023).

264. *See* ODNI, *Annual Threat Assessment of the U.S. Intelligence Community* (2025), https://perma.cc/SAG6-LZ5C; Press Release, FED. BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CTR., 2025 FBI INTERNET CRIME REPORT (Apr. 6, 2026), https://perma.cc/7TZZ-662A; Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise (Jan. 17, 2025), https://perma.cc/WY9C-3GKQ, *supra note* 213.

265. 2023 National Cybersecurity Strategy, *supra note* 260.

on which the whole-of-government approach depends.[266] Preserving the United States' capacity to shape the international cyber order will therefore require more than retaining the formal legal authorities described in this Article; it will require restoring the institutional infrastructure that makes those authorities operationally effective. Recent erosions in cyber diplomacy, domestic cyber defense, and intelligence-sharing risk reducing an integrated deterrence framework to a set of siloed instruments deployed without strategic coherence.[267] The imperative for reinvestment could not be more urgent. The accelerating proliferation of ransomware, cryptocurrency-enabled money laundering, and state-sponsored cybercrime, driven by adversaries such as North Korea, Russia, Iran, and China,[268] reflects a threat environment evolving faster than the institutions charged with defending against it. China's 2024 breach of the U.S. Treasury Department and several major telecommunications networks[269] stands as a stark reminder that

266. *See* 2025 CSC REPORT, *supra* note 1.

267. *See id.*

268. *See, e.g.*, Press Release, U.S. DEP'T OF THE TREASURY, Treasury Designates Iranian-Based Financial Facilitators of Malicious Cyber Activity and For the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), https://perma.cc/S6VW-63EM; Press Release, U.S. DEP'T OF THE TREASURY, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), https://perma.cc/BY5K-SZ8E. *Compare* Press Release, FED. BUREAU OF INVESTIGATION, FBI Releases Internet Crime Report (Apr. 4, 2024), https://perma.cc/DZN9-9K5D, and FED. BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CTR., 2023 INTERNET CRIME REPORT (Apr. 24, 2024), https://perma.cc/WTA3-CLGF (reporting that the FBI received a record 880,418 complaints in 2023, with potential losses exceeding $12.5 billion, a 10% increase in complaints and a 22% increase in losses compared to 2022); *with* Press Release, FED. BUREAU OF INVESTIGATION, FBI's 2024 Internet Crime Complaint Center Report Released (Apr. 24, 2025), https://perma.cc/93YD-A7LB; *and* FED. BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CTR., 2024 INTERNET CRIME REPORT (Apr. 24, 2025), https://perma.cc/Z2SL-Z7LE (reporting that the FBI received a record 859,532 complaints in 2024, with potential losses exceeding $16.6 billion, a 33% increase in complaints and a 33% increase in losses compared to 2023);. *See also* RANSOMWARE ADVISORY, *supra* note 39, at 1 (describing the Russian-linked 2020 cyberattack that breached multiple U.S. government agencies, including DHS, Defense, State, Treasury, Commerce, and Agriculture); Michael Holmes, *Why the OPM Hack is Far Worse Than You Can Imagine*, OODA LOOP (Mar. 11, 2016), https://perma.cc/F8F6-33V5 (describing the OPM attack as possibly the most significant in U.S. history, surpassing even the infamous Chinese hack of the OPM, further underscoring the critical importance of a robust sanctions regime); Zachary B. Wolf, *The Suspected Russian Hack of the U.S. Government, Explained*, CNN (Dec. 15, 2020), https://perma.cc/TR6R-ME3G; David E. Sanger, Nicole Perlroth & Julian E. Barnes, *Billions Spent on U.S. Defense Failed to Detect Giant Russian Hack*, N.Y. TIMES (Dec. 16, 2020), https://perma.cc/KM3N-ZGFZ.

269. Suspected China-Linked Hack on US Telecoms Worst in Nation's History, Senator Says, REUTERS (Nov. 22, 2024), https://perma.cc/2H8V-2DMK (reporting that a China-linked intrusion into multiple U.S. telecommunications providers constituted the "worst telecom hack in our nation's history, " stealing U.S. customer call records and communications from individuals engaged in government or political activity); Andrea Mitchell & Nicole Moeder, S*weeping Chinese Hack of U.S. Telecoms Firms is "Still Going On," Homeland Security Secretary Says*, NBC NEWS (Dec. 18, 2024), https://perma.cc/V8FW-3EBG (describing a long-running Chinese espionage campaign, one of the largest intelligence compromises in U.S. history, that breached eight U.S. telecom and internet service providers, as part of a broader intelligence operation by China-backed hacking group known as Salt Typhoon); Eric Tucker, *Chinese Hackers Accessed Workstations and Documents In a Major Cyber Incident, Treasury Says*, AP NEWS (Dec. 31, 2024), https://perma.cc/QJ22-JE5H (reporting that China-linked actors accessed Treasury Department workstations and exfiltrated unclassified documents); Raphael Satter & A.J. Vicens, *US Treasury Says Chinese Hackers Stole Documents in Major Incident*, REUTERS (Dec. 31, 2024), https://perma.cc/SL5U-D39Z (detailing that China state-sponsored hackers, associated with an

even the most sophisticated infrastructures remain vulnerable to determined, well-resourced foreign actors. In an era in which artificial intelligence will accelerate cyber intrusion[270] and cryptocurrency will continue to facilitate cross-border illicit activity,[271] the central challenge is no longer whether the United States possesses the legal and operational tools to respond to these threats, but whether it will sustain the institutional capacity and strategic clarity to use them coherently.

