FOUNDATION FOR DEFENSE OF DEMOCRACIES

The Attack on America's Future

Cyber-Enabled Economic Warfare

Edited by Samantha F. Ravich and Annie Fixler

October 2022

The Attack on America's Future

Cyber-Enabled Economic Warfare

Edited by
Samantha F. Ravich
and Annie Fixler

October 2022

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

INTRODUCTION

By Samantha F. Ravich and RADM (Ret.) Mark Montgomery

In 2018, the Foundation for Defense of Democracies (FDD) published a series of monographs analyzing cyber-enabled economic warfare (CEEW) as practiced by Russia, China, North Korea, and Iran. The four studies brought together for the first time an assessment of each adversary's CEEW attacks on America's economic infrastructure. At the time, the term CEEW was only beginning to seep into the consciousness of the U.S. national security community. The White House had used the term in its 2017 National Security Strategy, noting how adversaries are using technology to "weaken our businesses and our economy."[1] But the connection between such malicious activities and the overall strategies of America's four principal adversaries remained unclear.

The risks associated with CEEW are now clearer, thanks less to the rigorous analysis of adversarial intentions than to the increased scale, scope, and frequency of attacks across the American economic landscape. Still, the federal government has a blind spot that leaves the United States vulnerable to a

1. The White House, "National Security Strategy of the United States of America," December 2017, page 21. (https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)

catastrophic strategic surprise — one that could simultaneously destabilize the U.S. electrical grid, water supply, banking system, transportation sector, or other critical infrastructure necessary for survival. That blind spot is intelligence that anticipates the adversary's strategy. For too long, the United States has tried to patch its way to safety with the enemy inside its networks.

> **"For too long, the United States has tried to patch its way to safety with the enemy inside its networks."**

Roberta Wohlstetter's 1962 book *Pearl Harbor: Warning and Decision* warns of the perils of missing "a particular enemy move or intention" amidst a vast amount of intelligence.[2] The book has remained relevant over the decades as the United States successfully avoided a thermonuclear surprise attack by the Soviets, on the one hand, but failed to anticipate jet planes flying into skyscrapers, on the other. Wohlstetter informed generations of Cold War and counterterrorism intelligence analysts that signals not only must be gathered and illuminated to inform policymakers but must also be broken down and dissected to help guide future intelligence collection. Only then can the United States decipher the enemy's decision-making structures and gain insight into the adversary's larger strategic plan.

In FDD's 2018 CEEW reports, we focused on reading the signals. Four years hence, this monograph's updated chapters on Russia, China, North Korea, and Iran embark upon the hard task of breaking down and dissecting those signals. In each chapter, the authors analyze what these adversaries may do next and how the U.S. government and private sector might disrupt those plans.

Russia

In his 2018 monograph for FDD, Boris Zilberman was one of the first scholars to detail how Moscow employs both state actors and proxies to get inside the information and communications technology (ICT) supply chain that is vital to America's economic wherewithal. He documented how Kaspersky Lab demonstrated "technical knowhow, market foresight, and government cooperation [to] produce not only a global tech giant but also a serious national security threat."[3]

Today, as Ryan Tully and Logan Weber describe herein, the Kremlin exploits "the gaps that prevent Washington from definitively attributing hostile cyber actions to the Russian government." The authors emphasize that "Russia's intelligence services seem to understand, perhaps better than American lawmakers, the constraints on the U.S. intelligence community when a foreign adversary shifts — physically or virtually — from operating outside of American borders to operating from within." As Tully and Weber note, the U.S. intelligence community is generally restricted from looking inward at the U.S. populace or infrastructure. Thus, policymakers must grapple with difficult tradeoffs between security and privacy embedded within the current legal framework. Tully and Weber also urge greater intelligence collection and analysis of "Moscow's surveillance dragnet" as an "enabler of CEEW operations abroad."

As this volume approached publication, Russia invaded Ukraine. Russian artillery continues to pulverize Ukrainian villages, while Russian missiles wreak havoc in major cities. The Kremlin even rattled its nuclear saber. Generally missing in action, however, was Russia's vast cyber capability. While there were some notable attacks such as that against California-based global satellite communications provider

2. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), pages 2–3.
3. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, June 2018, page 7. (https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare)

Viasat,[4] there was no "shock and awe" cyberattack that crippled Ukraine's critical infrastructure in one fell swoop. Rather, there were "hundreds of far more subtle attacks, many timed to coincide with incoming missile or ground attacks."[5] Theories vary as to why. One theory that will require more investigation: Did the Kremlin worry that a significant cyber strike might quickly leap from the Ukrainian battlefield to other domains, inviting Western retaliation? As National Cyber Director Chris Inglis hypothesized, perhaps the Russians "kind of understand that there are thresholds — they don't know quite where those thresholds are, and they don't want to cross those."[6]

"The analysis presented here sets the stage for understanding how Russia may deploy its cyber capabilities over the next few years given its unimpressive display of hard power in Ukraine and an economy weakened due to western sanctions."

While the fog of war is too dense to discern potential shifts in Russia's longer-term CEEW strategy, the analysis presented here sets the stage for understanding how Russia may deploy its cyber capabilities over the next few years given its unimpressive display of hard power in Ukraine and an economy weakened due to Western sanctions. The Kremlin will have limited options to undermine its adversaries — which have multiplied in the last few months. The war in Ukraine will force Russia to prioritize asymmetric means to seek revenge and regain parity. CEEW will become an increasingly attractive option.

China

The Chinese CEEW battlespace has also grown more complex and dangerous since 2018, when author Zack Cooper explored the changing contours of China's cyber operations. Cooper wrote that China's hostile CEEW activity had "not garnered the public attention warranted by its severity" despite the fact that "China is engaged in wide-ranging cyber intrusions and network exploitations causing massive damage to U.S. and other foreign firms annually."[7]

After four additional years of attacks and broken promises from the People's Republic of China, we pick up the narrative where Cooper left off, exploring the fundamentals of Chinese CEEW, writing that it grows out of central tenets in China's "long-standing approach to political warfare." Chinese doctrine views cyber and economic tools as "direct and powerful means of influencing public opinion, altering an adversary's political environment, and diminishing its resolve in a crisis."

The chapter digs into the Chinese Communist Party's (CCP's) quest for control of global ICT infrastructure and the "technologies, supply chains, and services that constitute it," noting this "is a central front" in CEEW. To understand and then undermine China's CEEW strategy going forward, the United States should focus on ICT, which includes 5G and other telecommunications equipment, satellite navigation, cloud computing, and integrated circuits. China seeks to dismantle the U.S. and allied stake in these markets through cyber-espionage and sabotage as well as non-market coercion so that Beijing can "control key nodes in the global economy." A powerful tool to combat

4. Martin Matishak, "Western powers blame Russia for Ukraine satellite hack," *The Record*, May 10, 2022. (https://therecord.media/eu-uk-blame-russia-for-ukraine-satellite-hack)
5. Kate Conger and David E. Sanger, "Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds," *The New York Times*, April 27, 2022. (https://www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html)
6. National Cyber Director Chris Inglis, "Strengthening America's Cyber Resiliency: A Conversation with the National Cyber Director," *Remarks at the Foundation for Defense of Democracies*, June 2, 2022. (https://www.fdd.org/events/2022/06/02/strengthening-americas-cyber-resiliency-a-conversation-with-the-national-cyber-director)
7. Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, September 2018. (https://www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare)

risks associated with Chinese ICT in U.S. critical infrastructure is Executive Order 13873 of 2019, "Securing the Information and Communications Technology and Services Supply Chain."[8] Codifying this executive order in law could provide the Commerce Department with the will and resources needed to "establish a quasi-'import control' regime around ICT equipment."

North Korea

The evolution of North Korean and Iranian CEEW over the last four years should compel U.S. policymakers to ask whether the intelligence community has more than a passing understanding of the enemy's plan.

FDD's North Korea monograph in 2018 analyzed how the Kim regime deploys its cyber capabilities as an "All-Purpose Sword." Authors David Maxwell and Mathew Ha wrote, "As diplomatic efforts to dismantle North Korea's nuclear weapons program move forward — or even if they do not — the flexibility and plausible deniability of cyber capabilities may make them an even more attractive weapon for the Kim regime."[9]

And yet, as Ha notes in his update, Pyongyang has not employed its cyber capabilities for military ends in recent years. Rather, North Korea has wielded its all-purpose sword "to reap financial, political, and strategic benefits that are essential to prolonging the Kim regime's survival," with a primary focus on "financially motivated cybercrime." Ha posits that the Kim regime "has calibrated its cyber provocations to remain within the gray zone between war and peace so as not to elicit a military response from South Korea and the United States." At what point this calculus might change is not clear. Continued disintegration of North Korea's domestic economy may lead Kim to move away from grand larceny and toward CEEW to coerce financial concessions from Washington and its allies. Or the Kim regime may simply miscalculate the line that separates the gray zone from outright warfare. These scenarios require continued vigilance and analysis to predict and prevent.

"The evolution of North Korean and Iranian CEEW over the last three years should compel U.S. policymakers to ask whether the intelligence community has more than a passing understanding of the enemy's plan."

Ha makes a strong case that a potential shift in North Korea's CEEW strategy toward a more aggressive stance could occur as the regime fills its cryptocurrency coffers. Pyongyang's persistent theft from cryptocurrency exchanges could enable it to "build large reserves in numerous cryptocurrencies to spend in a cryptocurrency-based system of exchange independent of the U.S.-led financial system." Ha explores Pyongyang's development of a cryptocurrency-based system as a potential pathway to *juche* ("self-reliance") — the bedrock of the Kim regime's ideology. With the total value of the cryptocurrency market around $1 trillion,[10] the allure for the cash-strapped North Korean regime is obvious. Still, Ha acknowledges that Pyongyang's "ability to leverage cryptocurrencies for these greater objectives will likely be contingent upon technological advances by other rogue states with more robust economies that are more important to global trade." The United States should carefully monitor whether North Korea is leveraging Russian and Chinese advances in the field of digital currency to undermine the international sanctions regime built to thwart Pyongyang's nuclear and missile ambitions.

8. Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019. (https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain)
9. David Maxwell and Mathew Ha, "Kim Jong Un's 'All-Purpose Sword,'" *Foundation for Defense of Democracies*, October 2018. (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword)
10. Elizabeth Howcroft, "Cryptocurrency market value slumps under $1 trillion," *Reuters*, June 13, 2022. (https://www.reuters.com/business/finance/cryptocurrency-market-value-slumps-under-1-trillion-2022-06-13)

Iran

Like North Korea, the Islamic Republic of Iran has seemingly pulled back on its CEEW activities, though it is not clear why.

Annie Fixler observes that Tehran clearly has the means to conduct such attacks, as illustrated by Iran's distributed denial of service (DDoS) attacks on the U.S. financial sector in 2011–2013, the Shamoon attacks against Saudi Aramco in 2012, and the 2019 cyberattacks against Bahrain's Electricity and Water Authority. Still, despite the U.S. assassination of Qassem Soleimani, commander of the Islamic Revolutionary Guard Corps Quds Force — Iran has refrained from wielding CEEW in a more devastating fashion over the past four years. Iranian hackers, however, have demonstrated improving capabilities and an ability to learn lessons from the successful operations of other U.S. adversaries.

Fixler counsels that the lack of "spectacular cyberattacks against the United States" should not lead policymakers to assume the United States has deterred Iran. There is not enough evidence to make this judgement. And even if Iran were temporarily deterred in its use of CEEW, "[d]eterrence is not static," as Fixler thoughtfully writes. "It requires regular maintenance."

If Fixler is right that Iran, like North Korea, has relegated CEEW tools and techniques to the fringes, there may be lessons for deterring non-near-peer competitors and rising cyber-weapon states. However, as Fixler concludes, "Underestimating a committed adversary is dangerous, and a misdiagnosis risks underinvestment in intelligence gathering, leading to strategic surprise." While it is possible Washington has deterred Iran, it is equally likely Tehran has "elected not to expend limited resources on destructive attacks but to maintain the capability to employ them later on. After all, cyber-espionage can always be a steppingstone to more aggressive operations, and it can be difficult to parse motive from a few lines of code." Washington "cannot afford to discount or dismiss Iran as a significant cyber threat."

Recommendations

In addition to the country-specific recommendations in this monograph, the United States should undertake the following overarching steps to better protect itself against CEEW.

1. **Improve focus within the intelligence community on the CEEW challenge.** With America's nation-state adversaries developing and utilizing CEEW tools, the intelligence community must bring increased focus to this issue. It must prioritize resources and personnel to better understand adversary CEEW campaigns, particularly the adversary's economic interests, and to determine how to rapidly assess and distribute this information to allies and private-sector partners. The Office of the Director of National Intelligence's National Counterintelligence and Security Center is positioned to lead this effort, alongside efforts underway at the Treasury Department, if properly tasked and resourced.