As a priority, the United States should rebuild the interagency "spine" of U.S. cyber governance.[272] Reinvestment in core civilian institutions such as CISA and NIST, paired with strengthened allied capacity building and the restoration of a reliable public–private collaboration framework,[273] would reinforce deterrence by denial and reduce the strategic payoff of malicious cyber operations. These investments would ensure that sanctions and prosecutions operate as force multipliers rather than substitutes for baseline cyber resilience.

At the same time, the effectiveness of sanctions and prosecutions will increasingly depend on whether the United States can disrupt cyber ecosystems rather than merely punish individual actors. The federal government has already begun to move in this direction, leveraging designations, indictments, forfeiture actions, and coordinated international partner operations to target ransomware infrastructure, virtual-asset laundering networks, and other enabling nodes.[274] Yet these efforts remain uneven and too often episodic. Future campaigns should more systematically prioritize the financial and technical enabler networks that make malicious cyber activity scalable and profitable, including ransomware brokers, virtual-asset laundering networks, illicit infrastructure providers, front companies, and state-linked intermediaries. Doing so requires a more coordinated and operationally repeatable use of Treasury and Justice authorities, pairing sanctions designations with indictments, forfeiture actions, and allied operations to impose friction across the full lifecycle of cybercrime. It also requires a more consistent application of these tools across adversaries, including narrowing the gap between public attribution through indictments and economic isolation through sanctions, particularly in cases of China-linked cyber theft, where uneven

Advanced Persistent Threat ("APT") group, stole Treasury documents in what the agency described as a "major incident"); Sean Lyngaas, *Chinese Hackers Breached US Government Office that Assesses Foreign Investments for National Security Risks*, CNN (Jan. 10, 2025), https://perma.cc/B4SC-54A9 (explaining that Chinese hackers penetrated the Treasury Department's Committee on Foreign Investment in the United States ("CFIUS"), which reviews foreign investment transactions for national security concerns).

270. NATIONAL CYBER SECURITY CENTRE, *Impact of AI on cyber threat from now to 2027* (May 7, 2025), https://perma.cc/AHQ4-UCNK; NATIONAL CYBER SECURITY CENTRE, *The near-term impact of AI on the cyber threat* (Jan. 24, 2024), https://perma.cc/8DCB-G92P; 2025 FBI INTERNET CRIME REPORT, *supra note* 264.

271. Garantex Cryptocurrency Exchange Disrupted in International Operation, *supra note* 165; Treasury sanctions related to Lazarus Group, *supra note* 165.

272. *See* 2025 CSC REPORT, *supra* note 1; 2023 National Cybersecurity Strategy, *supra note* 260.

273. 2023 National Cybersecurity Strategy, *supra note* 260; CISA, *Partnership and Collaboration*, https://perma.cc/DK2V-DW3T.

274. 2023 National Cybersecurity Strategy, *supra note* 260; CISA Partnership and Collaboration, *supra note* 273.

application risks undermining the credibility of deterrence and weakening the norm-building function of the U.S. response.

Finally, the United States should institutionalize a doctrine of sequenced cyber cost imposition, formalizing practices it already employs but too often executes in parallel or episodically. When properly synchronized, military disruption can degrade operational capability; indictments can create a public evidentiary record that reinforces attribution and delegitimizes state-linked cyber activity; sanctions can constrain operational finance and deny access to the international financial system; and diplomacy can internationalize the response while reinforcing emerging norms of responsible state behavior.[275] The goal is not to create new tools, but to develop a repeatable strategy that compels existing instruments to operate as mutually reinforcing components of cumulative statecraft rather than as parallel, ad hoc responses to malicious cyber activity.

The 2025 National Security Strategy's emphasis on economic statecraft, allied coordination, and long-term strategic competition reinforces the cyber-specific approach articulated in the 2023 National Cybersecurity Strategy and the 2023 Department of Defense Cyber Strategy, which frame cyber capabilities, public attribution, sanctions, law enforcement, diplomacy, and partner capacity building as mutual reinforcing instruments of U.S. power.[276] The United States therefore stands at an inflection point. Whether it can continue to impose meaningful costs on malicious cyber actors, reinforce emerging international norms, and safeguard the integrity of its democratic, financial, and national security institutions will depend on its willingness to sustain, strengthen, and modernize the integrated cyber governance regime built over the past decade. The emerging rule-of-law framework in cyberspace, fragile, contested, and still in formation, will not endure through institutional complacency or apathy. It will require strategic clarity, institutional resilience, and sustained political commitment to adapt legal authorities and enforcement tools commensurate with the speed of technological change. The central question is not simply whether the United States can defend itself against the next major cyber intrusion, but whether it will retain the capacity to shape the norms and boundaries of state behavior in the digital domain, or whether those rules will instead be written by the very actors seeking to destabilize them. The durability of the U.S. playbook for digital warfare, and the rule-of-law framework it seeks to advance, will ultimately depend on that choice.

275. Cyber 101 – Defend Forward and Persistent Engagement, *supra note* 260.
276. *See* NSS, *supra* note 2.

***