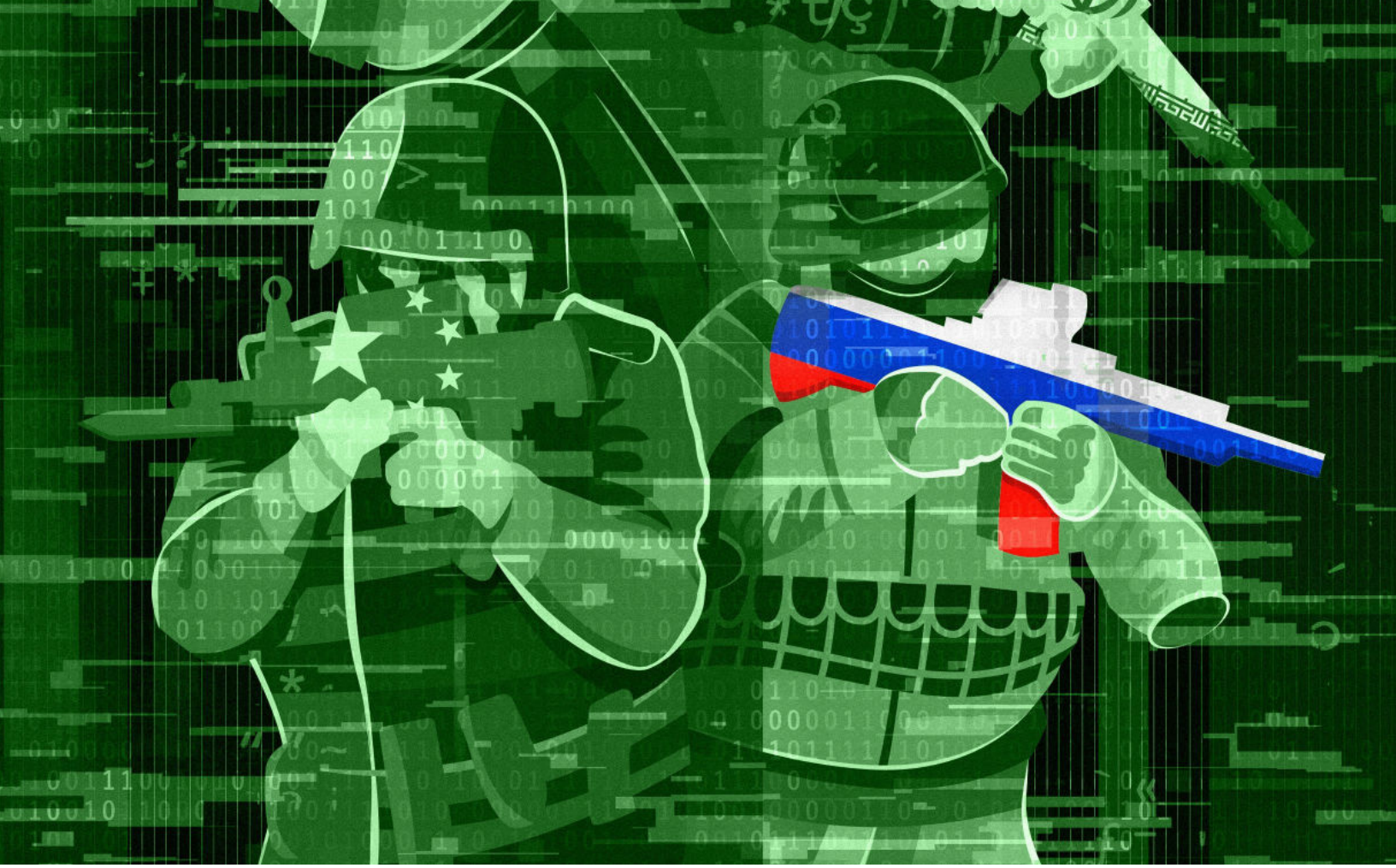
2. **Improve public-private collaboration efforts toprepare for the CEEW threat.** The United States needs an improved capacity to withstand CEEW attacks while reducing their frequency, scope, and scale. The nation must be prepared to respond to and recover from an attack, sustain critical functions even under degraded conditions, and, in some cases, restart those functions after a disruption. The United States must also raise the level of security across the cyber ecosystem. Because the private sector owns and operates the vast majority of that ecosystem, scaling up security necessitates public-private cooperation. The public and private sectors need to identify, assess, and mitigate risk across all elements of critical infrastructure in order to defend it. The government must build a better understanding of threats, with the aim of informing the private sector and directing government efforts to counter malicious cyber activities. While recognizing that private-sector entities have primary responsibility for the defense and security of their networks, the U.S. government has unique authorities, resources, and offensive cyber capabilities it can employ to support the private sector.

3. **Develop economic contingency plans.** A critical element of public-private collaboration is economic planning. While Washington has adequately identified and planned for key military contingencies, it must account for the entire spectrum of conflict where CEEW could occur. Adversaries will likely operate in the gray zone, skirting the line of armed conflict. They are likely to wage war first on an economic front or by employing a combination of economic coercion and critical-infrastructure disruption to raise pressure on the United States and its allies. To develop economic contingency plans, Washington needs a better understanding of U.S. and allied economic strengths and vulnerabilities. This planning should include economic actions that impose costs on attackers. (See the following recommendation.) It should also map out a list of options to mitigate risks, build resilience, and rapidly restart the economy. A key component of this economic contingency planning is the government-led Continuity of the Economy efforts directed by the National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA). These efforts will help coordinate, exercise, and refine government and private-sector efforts to build economic resilience. They will help ensure the United States is not caught flat-footed by an adversary's CEEW efforts and will assist in the rapid restart and recovery of the U.S. economy in case of a widespread disruption.

4. **Expand the use of economic statecraft.** Economic statecraft tools, such as sanctions and export controls, are appropriate responses to adversary CEEW attacks, since they are reciprocal. Sanctions could impose withering costs on the officials, firms, and governments who direct or benefit from acts of CEEW, especially if the sanctions are multilateral. Meanwhile, export controls — again, preferably multilateral — can limit access to key Western technologies that facilitate economic warfare against the United States and its allies. In addition, restrictions on the use of ICT equipment and services received from companies in hostile states can mitigate the risk of those governments, particularly China, utilizing the technological reach of their companies for cyber-enabled intellectual property (IP) theft and critical-infrastructure disruption.

5. **Improve U.S. gray zone capabilities.** To compete effectively in the gray zone, the United States and its allies must be willing to employ diplomatic, information, military, and economic tools using a strategic approach involving "defend forward" operations. The concept of defend forward posits that to disrupt and defeat ongoing adversary campaigns, the United States must proactively and persistently detect, observe, pursue, and counter adversaries' operations and, where appropriate, impose costs on the adversary. The concept further posits that proactive responses to adversary gray zone operations signal that the U.S. government will respond to CEEW attacks, even those that do not cause physical destruction or death. Among other things, this will require the development of comprehensive information operations campaigns to counter adversary disinformation and support U.S. policies and interests.

Whereas FDD's 2018 monographs were meant as a clarion call to recognize the importance of CEEW, the chapters contained herein seek to encourage intelligence gathering and responses to the adversary's CEEW battle plan. Now more than ever, as American lives are dependent upon a network that moves at the pace of data, the United States must live by the credo, "To be forewarned is to be forearmed."



POSSIBLE FUTURES FOR RUSSIA'S CEEW PLAYBOOK

By Ryan Tully and Logan Weber

Introduction

Over the past four years, Russia has used cyber operations to engage in espionage, disinformation campaigns, and supply chain disruptions. While the tools and tactics of each operation vary, their overarching goal is to weaken the United States through a digital assault on its diplomatic, intelligence, military, and economic wherewithal. The Kremlin has embraced an asymmetric strategy because it lacks the economic and conventional military might to compete directly with the United States.[11] Indeed, Russia uses non-kinetic, covert, or deniable means such as CEEW.

Russian cyber operations have historically focused on military and political targets. But over the past decade, these operations have increasingly targeted economic assets such as critical infrastructure and software products.[12] As Boris Zilberman explained in his 2018 FDD study on Russian CEEW, Moscow initially

11. Robert Berls Jr., "The State of the Russian Economy: Balancing Political and Economic Priorities," *Nuclear Threat Initiative*, July 13, 2021. (https://www.nti.org/analysis/articles/state-russian-economy-balancing-political-and-economic-priorities)
12. Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016. (https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111)

focused on infiltrating technology supply chains.[13] These "beachheads" enabled Russian incursions into targets ranging from private-sector assets to public-sector data repositories. Now, Moscow's focus has broadened further, aiming to "gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling — now or in the future — targets of interest to the Russian government," according to a Microsoft report.[14]

American policymakers have long been aware of Chinese cyber-espionage operations within the U.S. economic sphere and have, of late, recognized China's CEEW activity. However, U.S. officials have often underemphasized the economic impacts and indirect strategic effects of Moscow's cyber operations, focusing more on the threat of Russian cyber-espionage and disinformation operations. It is now clear that Russia has the intention and capability to undermine key parts of the American economy.[15]

This chapter begins by examining two critical facets of Russian cyber strategy. First, the Kremlin has vigorously used cyber means to consolidate President Vladimir Putin's political and economic control in Russia. However, the System of Operative Search Measures (SORM), Moscow's surveillance dragnet, is not only a tool for domestic control but also a likely enabler of CEEW operations abroad.

"The System of Operative Search Measures (SORM), Moscow's surveillance dragnet, is not only a tool for domestic control but also a likely enabler of CEEW operations abroad."

Second, Russia is increasingly proficient in preventing Washington from definitively attributing hostile cyber actions to the Russian government. This is consistent with Russia's long tradition of muddying the information space, including through cyber-enabled influence operations against economic targets to advance Russia's strategic interests. Moscow obscures attribution by cooperating with cybercriminals. It has created a permissive environment for them in Russia that has helped fuel a cybercrime epidemic abroad, including Russian ransomware attacks against U.S. critical infrastructure. In addition, Russia's intelligence services seem to understand, perhaps better than American lawmakers, the constraints on the U.S. intelligence community when a foreign adversary shifts — physically or virtually — from operating outside of America's borders to operating from within.

After exploring these components of Russian strategy, this chapter presents two case studies showing how these techniques and tactics are operationalized. The chapter concludes with policy recommendations to help the U.S. and allied governments combat the Russian CEEW threat.

Russian CEEW Through the Lens of SORM

A systematic analysis of SORM sheds light on Moscow's current and future cyber tactics. SORM enables Russia's security services to monitor network traffic in Russia, including communications with the West — thereby helping to identify access vectors into the networks of Western companies. Moscow could use this access to obtain intelligence to provide Russian firms with advantages over their Western competitors.

An outgrowth of the KGB's telephonic monitoring system, SORM allows Russia's Federal Security Service (FSB) nearly unfettered access to all phone and

13. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, June 19, 2018. (https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare)
14. Tom Burt, "New Activity from Russian Actor Nobelium," *Microsoft*, October 24, 2021. (https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium)
15. Bob Weiss, "A Timeline of Russian Cyber-Exploits," *WyzGuys Cybersecurity*, December 21, 2020. (https://wyzguyscybersecurity.com/a-timeline-of-russian-cyber-exploits)

internet-based communications that travel in or through Russia.[16] Russia's other security services can request access to SORM as well. The system sits on top of existing internet infrastructure and integrates with other platforms so that a wide range of assets can be monitored.[17] Moscow requires telecommunications companies, internet service providers, and social media companies to install SORM equipment.[18] Since 2013, Moscow has also required Russian telecommunications providers and foreign technology companies to retain their data inside Russia.[19] Applications must be "SORM-compatible" to operate in Russia,[20] and the Russian government has issued large fines for non-compliance.[21]

In a 2018 publication for Lawrence Livermore National Laboratory, researcher J.A. Kerr predicted that SORM-related surveillance technologies and accompanying legal frameworks will continue to proliferate "across the former Soviet region, as these states share legal and institutional legacies, participate in common regional organizations, and also often share overlapping media markets and Internet resources." Likeminded regimes may grant Moscow access to their systems because they are indebted to Russia or to augment their own domestic surveillance capabilities. Russian hackers may also find these systems easier to penetrate because of their similarity to Russian systems. Kerr added that "experimentation and learning around information control at home can drive advances in 'political' or 'information' warfare capabilities in international competition."[22] The same holds true for augmenting CEEW capabilities; information collected can help guide the timing and targeting of attacks against adversarial economies.

"Likeminded regimes may grant Moscow access to their systems because they are indebted to Russia or to augment their own domestic surveillance capabilities."

Russia refined its surveillance techniques during the 2014 Winter Olympics in Sochi, where the Kremlin used SORM to monitor both Russian dissidents and foreigners. The FSB monitored every athlete, coach, journalist, politician, diplomat, company, vendor, and spectator who attended the games. Putin even placed senior FSB counterintelligence official Oleg Syromolotov in charge of Olympic security.[23]

At the time, the U.S. State Department's Bureau of Diplomatic Security warned that "trade secrets, negotiating positions, and other sensitive information may be taken and shared with competitors, counterparts, and/or Russian regulatory and legal entities."[24] For Moscow, the Olympics were an opportunity not only to showcase Russian athleticism and culture, but also

16. Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's War on the Internet* (NYC: Hachette Book Group, 2015), pages 83–84.
17. Adam Satariano, Paul Mozur, and Aaron Krolik, "When Nokia Pulled Out of Russia, a Vast Surveillance System Remained," *The New York Times*, March 28, 2022. (https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html)
18. Alina Polyakova, "Russia is Teaching the World to Spy," *The New York Times*, December 5, 2019. (https://www.nytimes.com/2019/12/05/opinion/russia-hacking.html). See also: Adam Satariano and Paul Mozur, "Russia is Censoring the Internet, With Coercion and Black Boxes," *The New York Times*, October 22, 2021. (https://www.nytimes.com/2021/10/22/technology/russia-internet-censorship-putin.html)
19. Zack Whittaker, "Documents Reveal How Russia Taps Phone Companies for Surveillance," *TechCrunch*, September 18, 2019. (https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance); Daria Litvinova, "Russia Fines Google for Violating Data Storage Law," *Associated Press*, July 29, 2021. (https://apnews.com/article/technology-europe-business-russia-data-storage-8cfce05469d996b6342899a2195ce6df)
20. Mitchell Clark, "Apple just gave Russia a spot on the iPhone to advertise its favorite apps to citizens," *The Verge*, March 16, 2021. (https://www.theverge.com/2021/3/16/22334641/apple-follows-russian-default-apps-law-setup-screen-options-user)
21. Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's War on the Internet* (NYC: Hachette Book Group, 2015), pages 211–212.
22. Jaclyn A Kerr, "The Russian Model of Internet Control and Its Significance," *Lawrence Livermore National Lab*, December 18, 2018. (https://www.osti.gov/servlets/purl/1491981)
23. Shaun Walker, "Russia to Monitor 'all communications' at Winter Olympics in Sochi," *The Guardian* (UK), October 6, 2013. (https://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics); "The 2014 Sochi Winter Olympics: Security and Humans Rights Issues," *Congressional Research Service*, January 26, 2014. (https://fas.org/sgp/crs/misc/R43383.pdf)
24. Shaun Walker, "Russia to Monitor 'all communications' at Winter Olympics in Sochi," *The Guardian* (UK), October 6, 2013. (https://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics)

to collect data for Russian CEEW efforts.[25] Every company or vendor that attended the games put at risk proprietary trade secrets and valuable IP that the FSB could funnel to state-backed entities or use to undercut or extort their competitors.

Such SORM-enabled surveillance would be particularly advantageous for the Russian energy sector. The Russian partner in any joint venture with a foreign firm — be it a state-owned bank such as Sberbank or state-controlled energy giant Rosneft — could employ surveillance that facilitates cyber-espionage against its foreign partner, including data acquisition outside the scope of the joint venture. For example, information gleaned through joint ventures with Saudi Arabian firms — such as those to which Riyadh agreed during Putin's October 2019 visit — could empower Moscow during a potential reprisal of the 2020 Russian-Saudi oil price war.[26]

Intergovernmental agreements on cybersecurity could also facilitate Russian CEEW through SORM. Russia has signed dozens of such agreements.[27] Any time foreign systems are connected to Russia, Moscow's intelligence services can use SORM to penetrate foreign entities by using information that passes through Russian phone exchanges, including calls, messages, and other data.[28] Washington and its allies and partners need to better understand how SORM facilitates covert Russian access to international trade and commerce data.

Russia Leverages the Complications of Attribution

After a cyber-enabled attack, identifying the perpetrator is not simple. To be sure, U.S. intelligence and private cybersecurity firms can track packets of information, malware, and network infrastructure around the world. But the need to correlate that information with signals and human intelligence as well as assessments of the attacker's tradecraft may complicate the government's ability to quickly determine the party responsible. And absent "high confidence and timely assessments," explains cybersecurity analyst Sarah Freeman, "accountability within the international space cannot be guaranteed."[29]

Russia — like all sophisticated cyber actors — understands these challenges and therefore uses multiple tactics to delay attribution and frustrate Washington's ability to respond. Beyond strategies to evade detection and complicate attribution at a technical level, Moscow also employs cybercriminals and other non-state hackers to obscure its role. The U.S. government and the press have documented this longstanding FSB practice.[30]

25. Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's War on the Internet* (NYC: Hachette Book Group, 2015), pages 241–245.
26. "Saudi Aramco signs 1 SPA and 9 MOUs with Russian Companies at the Saudi — Russian CEO Forum," *Saudi Aramco*, October 14, 2019. (https://www.aramco.com/en/news-media/news/2019/saudi-aramco-signs-1-spa-and-9-mous-with-russian-companies-at-the-saudi-russian-ceo-forum)
27. Zachary Greenhouse with George Barros. "The Kremlin Leverages Cyber Cooperation Deals," *Institute for the Study of War*, August 13, 2020. (http://www.understandingwar.org/backgrounder/kremlin-leverages-cyber-cooperation-deals)
28. Zach Whittaker, "Documents Reveal how Russia Taps Phone Companies for Surveillance," *TechCrunch*, September 18, 2019. (https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance)
29. Sarah Freeman, "Challenges of Cyber Attribution," *Women in International Security*, December 2, 2020. (https://www.wiisglobal.org/challenges-of-cyber-attribution)
30. U.S. Department of Justice, Press Release, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017. (https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions); Lesley Stahl, "The Growing Partnership Between Russia's Government and Cybercriminals," *CBS News*, April 21, 2019. (https://www.cbsnews.com/news/evgeniy-mikhailovich-bogachev-the-growing-partnership-between-russia-government-and-cybercriminals-60-minutes); Garrett Graff, "Inside the Hunt for Russia's Most Notorious Hacker," *Wired*, March 21, 2017. (https://www.wired.com/2017/03/russian-hacker-spy-botnet); U.S. Department of the Treasury, Press Release, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," December 5, 2019. (https://home.treasury.gov/news/press-releases/sm845); Frank Bajak, "The Kremlin is Providing a Safe Harbor for Ransomware," *Fortune*, April 16, 2021. (https://fortune.com/2021/04/16/kremlin-cybercriminals-ransomware-us-russia-sanctions); U.S. Department of the Treasury, Press Release, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," April 15, 2021. (https://home.treasury.gov/news/press-releases/jy0127)

Beyond sowing disinformation and hiding behind cyber proxies, Russia is adept at exploiting protections guaranteed under the U.S. Constitution. In a May 2018 speech, then-General Counsel of the National Security Agency (NSA) Glenn Gerstell raised the possibility that the Fourth Amendment (barring unreasonable searches and seizures) may hamstring U.S. efforts to stop cyberattacks when the hackers operate from within the United States. In effect, once foreign adversaries step onto U.S. shores (whether physically or virtually), they receive protections under the U.S. Constitution and cannot be surveilled to the same extent as when they are abroad.

Gerstell noted that U.S. "privacy laws in this area are generally backward looking,"[31] having failed to keep pace with rapidly evolving technology. For example, the legal definition of search and seizure has not adapted to account for when law enforcement authorities are pursuing bits or bytes that can be moved or destroyed in a millisecond. Nor has the law adequately grappled with what it means to be on U.S. soil when computer network infrastructure is global.

As Cyber Command and NSA chief General Paul Nakasone noted in March 2021 following the SolarWinds attack (described below), America's cyber adversaries understand and exploit legal constraints on U.S. authorities. The issue is not that U.S. intelligence and law enforcement "can't connect the dots," he explained. Rather, they "can't see all of the dots." Even when the intelligence community can "see what is occurring outside of the United States," America's "adversaries understand that they can come into the United States," use American internet service providers to conduct a malicious operation, and then quickly dismantle the infrastructure before U.S. civilian authorities can obtain a warrant and begin surveillance. Nakasone pleaded with lawmakers to enable the U.S. government (but not necessarily the NSA or Cyber Command) to increase its visibility into adversarial cyber-enabled attacks against government and private-sector entities.[32]

Case Studies

Russian cyber operations span a wide spectrum and exploit both software and hardware. While the motivations behind attacks vary, the capabilities employed reveal Russia's range of tools and how it exploits both SORM and the seams in American cyber defenses.

SolarWinds: Exploiting the Seams

Russia is exploiting attribution challenges and gaps in U.S. intelligence capabilities as it seeks to gain footholds throughout the global information technology supply chain. From these footholds, it can launch further cyber operations.[33] The SolarWinds operation provides a case in point.

In December 2020, the cybersecurity firm FireEye discovered that hackers, later determined to be associated with Russia's Foreign Intelligence Service (SVR), had compromised the Texas-based software company SolarWinds' Orion network management software. The hackers then used that access to produce and distribute malware to roughly 18,000 of the software's users across the U.S. government and private

31. Matthew Kahn, "NSA General Counsel Glenn Gerstell Remarks to Georgetown Cybersecurity Law Institute," *Lawfare*, May 24, 2018. (https://www.lawfareblog.com/nsa-general-counsel-glenn-gerstell-remarks-georgetown-cybersecurity-law-institute)
32. General Paul Nakasone, *Testimony Before the Senate Armed Services Committee*, March 25, 2021. (https://www.armed-services.senate.gov/imo/media/doc/21-17_03-25-20212.pdf)
33. Tim Starks, "Latest Russian espionage activity is broader then SolarWinds-style hacking effort, Microsoft's Tom Burt says," *CyberScoop*, October 25, 2021. (https://www.cyberscoop.com/tom-burt-q-and-a-russian-nobelium-resellers)

During a press briefing at the White House on February 17, 2021, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger tells reporters that nine federal agencies and around 100 companies were impacted by the SolarWinds hacking event. (Drew Angerer/Getty Images)

sector.[34] Once the victims inadvertently installed the Russian malware, the program deployed measures to evade detection,[35] then opened a backdoor through which the attackers conducted follow-on operations against select victims.[36] The Pentagon and intelligence agencies appear to be the only government bodies that avoided compromise. The hackers also compromised numerous private-sector entities, including major technology firms, hospitals, power companies, and financial institutions.[37]

While the malware's technical components helped prevent detection, there was a bigger problem: U.S. intelligence was nearly blind to the hackers' activity. Anne Neuberger, deputy national security advisor for cyber and emerging technology, plainly stated: "The intelligence community largely has no visibility into private-sector networks. The hackers launched the hack from inside the United States, which further made it difficult for the U.S. government to observe their activity."[38] The hackers seemed to understand this. They attacked at the seams of the U.S. government's authorities, jumping from foreign to U.S. infrastructure, renting servers from American "infrastructure-as-a-service" (IaaS) providers such as Amazon and GoDaddy before launching their intrusion.[39] In so doing, the hackers exploited the fact that domestic investigations are largely the purview of U.S. law enforcement and homeland security.

While the goal of the SolarWinds operation appears to have been espionage rather than a disruptive or destructive attack, the intelligence gleaned could undermine U.S. economic statecraft. For example, during the operation, the hackers searched U.S.

34. "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021. (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack); U.S. Federal Bureau of Investigation, Cybersecurity and Infrastructure Agency, Office of the Director of National Intelligence, and National Security Agency, Press Statement, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," January 5, 2021. (https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure)

35. Aaron Holmes, "5 takeaways from the Senate hearing on SolarWinds attacks," *Business Insider*, February 23, 2021. (https://www.businessinsider.com/5-takeaways-from-the-senate-hearing-on-solarwinds-attacks-2021-2)

36. U.S. Federal Bureau of Investigation, Cybersecurity and Infrastructure Agency, Office of the Director of National Intelligence, and National Security Agency, Press Statement, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," January 5, 2021. (https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure)

37. Maria Korolov, "The List of Known SolarWinds Victims Grows, as Do Attack Vectors," *Data Center Knowledge*, December 23, 2020. (https://www.datacenterknowledge.com/security/list-known-solarwinds-breach-victims-grows-do-attack-vectors)

38. Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, The White House, "Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021," *Remarks to the Press*, February 17, 2021. (https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021)

39. "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021. (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack)

government systems for information on potential sanctions against Russia.[40] Such information could allow potential Russian targets to better hide or secure their assets, reducing the effectiveness of U.S. sanctions.

Likewise, the hackers compromised the National Telecommunications and Information Administration, which advises the president on telecommunications policy, including internet and electromagnetic spectrum policy. Penetrating that organization could enable Moscow to identify companies the U.S. government believes are "untrusted vendors," thus enabling Russia to prioritize cyber-espionage against trusted vendors that will gain market share. Moscow could also glean how the U.S. government uses and prioritizes the electromagnetic spectrum, potentially enabling Russia to undermine U.S. government communications during a crisis.

"Even if initially intended merely for espionage, gaining access to internal systems establishes a 'beachhead' that Russian actors can use to exert influence, sow disinformation, or even launch disruptive or destructive attacks against the American economy."

Furthermore, Russian hackers could use this type of supply chain breach for a wide range of other nefarious purposes. Even if initially intended merely for espionage, gaining access to internal systems establishes a "beachhead" that Russian actors can use to exert influence, sow disinformation, or even launch disruptive or destructive attacks against the American economy.

As Zilberman warned in his 2018 study on Russian CEEW, the U.S. technology supply chain's vulnerability poses a growing threat to U.S. national security and economic prosperity.[41] After discovering the SolarWinds hack, the Biden administration took initial steps to address this threat, such as launching a supply chain review and issuing an executive order that increased cybersecurity and software transparency requirements for federal contractors.[42] Still, much more remains to be done.

Ransomware: Getting More Than Their Money's Worth

Ransomware groups are taking a toll on the U.S. economy as the frequency and severity of attacks skyrockets. Russia is home to many of the attackers.[43] As much as three quarters of all ransomware revenue in 2021 "went to organizations highly likely to be affiliated with Russia in some way," the blockchain data firm Chainalysis concluded.[44]

While the Russian government's role in these attacks remains unclear, Moscow has created a permissive

40. Joseph Menn and Christopher Bing, "Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes," *Reuters*, October 8, 2021. (https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07); "Microsoft Digital Defense Report," *Microsoft*, October 2021, page 59. (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi)

41. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, June 19, 2018, page 15. (https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare)

42. Executive Order 14017, "America's Supply Chains," February 24, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains); Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity)

43. Charlie Osborne, "LockBit ransomware operator: 'For a cybercriminal the best country is Russia," *ZeroDay Net*, February 4, 2021. (https://www.zdnet.com/article/lockbit-ransomware-operator-for-a-cybercriminal-the-best-country-is-russia)

44. "Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity," *Chainalysis*, February 14, 2022. (https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-russia-ransomware-money-laundering)

environment for cyber criminals.[45] A cache of leaked files from the Russia-based ransomware group Conti, for example, indicated these hackers enjoyed a mutual understanding with Russian authorities.[46] In return for making their services available to the state when required, Russian cybercriminals are generally free to continue hacking so long as they "don't ever work against [Russia or Russian] businesses," as Karen Kazaryan, CEO of the Moscow-based Internet Research Institute, put it. "If you steal something from Americans, that's fine."[47]

The chaos and damage these cybercriminals can cause was on full display in May 2021, when the Russia-based gang DarkSide launched a ransomware attack against Colonial Pipeline.[48] Colonial supplies over 45 percent of the fuel consumed on the U.S. East Coast and provides critical support for military, residential, and commercial facilities.[49] The U.S. government therefore considers Colonial Pipeline to be critical infrastructure — that is, infrastructure "considered so vital to the United States that [its] incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[50]

"The chaos and damage these cybercriminals can cause was on full display in May 2021, when the Russia-based gang DarkSide launched a ransomware attack against Colonial Pipeline."

On May 7, 2021, the hackers sent Colonial a note saying they had "exfiltrated" company data and encrypted its information technology systems, offering to return the files for $5 million.[51] The company immediately shut down all 5,500 miles of its pipelines to stop the malware's spread and to protect the company's operational networks.[52] Ultimately, Colonial paid the ransom after shutdowns caused gasoline shortages and major disruptions to land and air transportation across the East Coast, prompting the Federal Motor Carrier Safety Administration to declare a state of emergency.[53]

Less than two months later, another ransomware attack, this time attributed to the Russian ransomware group

45. Jeff Seldin, "US Accuses Russia of Stonewalling on Cybercrime," *Voice of America*, September 14, 2021. (https://www.voanews.com/a/6227401.html). See also: @ericgeller, "Harrington: 'We remain concerned that Russian cyber criminals will target U.S. critical infrastructure with ransomware attacks, either in support of Russian government or to take advantage of [the] more permissive operating environment in Russia,'" *Twitter*, May 24, 2022. (https://twitter.com/ericgeller/status/1529158808819355654)
46. Matt Burgess, "Leaked Ransomware Docs Show Conti Helping Putin from the Shadows," *Wired*, March 18, 2022. (https://www.wired.com/story/conti-ransomware-russia)
47. "How the Kremlin provides a safe harbor for Ransomware," *NBC News*, April 16, 2021. (https://www.nbcnews.com/tech/security/kremlin-provides-safe-harbor-ransomware-rcna699)
48. U.S. Federal Bureau of Investigation, Press Statement, "FBI Statement on Compromise of Colonial Pipeline Networks," May 10, 2021. (https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks)
49. Mike Jeffers and William Turton, "Ransomware attack shuts down biggest U.S. gasoline pipeline," *World Oil*, May 9, 2021. (https://www.worldoil.com/news/2021/5/9/ransomware-attack-shuts-down-biggest-us-gasoline-pipeline)
50. U.S. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," accessed June 24, 2022. (https://www.cisa.gov/critical-infrastructure-sectors)
51. Christina Wilkie, "Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate," *CNBC*, June 9, 2021. (https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html)
52. Joseph Blount, "Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure," *Testimony Before the House Committee on Homeland Security*, June 9, 2021. (https://homeland.house.gov/imo/media/doc/2021-06-09-HRG-Testimony-Blount.p)
53. "What We Know About the DarkSide Ransomware and the US Pipeline Attack," *Trend Micro*, May 12, 2021. (https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html)

REvil,[54] hit meat processing company JBS. The world's largest meat company by sales and the processor of one-fifth of America's meat supply, JBS paid the $11 million ransom.[55] President Joe Biden warned Putin to "take action" against Russia-based cybercriminals, threatening consequences if Russia failed to act.[56]

While Biden continued to raise these issues during bilateral conversations with Putin over the following six months,[57] U.S. officials found "no reduction in the overall pace of ransomware attacks" since the previous summer,[58] although attacks against high-profile targets apparently declined. "My guess is the Kremlin gave the message to criminals to stay off the front pages," said cyber expert Jim Lewis.[59] There is no public evidence, however, of such an order. It is equally likely that U.S. and allied counterattacks to confiscate ransomware profits and disable the network infrastructure of criminal groups convinced ransomware groups to refrain from attacking critical infrastructure.[60]

Unless held accountable by Washington and its allies, the Kremlin is unlikely to dismantle criminal enterprises that it can leverage for strategic gain. While Russia's security services might not be responsible for all cybercrime emanating from Russia, SORM ensures that Moscow knows who the perpetrators are. If it wanted, the Russian government could shut them down. The criminal activity has "served too many valuable purposes," Michael Daniels, a former White House cyber coordinator, noted.[61] Even the FSB's January 2022 arrest of REvil members, just as U.S.-Russia tensions were escalating ahead of the war in Ukraine, appeared to be geared toward sending a message to Washington, as opposed to cracking down on criminal hackers.[62] That message: Russia could be helpful against cybercriminals if America acquiesces to Russia's designs in Ukraine. As the war in Ukraine continued, Moscow

54. "REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says," *NPR*, June 3, 2021. (https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says)
55. Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," *The Wall Street Journal*, June 9, 2021. (https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781)
56. "Biden Tells Putin Russia Must Crack Down on Cybercriminals," *PBS*, July 9, 2021. (https://news.wttw.com/2021/07/09/biden-tells-putin-russia-must-crack-down-cybercriminals)
57. The White House, "Readout of Presidents Biden's Video Call with President Vladimir Putin of Russia," December 7, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/07/readout-of-president-bidens-video-call-with-president-vladimir-putin-of-russia)
58. Joseph Marks, "It's unclear whether Russia is cracking down on cyber attacks," *The Washington Post*, December 16, 2021. (https://www.washingtonpost.com/politics/2021/12/16/it-unclear-whether-russia-is-cracking-down-cyber-attacks). Data from private cybersecurity and cyber threat analysts reveals no decrease in the number of ransomware attacks. See: Adam Janofsky, "After a brief decline, organizations once again are bombarded with ransomware," *The Record*, April 13, 2022. (https://therecord.media/after-a-brief-decline-organizations-once-again-are-bombarded-with-ransomware)
59. Joseph Marks, "It's unclear whether Russia is cracking down on cyber attacks," *The Washington Post*, December 16, 2021. (https://www.washingtonpost.com/politics/2021/12/16/it-unclear-whether-russia-is-cracking-down-cyber-attacks)
60. Joseph Menn and Christopher Bing, "Exclusive: Governments turn tables on ransomware gang REvil by pushing it offline," *Reuters*, October 21, 2021. (https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21); U.S. Department of Justice, Press Release, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," June 7, 2021. (https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside); "FBI, US agencies look beyond indictments in cybercrime fight," *Associated Press*, January 18, 2022. (https://www.courthousenews.com/fbi-us-agencies-look-beyond-indictments-in-cybercrime-fight)
61. Joe Uchill, "Russia nixes US charges against REvil defendants as cooperation fizzles," *SC Media*, May 31, 2022. (https://www.scmagazine.com/analysis/ransomware/russia-nixes-us-charges-against-revil-defendants-as-cooperation-fizzles)
62. Jake Rudnitsky and William Turton, "Russia Detains REvil Ransomware Hackers at the Request of U.S.," *Bloomberg*, January 14, 2022. (https://www.bloomberg.com/news/articles/2022-01-14/russia-detains-revil-ransomware-hackers-at-u-s-s-request)

dropped the charges and reportedly explored recruiting the REvil hackers to work for the state.[63]

In addition to directly harming U.S. companies, ransomware attacks by Russia-based cybercriminals could support Russian intelligence collection. The hackers who attacked Colonial Pipeline obtained about 100GB of data on some 5,180 current and former Colonial employees, including personally identifiable information.[64] The FSB has a long history of using cybercriminals to collect intelligence abroad.[65] The FSB could also use SORM to obtain the data stolen by ransomware groups. Therefore, the United States should assume Moscow can use information stolen by cybercriminals to support CEEW or other cyber operations.

Recommendations

In his 2018 paper on Russian CEEW, Zilberman provided recommendations aimed at increasing private-sector awareness of the risks posed by Russian technology companies. He urged Washington to safeguard U.S. supply chains from malicious technology and to deny Russia access to advanced U.S. technology.[66]

Even prior to Russia's February 2022 invasion of Ukraine, the United States had done this. The Commerce Department has added Russian cyber entities to its growing Entity List, barring exports and re-exports of U.S. technology to designated entities and, in many circumstances, to Russia as a whole.[67] The Treasury Department has imposed sanctions prohibiting transactions with designated individuals or entities.[68] The Justice Department has charged numerous Russian state and criminal hackers.[69] The issue has been featured in public congressional hearings.[70] Since February, Washington has sanctioned numerous entities in the Russian technology sector, including ones supporting the Russian military.[71]

Moscow's CEEW strategy, however, is purposefully broad, employs a variety of actors, and feigns ignorance regarding cybercrime emanating from Russian territory. As such, the U.S. government not only needs new and

63. Joseph Marks, "Hopes of Russian help on ransomware are officially dead," *The Washington Post*, June 1, 2022. (https://www.washingtonpost.com/politics/2022/06/01/hopes-russian-help-ransomware-are-officially-dead)
64. "What's the latest fallout from the Colonial Pipeline hack?" *Government Technology*, August 17, 2021. (https://www.govtech.com/question-of-the-day/whats-the-latest-fallout-from-the-colonial-pipeline-hack)
65. See: U.S. Department of Justice, U.S. Attorney's Office for the Northern District of California, Press Release, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017. (https://www.justice.gov/usao-ndca/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and); Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017. (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html)
66. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, June 19, 2018, pages 17–18. (https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare)
67. Final Rule to the Export Administration Regulations (EAR) Adding Entities to the Commerce Entity List, U.S. Department of Commerce, Bureau of Industry and Security, 83 Federal Register 48532, September 26, 2018. (https://www.federalregister.gov/documents/2018/09/26/2018-20954/addition-of-certain-entities-to-the-entity-list-revision-of-an-entry-on-the-entity-list-and-removal)
68. U.S. Department of the Treasury, Press Release, "Treasury Takes Further Action Against Russian Linked Actors," January 11, 2021. (https://home.treasury.gov/news/press-releases/sm1232)
69. See, for example: U.S. Department of Justice, Press Release, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," October 19, 2020. (https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and)
70. Director of National Intelligence Daniel R. Coats, Office of the Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," *Statement for the Record Before the Senate Select Committee on Intelligence*, January 29, 2019. (https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf)
71. See, for example: U.S. Department of the Treasury, Press Release, "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," March 31, 2022. (https://home.treasury.gov/news/press-releases/jy0692)

flexible approaches to deterrence and mitigation but also better intelligence collection and analysis regarding Russia's CEEW playbook, including the role of SORM. It is also past time to consider whether and how some U.S. laws constructed prior to the cyber age may need to be revised.

1. **Resource and prioritize intelligence collection and analysis concerning Russian CEEW.** A better understanding of the officials and institutions directing and implementing Moscow's cyber policies, operations, and technological development will help Washington predict — and hopefully deter or defend against — future Russian CEEW activities. Washington should focus particularly on gaining a thorough understanding of SORM and the relationship between Russia's security services and the various cybercriminal groups operating in Russia.

2. **Require IaaS providers to "know your customer."** Today, legitimate and illegitimate actors alike are utilizing off-site servers, cloud storage, and virtual machines for operational simplicity. These IaaS providers offer servers, storage, and hardware on demand. Companies use IaaS providers instead of investing in their own network servers. By requiring IaaS providers to conduct due diligence on their clients, Washington can help prevent hackers from using American companies to support cyberattacks. This information could also help law enforcement agencies hunt down malicious cyber actors. Anti-money laundering laws require financial institutions and others to conduct "Know Your Customer" due diligence on potential clients and to continuously monitor those clients' use of their financial services. The U.S. government should require IaaS providers to do the same.

   The Trump administration attempted to address this challenge by issuing Executive Order 13984, mandating regulations that require IaaS providers to conduct due diligence on their customers.[72] President Biden wisely left the executive order in place.[73]

   This is a good first step, but Washington works best when the executive and legislative branches act in unison. Executive Order 13984 would function better as a statute, with strict penalties for violations. Congressional hearings can further help to assess the threat IaaS poses and to produce effective legislation to counter it.

3. **Conduct studies on the tradeoffs between privacy and security for intelligence collection against adversarial foreign persons.** In the years before the 9/11 attacks, al-Qaeda realized the United States had a vulnerable gap between law enforcement and intelligence authorities — a gap the terrorists exploited to deadly effect. Following 9/11, the legislative and executive branches worked collaboratively to help prevent future attacks against the homeland.

   Today, by using IaaS providers to launch attacks, hackers can evade U.S. intelligence agencies, which cannot surveil domestic entities and individuals in the same way they can against targets abroad. As then-National Security Advisor Robert O'Brien stated in January 2021, "abuse of United States IaaS products" by malign cyber actors "has played a role in every cyber incident during the last four years, including the actions resulting in the penetrations of the United States firms FireEye and SolarWinds."[74] The

72. Paul Amberg, Eunkyung Kim Shin, Brian Hengesbaugh, Michael Stoker, and Yu (Iris) Zhang, "US Government Issues Executive Order to Address the Use of US IaaS Products by Foreign Malicious Cyber Actors," *Sanctions and Export Controls Update*, February 9, 2021. (https://sanctionsnews.bakermckenzie.com/us-government-issues-executive-order-to-address-the-use-of-us-iaas-products-by-foreign-malicious-cyber-actors)

73. U.S. Department of Commerce, Press Release, "Commerce Department Seeks Input in Development of Cyber Rules to Deter Malicious Use of Cloud Services," September 24, 2021. (https://www.commerce.gov/news/press-releases/2021/09/commerce-department-seeks-input-development-cyber-rules-deter-malicious)

74. National Security Advisor Robert C. O'Brien, U.S. National Security Council, Press Statement, "Statement from National Security Advisor Robert C. O'Brien," January 19, 2021. (https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011921)

executive and legislative branches must again wrestle with the authorities governing intelligence and law enforcement activity, both at home and abroad.

As technology evolves and surveillance by states, non-state actors, and private companies becomes more ubiquitous, the debate regarding privacy and security will only grow more heated. In the context of understanding and deterring Russian CEEW, however, one should frame the security vs. privacy debate through the lens of whether current Foreign Intelligence Surveillance Act requirements limit the intelligence community's ability to collect against valid foreign targets once they arrive in the United States. U.S. adversaries know how to exploit these constraints. Congress should mandate a commission or direct government agencies to conduct an in-depth study of the costs and benefits of the prohibition against collection against non-U.S. persons physically or virtually located inside the United States. The first step in fixing this problem is to understand the current legal framework's tradeoffs and limitations.

4. **Increase analysis and public awareness of Russian CEEW information operations.** Part of Washington's challenge in countering Russian CEEW stems from a lack of understanding across the executive and legislative branches and by the American public. The U.S. National Counterintelligence Strategy for 2020–2022 noted that "defend[ing] against hybrid attack methods that involve supply chain, cyber, technical means and insider enabled attacks" requires, among other things, "deepening our understanding of our adversaries' cyber and technical threat intent and capability." It also necessitates "work[ing] across the whole-of-government, the private sector, and the American public to enhance mechanisms for information sharing and implement more effective defenses."[75]

   Congress and the executive branch must work together to fully resource and implement that strategy. For example, the aforementioned strategy notes that to achieve its goals, the intelligence community must "[d]evelop, train, and retain a cadre of cyber counterintelligence and technical security experts" to "allow for more rapid recognition of threats and vulnerabilities, and more agile responses and integrated approaches to counter adversary cyber and technical activities." The intelligence community also needs "new capabilities to track and counter foreign cyber and technical operations against the United States and leverage partnerships with the private sector to develop effective countermeasures."[76]

5. **Enhance cyber diplomacy to combat ransomware and other cyber threats from Russia.** Given its SORM capabilities, Moscow likely knows who is responsible for the cybercrime emanating from its borders but is unlikely to do anything about it. Washington needs a more robust diplomatic engagement strategy with U.S. allies to combat ransomware attacks and other cybercrimes originating in Russia.

   Until recently, there had been no individual at the State Department with both the appropriate seniority and exclusive mission to take on this problem. In April, the department inaugurated its new Bureau of Cyberspace and Digital Policy, realigning teams across the department.[77] A Senate-confirmed ambassador will lead the bureau. Congress should codify this new bureau into law. With congressional backing, the bureau and its leader can marshal the bureaucracy to communicate U.S. positions on cyber policy and rally U.S. allies to combat cyber challenges. This could include a concentrated effort

75. Office of the Director of National Intelligence, National Counterintelligence and Security Center, "National Counterintelligence Strategy of the United States of America 2020-2022," January 2020, page 10. (https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf)
76. Ibid.
77. Aaron Schaffer, "It's a big day at the State Department for U.S. cyberdiplomacy," *The Washington Post*, April 4, 2022. (https://www.washingtonpost.com/politics/2022/04/04/its-big-day-state-department-us-cyberdiplomacy)

at the United Nations, the Organization for Security and Cooperation in Europe, and elsewhere. It should also include ensuring European governments and companies understand SORM and how it puts European privacy at risk. The head of the new bureau should also lead efforts to counter the proliferation of SORM-related technologies and legal frameworks in developing countries.

Finally, Washington should also establish an Interagency Working Group (IWG) for ransomware, as recommended by the Ransomware Task Force. The task force stated that the National Security Council, Office of the National Cyber Director, State Department, Department of Homeland Security, Justice Department, Treasury Department, and other relevant IWG members "should engage international allies and partners to build a like-minded coalition against ransomware and ensure policy coordination." The U.S. government should also "establish an international coalition to combat ransomware criminals" by "building [the] legal case against criminal actors, pursuing targets/groups through pooling resources and tools, and amplifying takedowns when they happen."[78]

Conclusion

In 1972, the late RAND analyst Andrew Marshall (who later created the Pentagon's Office of Net Assessment, which he ran for more than 40 years) wrote a classified report titled "Long-Term Competition with the Soviets: A Framework for Strategic Analysis." Declassified in 2010, the report argued that Washington needed "improved models of Soviet decisionmaking processes," and that more "account must be taken of the fact that Soviet force posture emerges … from a complex decisionmaking process involving many organizations with conflicting goals."[79]

Today's challenge is to understand Moscow's CEEW decision-making process from the ground up — the technology on which it depends to gather data (SORM); the advantages Russian hackers perceive and exploit in the gaps in U.S. law enforcement and intelligence gathering authorities; and the personnel and policies that direct and operationalize Russian cyber and information operations. As Marshall surmised in that Cold War treatise, the U.S.-Soviet "competition will be prolonged — indeed, for planning purposes, endless." So, too, with the challenge America faces from Russian CEEW.

78. Ransomware Task Force, "Combating Ransomware," *Institute for Security and Technology*, May 2021, pages 21–22. (https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf)
79. Andrew W. Marshall, "Long-Term Competition with the Soviets," *RAND Corporation*, April 1972. (https://www.rand.org/pubs/reports/R862.html)

CHINA'S ACCELERATING CEEW CAMPAIGN

By Samantha F. Ravich and RADM (Ret.) Mark Montgomery

Introduction[80]

In the four years since the Foundation for Defense of Democracies published its first study on Chinese CEEW,[81] the United States and the People's Republic of China have remained locked in a long-term struggle for political, military, and economic dominance. As the United States endeavors to lead and preserve the international order, Beijing seeks to alter global dynamics to promote its interests while diminishing the influence of the United States and other free-market democracies.[82] Accordingly, China's use of CEEW has increased in scope, scale, and frequency.

80. The authors would like to thank John Costello for the exceptional research and expertise he contributed to this paper prior to joining the Office of the National Cyber Director.

81. Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, September 5, 2018. (https://www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare)

82. Vijay Gokhale, "China is Gnawing at Democracy's Roots Worldwide," *Foreign Policy*, December 18, 2020. (https://foreignpolicy.com/2020/12/18/china-democracy-ideology-communist-party)

Beijing's approach to CEEW combines IP theft, economic coercion, critical-infrastructure disruption, and the large-scale collection of personally identifiable information of U.S. citizens. For the United States and allied countries to deter and confront Chinese CEEW, they must understand how Beijing views this toolset. This chapter therefore begins by delving into the Chinese military doctrine that undergirds Beijing's approach to CEEW.

While other adversaries simply seek to weaken the United States and its allies, China also seeks to control the infrastructure of the global economy. Beijing's plan to dominate the global ICT domain is one of the clearest examples of CEEW in action. To that end, China is planting its equipment throughout the global infrastructure and then leveraging that equipment to gather, manipulate, or otherwise control the vast amounts of data moving through the system.[83]

Yet Beijing is not just looking to control data flows. Beijing is also pursuing self-reliance and eventual dominance over ICT. To mitigate its susceptibility to U.S. influence, China wants to become leader in the development of new technology instead of just an importer of technology and manufacturer of final goods.[84] To that end, Beijing combines state-directed support for national champions and barriers against foreign firms operating within its borders with illicit and hostile CEEW activities such as IP theft, cyber manipulation, and economic coercion. Altogether, China has implemented a coherent long-term strategy to control key nodes in the global economy and communications infrastructure — all at the expense of the United States and its allies.

Chinese CEEW, Political Warfare, and 'Winning Without Fighting'

CEEW is an American concept that aligns with the Chinese approach to strategic competition. In that context, CEEW is effectively a subset of Beijing's long-standing approach to political warfare (政治战), as encapsulated by the "Three Warfares" (三战) doctrine first enunciated by the People's Liberation Army (PLA) in 2003. These three techniques — public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战)[85] — are intended to shape domestic and foreign attitudes and perceptions in ways that advance China's interests and constrain the political and military options of China's opponents during times of peace, crisis, and conflict.[86] For Chinese analysts, a principal advantage of CEEW and other forms of political warfare is their potential to exploit American vulnerabilities while avoiding escalation to war.

In Chinese texts, political warfare goes beyond media or propaganda operations to include all direct and indirect means of manipulation. While Chinese political-warfare literature does not directly address in depth the fusion of cyber and economic tools, Chinese analysts consider these tools, used alone or together, to be powerful means of influencing public opinion, altering an adversary's political environment, and diminishing its resolve in a crisis.[87] More importantly, CEEW techniques reduce the risk of a conventional military confrontation — a domain where China feels, at least for now, unprepared to challenge the United States and its allies.

83. Samantha F. Ravich and Annie Fixler, "The Economic Dimension of Great-Power Competition and the Role of Cyber as a Key Strategic Weapon," *Heritage Foundation*, October 30, 2019. (https://www.heritage.org/military-strength/topical-essays/the-economic-dimension-great-power-competition-and-the-role)
84. James Andrew Lewis, "China's Pursuit of Semiconductor Independence," *Center for Strategic and International Studies*, February 27, 2019. (https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence)
85. Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018. (https://warontherocks.com/2018/01/chinas-three-warfares-perspective)
86. Wu Jieming and Liu Zhifu, 舆论战心理战法律战概论 [*An Introduction to Public Opinion Warfare, Psychological Warfare, and Legal Warfare*] (Beijing: National Defense University Press, 2014), page 11.
87. Ibid., page 100.

China's long-established concept of "winning without fighting" (不战而胜) favors indirect or unconventional methods to achieve strategic objectives while avoiding unnecessary escalation or crises.[88] Chinese strategists argue that the globalization of economics and information flows has "significantly increased the restriction of warfare," channeling countries toward smaller conflicts or non-military confrontations, to which Chinese political warfare is uniquely suited.[89] For example, cyberattacks can exert "a direct and powerful influence" on an adversary's economic system, precipitating social, economic, or political collapse.[90]

While Chinese scholars believe the United States is adept at deploying unconventional or "hybrid" warfare, they also recognize that America and its allies face considerable difficulty when it is used against them.[91] These scholars cite the 2014 Russian invasion of Crimea as a notable example.[92] Another theme in Chinese views of the United States is that America's prevailing strengths can, with the right tools, become vulnerabilities that Beijing can exploit via asymmetric cyber operations and cyber-enabled economic coercion.

Chinese strategists see the U.S. political system and private sector as principal areas of vulnerability. Many Chinese scholars have asserted that economic disruptions would be particularly effective in undermining America's political resolve during a crisis, since the party out of power would blame the incumbent administration amidst mounting economic losses.[93] Beijing also believes it can leverage U.S. industry to advance China's objectives — or at least temper U.S. actions that would harm Chinese interests. Vice Foreign Minister Xie Feng, for example, urged U.S. businesses to push the U.S. government to pursue more CCP-friendly policies, warning that businesses cannot expect to "make a fortune in silence."[94]

"America's prevailing strengths can, with the right tools, become vulnerabilities that Beijing can exploit via asymmetric cyber operations and cyber-enabled economic coercion."

Chinese authors also view cyber and economic tools as useful means to test the reliability of U.S. security guarantees. PLA military theorists discuss the concept of a "divide, break, and exploit" (分化瓦解，酌情利用) economic policy that seeks to create division and discord among U.S.-led coalitions.[95] In this scenario, China would utilize CEEW techniques, coupled with traditional economic coercion that falls below the threshold of armed conflict, to show that America's allies cannot rely on U.S. protection. Absent a threat of physical harm to U.S. citizens or military personnel, the thinking goes, American politicians, voters, and corporate leaders would see little benefit in defending a foreign country against economic coercion.

88. Sun Tzu emphasized "subduing the enemy's troops without fighting" (不战而屈人之兵), a dictum expanded by Mao Zedong in his guerilla tactics: "the elimination of the enemy is to remove the enemy's arms, which is also so-called 'depriving the enemy's strength to resist' and not to completely eliminate their flesh." See: 战略学 [*Science of Military Strategy*], Ed. Shou Xiaosong (Beijing: Academy of Military Sciences Press, 2013), pages 109–110. (https://nuke.fas.org/guide/china/sms-2013.pdf)
89. Wu Jieming and Liu Zhifu, 舆论战心理战法律战概论 [*An Introduction to Public Opinion Warfare, Psychological Warfare, and Legal Warfare*] (Beijing: National Defense University Press, 2014), page 123.
90. Ibid., pages 166–167.
91. Li Shuyin, "俄罗斯发力混合战争 [Russia Gives Force to Hybrid Warfare]," *PLA Daily* (China), February 19, 2016. (http://www.71.cn/2016/0219/864616.shtml)
92. Ni Haining, "军事理论创新要把握三个维度 [Military Theory Innovation Must Grasp the Third Dimension]," *PLA Daily* (China), March 23, 2016. (http://www.xinhuanet.com/mil/2016-03/23/c_128825477.htm)
93. See, for example: Xu Dianqing and Li Xin, 中国不怕 [*China Is Not Scared*] (Beijing: Social Sciences Academic Press, 2011), page 107.
94. Helen Davidson, "Beijing warns China-Linked U.S. Businesses: You Cannot 'Make a Fortune in Silence,'" *The Guardian* (UK), December 2, 2021. (https://www.theguardian.com/world/2021/dec/02/beijing-warns-china-linked-us-businesses-you-cannot-make-a-fortune-in-silence)
95. 高技术战争经济论 [*Economic Theory of High-Technology Warfare*], Eds. Song Fangmin and Zhang Wenyuan (Beijing: Academy of Military Sciences Press, 2003), page 388.

CEEW Techniques

IP Theft

Cyber-enabled IP theft is the most well-recognized and longstanding CEEW tactic employed by the CCP. Beijing "continues to use cyber espionage to support its strategic development goals—science and technology advancement, military modernization, and economic policy objectives," the U.S. intelligence community reported in 2018.[96] A U.S. government assessment in June 2021 confirmed that China is "aggressively" targeting U.S. and allied technology, both commercial and military.[97]

Despite a dip in Chinese IP theft following the 2015 summit between President Barack Obama and Chinese leader Xi Jinping, cybersecurity researchers and the U.S. government have seen a resurgence of Chinese cyber intrusions beginning in 2017 and continuing today.[98] In the fall of 2021, U.S. Trade Representative Katherine Tai stated that the Biden administration was prepared to "build on" existing tariffs against China first imposed under the Trump administration in response to China's IP theft and unfair practices related to technology transfer.[99] She said the phase one agreement between the United States and China meant to alleviate these issues has "not meaningfully address[ed] the fundamental concerns that we have with China's trade practices."[100] Six months later, the Office of the U.S. Trade Representative's annual IP report continued to rank China among the most egregious violators.[101]

The People's Republic of China strives to weaken IP protection via Chinese courts. Specifically, Beijing is using "anti-suit injunctions" to block foreign companies from taking legal action to protect trade secrets. In one case, Xiaomi, a large Chinese consumer electronics and smartphone producer, secured an injunction barring Delaware-based InterDigital from pursuing a patent infringement case against Xiaomi, not only in China but worldwide. A Chinese court ruled that if InterDigital continued to press its legal rights, the company would be fined nearly $1 million per week.[102]

Critical-Infrastructure Intrusions

Cyber-enabled critical-infrastructure disruption is a focal point of Chinese military literature. Military theorist Ye Zheng argues that cyber operations against critical infrastructure can generate "space and time on the battlefield," delaying and confounding an adversary's response until Chinese forces can establish a new status quo for concessions and negotiation.[103] While focused

96. Office of the Director of National Intelligence, "Foreign Economic Espionage in Cyberspace," 2018, page 7. (https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)
97. Sean Lyngaas, "US Agencies Circulate Warning about 'Aggressive' Chinese Hacking Effort to Steal Secrets from a Range of Targets," *CyberScoop*, July 16, 2021. (https://www.cyberscoop.com/china-hacking-fbi-biden-alert-ip)
98. Office of the United States Trade Representative, "Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation," November 20, 2018, page 11. (https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf); Sean Gallagher, "New Data Shows China has 'Taken the Gloves Off' in Hacking Attacks on US," *ARSTechnica*, November 1, 2018. (https://arstechnica.com/information-technology/2018/11/new-data-shows-china-has-taken-the-gloves-off-in-hacking-attacks-on-us); "Update 1-U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," *Reuters*, November 9, 2018. (https://www.reuters.com/article/usa-china-cyber-idUKL2N1XK06K)
99. Steven Overly, "U.S. trade chief: Biden will build from Trump-era tariffs to confront China," *Politico*, September 30, 2021. (https://www.politico.com/news/2021/09/30/biden-trump-tariffs-china-514866)
100. Ambassador Katherine Tai, "New Approach to the U.S.-China Trade Relationship," *Remarks Delivered at the Center for Strategic and International Studies*, October 4, 2021. (https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2021/october/remarks-prepared-delivery-ambassador-katherine-tai-outlining-biden-harris-administrations-new)
101. Ana Swanson, "China Continues to Fall Short of Promises to Protect Intellectual Property, U.S. Says," *The New York Times*, April 27, 2022. (https://www.nytimes.com/2022/04/27/business/economy/china-trade-intellectual-property.html)
102. Josh Zumbrun, "China Wields New Legal Weapon to Fight Claims of Intellectual Property Theft," *The Wall Street Journal*, September 26, 2021. (https://www.wsj.com/articles/china-wields-new-legal-weapon-to-fight-claims-of-intellectual-property-theft-11632654001)
103. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," *National Defense University*, October 2018, page 47. (https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf)

on targeted disruptions of critical infrastructure that supports adversary military capabilities, Chinese strategists acknowledge that such disruptions may "sow fear and panic amongst the enemy," "compel adversaries away from rash activities," and "paralyze a nation's economy and sow societal disorder, allowing one country to impose its will upon the other."[104]

China's conception of military conflict in cyberspace blurs the distinction between peace and war. As Zheng notes, "the strategic game in cyberspace is not limited by time and space, does not distinguish between peace and war, and has no frontline and homefront."[105] In CEEW, the ability to coerce an adversary through critical-infrastructure disruption in wartime is contingent upon cyber intrusions conducted in peacetime.

Despite this emphasis in the literature, the PLA has been relatively slow to operationalize critical-infrastructure disruption in its cyber operations — at least compared to other sophisticated adversaries, such as Russia.[106] The Biden administration revealed last year that between 2011 and 2013, China compromised nearly two dozen U.S. oil and natural gas pipelines, potentially to disrupt or damage their operation.[107] In 2014, then-NSA Director Mike Rogers stated that China, along with Russia, was capable of mounting cyberattacks against the U.S. electric grid.[108]

Since then, China's investment in such operations has accelerated sharply, and critical-infrastructure intrusions by Chinese cyber actors have increased. In 2019, the Office of the Director of National Intelligence reported publicly for the first time that Chinese cyber actors could "launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure," and singled out oil and natural gas pipelines as a sector that could be disrupted for days or even weeks.[109] The U.S. intelligence community reaffirmed this in 2021.[110]

Cyberattacks on critical infrastructure could disrupt a U.S. military mobilization in defense of Taiwan or interfere with other military operations by China's adversaries.[111] In mid-2020, amid border skirmishes with India, suspected Chinese actors targeted Indian critical-infrastructure sites, including "a dozen critical nodes across the Indian power generation and transmission infrastructure" as well as two Indian seaports.[112] These intrusions may have caused power outages in Mumbai in October 2020, which effectively halted economic activity within one of

104. *Lectures on Joint Campaign Information Operations* [联合战役信息作战教程], Ed. Yuan Wenxian (Beijing: Military Science Press, 2009), page 109. Yuan Wenxian served as the director of the Information Operations and Command Training Teaching and Research Department of the PLA National Defense University.
105. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," *National Defense University*, October 2018, page 45. (https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf)
106. Tim Starks, "'Almost Every Nation' Now has Cyber Vulnerability Exploitation Program, NSA Official Says," *CyberScoop*, September 29, 2021. (https://www.cyberscoop.com/rob-joyce-nsa-cyber-exploitation-program)
107. Dustin Volz, "China Compromised U.S. Pipelines in Decade-Old Cyberattack, U.S. Says," *The Wall Street Journal*, July 20, 2021. (https://www.wsj.com/articles/new-pipeline-cybersecurity-requirements-issued-by-biden-administration-11626786802)
108. Ken Dilanian, "NSA Director: China can Damage US Power Grid," *Associated Press*, November 20, 2014. (https://apnews.com/article/cb45fcf4e9c9453d8fb0098e445ae425)
109. Director of National Intelligence Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," *Statement for the Record Before the Senate Select Committee on Intelligence*, January 29, 2019, page 5. (https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf)
110. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, page 5. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf)
111. James Mulvenon, *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND Corporation, 1999), page 176.
112. David Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, September 27, 2021. (https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html); Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," *Recorded Future*, February 28, 2021. (https://www.recordedfuture.com/redecho-targeting-indian-power-sector)

India's major economic centers,[113] although the linkage remains unconfirmed.

Cyber-Enabled Economic Coercion

FDD's 2018 report on Chinese CEEW detailed Beijing's use of cyber-enabled economic coercion, drawing attention to attacks on the South Korean conglomerate Lotte Group after the company agreed to let Seoul use a Lotte-owned golf course for U.S. missile defense deployments.[114] Chinese actors continue to use this tactic, which seeks to compel action rather than cause disruption or chaos. Weeks after Nairobi rejected a free trade agreement between the East African Community countries and Beijing in May 2018, for example, Chinese actors began aggressively conducting cyber intrusions against Kenya.[115] There is no indication, however, that this tactic succeeded in changing Kenya's policies.[116]

It can be difficult to distinguish cyber-enabled economic coercion from traditional cyber-espionage, including intelligence gathering for advantage in economic negotiations. While the United States should not tolerate adversaries' espionage operations, they warrant a different response than attempted (or successful) coercion.

Mass Collection of Personally Identifiable Information

Since China's 2014 hacks of the Office of Personnel Management and health insurance company Anthem, Chinese cyber actors have only increased efforts to steal the personally identifiable information,[117] personal health information,[118] and financial records[119] of U.S. citizens.[120] In 2020, the Department of Homeland Security assessed that China will continue to use "cyber espionage to steal … personally identifiable information (PII) from U.S. businesses and government agencies to bolster their civil-military industrial development, gain an economic advantage, and support intelligence operations."[121]

While the long-term objectives of these data breaches are not entirely clear, U.S. officials and analysts theorize that China is building a large database of U.S. citizens to identify targets for espionage operations, such as

113. Sahil Joshi and Divyesh Singh, "Mega Mumbai Power Outage may be Result of Cyber Attack, Final Report Awaited," *India Today* (India), November 20, 2020. (https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20)
114. Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, September 5, 2018. (https://www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare)
115. Business Daily, "Kenya Rejects China-EAC Free Trade Agreement," *The East African* (Africa), May 15, 2018. (https://www.theeastafrican.co.ke/business/Kenya-rejects-China-EAC-free-trade-agreement/2560-4562142-x5dhrgz/index.html); Justin Lynch, "China is Hacking the Same Countries it Trades with," *C4ISRNET*, August 14, 2018. (https://www.fifthdomain.com/international/2018/08/17/china-is-hacking-countries-is-trades-with)
116. Duncan Miriri, "China Ready for Trade Talks with East Africa Bloc: Ambassador to Kenya," *Reuters*, June 10, 2019. (https://www.reuters.com/article/us-kenya-china-trade/china-ready-for-trade-talks-with-east-africa-bloc-ambassador-to-kenya-idUSKCN1TB1EC)
117. David E. Sanger, Nicole Perlroth, Glenn Thrush, and Alan Rappeport, "Marriott Data Breach is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *The New York Times*, December 11, 2018. (https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html)
118. U.S. Department of Justice, Press Release, "Member of Sophisticated China-Based Hacking Group Indicated for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," May 9, 2019. (https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including)
119. U.S. Department of Justice, Press Release, "Chinese Military Personnel Charger with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," February 10, 2020. (https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking)
120. Ellen Nakashima, "With a Series of Major Hacks, China Builds a Database on Americans," *The Washington Post*, June 5, 2015. (https://www.washingtonpost.com/world/national-security/in-a-series-of-hackschina-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fdd580f1c5d44e_story.html)
121. U.S. Department of Homeland Security, "Homeland Threat Assessment," October 2020, page 8. (https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf)

military members, federal employees, or executives in strategic industries.[122] This could amplify the impact of both commercial espionage and CEEW.

China's data harvesting may also advance China's artificial intelligence (AI) capabilities. AI needs large data sets on which to train to compute faster and develop more useful insights.[123] The National Security Commission on Artificial Intelligence warned that "adversaries' systematic efforts to harvest data on U.S. companies, individuals, and the government is about more than traditional espionage." Illegally acquired data combined with commercial data could enable China to "monitor, control, and coerce" individuals beyond its borders. The report warns, "Personal and commercial vulnerabilities become national security weaknesses as adversaries map individuals, networks, and social fissures in society; predict responses to different stimuli; and model how best to manipulate behavior or cause harm."[124]

China Seeks Control of ICT

Control of global ICT infrastructure and its constituent technologies, supply chains, and services is a central front in the competition between Washington and Beijing. ICT includes 5G and other telecommunications equipment as well as satellite navigation, cloud computing, and integrated circuits. Leadership in this field figures prominently in each country's long-term economic and military development.

China's 14th Five Year Plan (FYP), announced in March 2021, is a key indicator of Beijing's global ambitions in ICT.[125] The country's National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020),[126] the 13th FYP,[127] and Made in China 2025[128] have all stressed the need for China to adopt an "innovation-driven" economic model. The 14th FYP, however, demonstrates a marked shift in tone, stressing a reduction in Chinese dependence on foreign technology through greater "self-reliance." The 14th FYP makes clear China's future economic and national security are inextricably linked to control and influence over the global technology environment. Most importantly, the CCP believes that U.S.-controlled or dominated global ICT industry threatens China's national security.

In Beijing's view, the United States has abused its leadership in ICT to conduct global surveillance, undercut China's economic ambitions, and thereby stymie China's rise. The contents of the Edward Snowden leaks in 2013, which alleged the United States leveraged its technology companies for global surveillance and reconnaissance, remain a lens through which China views the battlespace. Its strategic literature is rife with information security concerns stemming from U.S. dominance in technology. Chinese

122. Ellen Nakashima, "With a Series of Major Attacks, China Builds a Database on Americans," *The Washington Post*, June 5, 2015. (https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html)
123. Samantha Ravich, "Artificial Intelligence and the Adversary," *The Wall Street Journal*, December 3, 2019. (https://www.wsj.com/articles/artificial-intelligence-and-the-adversary-11575417680)
124. U.S. National Security Commission on Artificial Intelligence, "Final Report," March 19, 2021, pages 49–50 (https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf)
125. "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," *Xinhua News Agency* (China), March 12, 2021. (https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf)
126. PRC State Council, "The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)," 2006. (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf)
127. Wen Ya, "中华人民共和国国民经济和社会发展第十三个五年规划纲要 [Outline of the Thirteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China]," *Xinhua News Agency* (China), March 17, 2016. (http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm)
128. U.S. Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protections," 2017. (https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf)

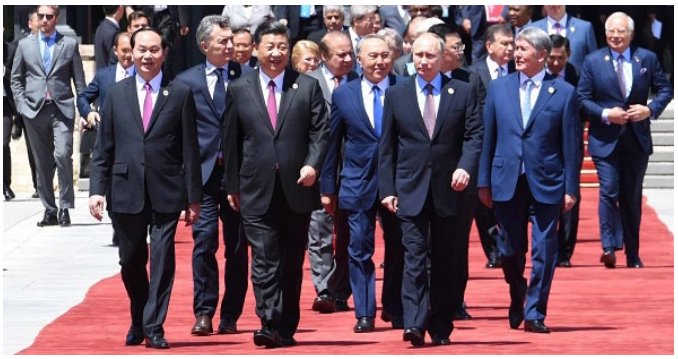
officials have repeatedly dismissed U.S. concerns about Huawei, ZTE, and other PRC national champions as hypocritical.[129] In response to tariffs and increased export controls on Chinese semiconductors, Chinese officials also accused Washington of protectionism.[130]

Such accusations draw a false equivalence between U.S. and Chinese actions but reflect Beijing's goal of controlling the ICT infrastructure. As such, China has poured billions of dollars into the expansion of its ICT industry, to include 5G and semiconductors. In 2019, China established an Advanced Manufacturing Fund of $20.9 billion[131] and a National Semiconductor Fund of $28.9 billion.[132] In 2020, China's foremost producer of integrated circuits, the Semiconductor Manufacturing International Co., received $2.25 billion in financing from state-backed funds.[133] Additionally, in response to expanded U.S. export controls, the Finance Ministry introduced a two-year waiver on corporate tax payments for software developers and integrated circuit manufacturers.[134]

Huawei, the bellwether of China's tech giants and a perennial target for those concerned about Chinese influence over ICT, best illustrates the role of state financing. According to *The Wall Street Journal*, Huawei has received more than $75 billion in state-backed aid, including more than $45 billion in loans and credit lines from government lenders, tax breaks worth $25 billion, $1.6 billion in grants, and $2 billion in land discounts.[135] This has allowed the company to invest far more in research and development than its competitors, including some $15 billion in 2018.[136] Additionally, subsidies and preferential financing have allowed Huawei to lower its prices, undercutting competitors by up to 30 percent in a bid to achieve rapid market penetration and expand globally.[137]

When the United States pushed its allies to restrict Huawei's entry into their 5G infrastructure, they initially balked at the higher prices of other providers.[138] Washington was ultimately successful and reduced Huawei's global market share,[139] but it will take a similarly significant diplomatic campaign (combined with export controls or other restrictions that reduce Chinese access to critical component technology) for the United States to push back against China's efforts to control other parts of the global ICT infrastructure and supply chain. If, for example, China were to establish a microchip production capability on par with that of Western companies, Beijing would likely try to control exports of raw materials, undercut market prices, and

129. Arjun Kharpal, "China Accuses US of Hypocrisy over Huawei, Highlighting Claims it Spied on German Leader Merkel," *CNBC*, February 17, 2020. (https://www.cnbc.com/2020/02/17/china-accuses-us-of-hypocrisy-over-huawei-says-it-spied-on-merkel.html)
130. Catherine Wong, "China will Increase Support, Subsidies for Tech Firms, Officials Says," *South China Morning Post* (Hong Kong), May 24, 2019. (https://www.scmp.com/news/china/politics/article/3011715/china-will-increase-support-subsidies-tech-firms-official-says)
131. Yoko Kubato, "China's New $21 Billion High Tech Manufacturing Fund Likely to Rankle U.S.," *The Wall Street Journal*, November 20, 2019. (https://www.wsj.com/articles/chinas-new-21-billion-high-tech-manufacturing-fund-likely-to-rankle-u-s-11574250074)
132. Yoko Kubato, "China Sets Up New $29 Billion Semiconductor Fund," *The Wall Street Journal*, October 25, 2019. (https://www.wsj.com/articles/china-sets-up-new-29-billion-semiconductor-fund-11572034480?mod=article_inline)
133. Yusho Cho, "Eyeing US, China Wields $33bn Subsidies to Bolster Chips, Defense," *Nikkei Asia* (Japan), May 17, 2021. (https://asia.nikkei.com/Politics/International-relations/US-China-tensions/Eyeing-US-China-wields-33bn-subsidies-to-bolster-chips-defense)
134. Catherine Wong, "China will Increase Support, Subsidies for Tech Firms, Officials Says," *South China Morning Post* (Hong Kong), May 24, 2019. (https://www.scmp.com/news/china/politics/article/3011715/china-will-increase-support-subsidies-tech-firms-official-says)
135. Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *The Wall Street Journal*, December 25, 2019. (https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736)
136. "No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge," *Bloomberg*, April 25, 2019. (https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g)
137. Lindsay Maizland and Andrew Chatzky, "Huawei: China's controversial Tech Giant," *Council on Foreign Relations*, August 6, 2020. (https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant#chapter-title-0-5)
138. Gwenaelle Barzic, "Europe's 5G to cost $62 Billion more if Chinese Vendor Banned: Telcos," *Reuters*, June 7, 2019. (https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3)
139. Dan Strumpf, "U.S. Set Out to Hobble China's Huawei, and so it has," *The Wall Street Journal*, October 7, 2021. (https://www.wsj.com/articles/u-s-set-out-to-hobble-chinas-huawei-and-so-it-has-11633617478?redirect=amp#click=https://t.co/ZYiPfiuJX2)



Chinese leader Xi Jinping meets with foreign delegation heads and guests after the first session of the Leaders' Roundtable Summit at the Belt and Road Forum for International Cooperation on May 15, 2017, in Beijing, China. (Xinhua/Rao Aimin via Getty Images)

otherwise undermine Western firms to drive them from the field.[140]

The CCP's foreign aid and development strategies also support its desire to dominate in ICT. The Digital Silk Road (数字丝绸之路; DSR)[141] campaign, an initiative Beijing launched in 2015 to complement the physical infrastructure projects of the Belt and Road Initiative (一带一路; BRI), focuses on building "China-centric digital infrastructure, exporting industrial overcapacity, [and] facilitating the expansion of Chinese technology corporations," among other objectives.[142] One of the DSR's four major projects entails investing in "digital infrastructure abroad, including next-generation cellular networks, fiber optic cables, and data centers."[143] The DSR also provides support to tech giants such as Huawei, ZTE, and others to "pursue commercial business opportunities and be involved at all levels of the digital infrastructure built along the DSR."[144]

Over the years, China's IP theft has helped support the growth of its ICT sector. Huawei, for example, faces pending federal charges for theft of trade secrets, sanctions evasion, and racketeering.[145]

Finally, China promotes global technical standards to support its ICT strategy. Standards confer first-mover advantages on the companies that propose them. Companies earn royalties from standards-essential patents, potentially a significant source of revenue for Chinese companies. At the same time, Beijing is using its influence in these forums to undermine human rights and privacy in the ICT ecosystem by promoting technical standards that facilitate government surveillance.[146]

140. Mark Montgomery and Trevor Logan, "How to Stop China from Controlling the Global Semiconductor Industry," *Foundation for Defense of Democracies*, July 20, 2021. (https://www.fdd.org/analysis/2021/07/20/stopping-china-from-controlling-semiconductor-industry)
141. PRC National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce, "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," March 28, 2015. (Archived version available at: https://web.archive.org/web/20150717042806/https://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html)
142. Joshua Kurlantzick, "Assessing China's Digital Silk Road: A Transformative Approach to Technology Financing or a Danger to Freedoms?" *Council on Foreign Relations*, December 18, 2020. (https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger)
143. Clayton Cheney, "China's Digital Silk: Strategic Technological Competition and Exporting Political Illiberalism," *Council on Foreign Relations*, September 26, 2019. (https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political)
144. Robert Greene and Paul Triolo, "Will China Control the Global Internet via its Digital Silk Road?" *Carnegie Endowment for International Peace*, May 8, 2020. (https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857)
145. U.S. Department of Justice, Press Release, "Chinese Telecommunication Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," February 13, 2020. (https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering); Sam Cooper, "Inside the Chinese Military Attack on Nortel, *Global News* (Canada), August 25, 2020. (https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel); Erik Schatzker, "Huawei Sting Offers a Rare Glimpse of the U.S. Targeting a Chinese Giant," *Bloomberg*, February 4, 2019. (https://www.bloomberg.com/news/features/2019-02-04/huawei-sting-offers-rare-glimpse-of-u-s-targeting-chinese-giant); "Assessing Huawei Risk: How the Track Record of the CCP Should Play into the Due Diligence of Huawei's Partners and Customers," *RWR Advisory Group*, May 2019. (https://www.rwradvisory.com/wp-content/uploads/2019/05/Assessing-Huawei-Risk.pdf)
146. Natalie Thompson and Mark Montgomery, "Strengthening U.S. Engagement in International Standards Bodies," *Day One Project*, June 2021, pages 1–4. (https://www.dayoneproject.org/ideas/strengthening-u-s-engagement-in-international-standards-bodies). See also: Mark Montgomery and Theo Lebryk, "China's Dystopian 'New IP' Plan Shows Need for Renewed US Commitment to Internet Governance," *Just Security*, April 13, 2021. (https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance)

Surveillance and Data Collection

The United States and its allies recognize the risks of allowing Chinese technology companies into their markets. When the U.S. Federal Communications Commission (FCC) denied China Mobile's application to provide telecommunications services in the United States, then-FCC Chairman Ajit Pai warned that "if this application were granted, the Chinese government could use China Mobile to exploit our telephone network to increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network."[147]

Both the U.S. and allied governments have reportedly found evidence of Huawei equipment being used for such purposes.[148] In 2019, Dutch intelligence launched an investigation into Huawei's role in espionage. Dutch security chief Dick Schoof pointedly stated that "when it comes to our vital infrastructure or 5G, we say: you should not want to buy hardware and software from countries that have an offensive cyber program aimed at Dutch national security."[149] Annual reports from a British oversight board that evaluates Huawei-related infrastructure security risks consistently raise concerns about the engineering and cybersecurity of Huawei products and the company's failure to address previous concerns.[150] While these reports have not accused the CCP of leveraging Huawei for espionage or other nefarious purposes, Downing Street banned the company from core 5G infrastructure after deeming it a "high-risk vendor."[151] Meanwhile, when Sweden's Post and Telecom Authority banned Huawei from its 5G infrastructure, it noted, "The Swedish Security Service judges that the Chinese state and security services can influence and exert pressure on Huawei."[152]

One driver of these concerns is China's National Intelligence Law, which grants Chinese intelligence agencies broad authority to co-opt or compel any company, including China's tech giants, to assist with national intelligence work.[153] The law creates, in the words of one Chinese legal scholar, "affirmative legal responsibilities for Chinese and, in some cases, foreign citizens, companies, or organizations operating in China to provide access, cooperation, or support for Beijing's intelligence-gathering activities."[154] Beijing could demand that technology companies hand over information on foreign citizens, enable government access to databases or software, or install "backdoors" in their software that intelligence agencies can exploit.

147. U.S. Federal Communications Commission, "Statement of Chairman Ajit Pai," May 10, 2019. (https://docs.fcc.gov/public/attachments/DOC-357372A2.pdf)
148. Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *The Wall Street Journal*, February 12, 2020. (https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256); Jon Henley, "Huawei 'May Have Eavesdropped on Dutch Mobile Network's Calls,'" *The Guardian* (UK), April 19, 2021. (https://www.theguardian.com/technology/2021/apr/19/huawei-may-have-eavesdropped-on-dutch-mobile-networks-calls)
149. Lara Silva, "Huawei Might be Banned from the Netherlands as Espionage Investigation Starts," *Dutch Review* (Netherlands), May 16, 2019. (https://dutchreview.com/news/huawei-might-be-banned-from-the-netherlands-as-espionage-investigation-starts)
150. Annabel Murphy and Jack Parrock, "Huawei 5G: European Countries Playing 'Politics' with Network Bans, Chinese Company Says," *Euronews* (France), July 28, 2021. (https://www.euronews.com/next/2021/07/28/huawei-eyes-a-place-within-europe-s-digital-future-despite-5g-bans-in-some-countries)
151. "Britain Bans New Huawei 5G Kit Installation from September 2021," *Reuters*, November 29, 2020. (https://www.reuters.com/article/us-britain-huawei/britain-bans-new-huawei-5g-kit-installation-from-september-2021-idUSKBN28A005)
152. Charlie Duxbury, Stuart Lau, and Laurens Cerulus, "The EU's Front Line with China: Stockholm," *Politico*, February 10, 2021. (https://www.politico.eu/article/eu-front-line-china-stockholm)
153. PRC National People's Congress, "中华人民共和国国家情报法 [National Intelligence Law of the People's Republic of China]," June 12, 2018. (http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml)
154. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017. (https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense)

Forced Technology Transfer and 'De-Ciscoization'

Beijing has steadily increased restrictions on foreign ICT companies operating in China even as its own companies have expanded their international presence. Over the last two decades, China has issued several laws, regulations, and policies that disadvantage foreign firms relative to their Chinese counterparts, particularly in the ICT sector.[155] These measures have included forced joint ventures, technology transfer requirements, and weak enforcement of IP rights. State policies, such as Made in China 2025, "explicitly [aim] to develop advanced technologies while excluding foreign firms from Chinese markets for those technologies," according to Jeff Moon, former assistant U.S. trade representative for China.[156]

These efforts accelerated after the Snowden revelations, with some commentators calling for the "de-Ciscoization" (去思科化) of Chinese networks — that is, the removal of all U.S.-sourced technology.[157] Subsequently, U.S. companies operating in China have been subject to new measures under the National Cybersecurity Law of 2015[158] and the National Encryption Law of 2019,[159] which entail source code reviews, opaque security regulations, and exclusions from certain Chinese networks. These measures have reduced foreign firms' ability to compete in China. For Chinese companies, a privileged position in China's large domestic markets complements the extensive subsidies they receive from the government.

Attacks on and Through ICT Products

China is simultaneously promoting "information technology companies that could serve as espionage platforms" and conducting cyber operations against global ICT firms "whose products and services support government and private-sector networks worldwide," according to a 2020 Department of Homeland Security report.[160] China is "compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations," echoed the U.S. intelligence community in April 2021.[161]

Compromising a popular product or service provider enables Beijing to penetrate the firms that depend on it. For example, in the case of Operation Cloud Hopper, which began in 2014, Chinese hackers compromised managed service providers to penetrate hundreds of companies worldwide and across

155. U.S. Department of Defense, Annual Report to Congress, "Military and Security Developments Involving the People's Republic of China," 2020. (https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF)
156. Yoko Kubota, "China's New $21 Billion High-Tech Manufacturing Fund Likely to Rankle U.S.," *The Wall Street Journal*, November 20, 2019. (https://www.wsj.com/articles/chinas-new-21-billion-high-tech-manufacturing-fund-likely-to-rankle-u-s-11574250074). See also: "Appendix 5" in Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental*, January 2018. (https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf)
157. Zhao Yangge, "'去思科化' 时代分析师看好中兴通讯 [Analysts are optimistic about ZTE in the era of 'de-Ciscoization']," *Daily Economic News* (China), July 9, 2013. (https://business.sohu.com/20130709/n381051922.shtml)
158. PRC National People's Congress, "中华人民共和国网络安全法(草案) [Draft Cybersecurity Law of the People's Republic of China]," July 6, 2015. (Archived version available at: https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm)
159. "Cryptography Law of the P.R.C.," *China Law Translate*, October 27, 2019. (https://www.chinalawtranslate.com/en/cryptography-law)
160. U.S. Department of Homeland Security, "Homeland Threat Assessment," October 2020, page 8. (https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf)
161. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, page 8. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf)

numerous industries.[162] In 2017, suspected Chinese cyber actors inserted a backdoor into an update for CCleaner software, enabling access to the reportedly 2.7 million machines that downloaded the malicious patch.[163] Hackers then selected 40 affected IT companies, including Samsung, Sony, Intel, and Fujitsu for "second-stage" intrusion.[164]

"Compromising a popular product or service provider enables Beijing to penetrate the firms that depend on it."

In 2021, China twice exploited vulnerabilities in Microsoft Exchange Servers to access victims' networks, emails, and calendars.[165] By the time Microsoft patched the vulnerabilities, Chinese and other hackers had compromised tens of thousands of individual servers worldwide, including over 30,000 in the United States alone.[166] Separately, suspected Chinese cyber actors exploited the Pulse Secure virtual private network to compromise government agencies, defense contractors, and financial institutions across America and Europe.[167]

These attacks represent a substantial advance in Chinese cyber operational planning, demonstrating a prioritization of pervasive access through supply chain compromise rather than blunt spear phishing or exploitation of an individual target. Such attacks are difficult to detect and attribute. Even if an intrusion is discovered, one still must determine the origin of the initial compromise. For Beijing, such attacks have exceptional value because they enable persistent access, sustained collection, and tailored operations. They also reflect a broader shift from a "target-centric" strategy towards a "capability-centric" strategy, through which Beijing can pursue multiple CEEW objectives at once: economic espionage, economic coercion, critical-infrastructure disruption, and collecting personally identifiable information.

162. Richard Horne and Kris McConkey, "Operation Cloud Hopper," *PWC*, April 2017. (https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html); Robert Abel, "APT 10's Cloud Hopper Campaign Exposed," *SC Media*, April 6, 2017. (https://www.scmagazine.com/home/security-news/cybercrime/apt-10s-cloud-hopper-campaign-exposed); U.S. Department of Justice, Press Release, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," December 20, 2018. (https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion)

163. Lily Hay Newman, "Inside the Unnerving Supply Chain Attack that Corrupted CCleaner," *Wired*, April 17, 2018. (https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner); Kelly Jackson Higgins, "Chinese APT Backdoor Found in CCLeaner Supply Chain Attack," *Dark Reading*, March 12, 2018. (https://www.darkreading.com/endpoint/privacy/chinese-apt-backdoor-found-in-ccleaner-supply-chain-attack/d/d-id/1331250)

164. Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *ARSTechnica*, September 25, 2017. (https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs)

165. "Hafnium Targeting Exchange Servers with 0-day Exploits," *Microsoft*, March 2, 2021. (https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers); The White House, Press Release, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china)

166. Clare Duffy, "Here's What we Know so far about the Massive Microsoft Exchange Hack," *CNN*, March 10, 2021. (https://www.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html)

167. Brian Fung and Geneva Sands, "Suspected Chinese Hackers Exploited Pulse Secure VPN to Compromise 'Dozens' of Agencies and Companies in US and Europe," *CNN*, April 21, 2021. (https://www.cnn.com/2021/04/20/politics/fireeye-pulse-secure-vpn-exploit/index.html)

Recommendations

In Washington, recognition of the CEEW threat has grown substantially since FDD published its initial report on Chinese CEEW four years ago. Congress has passed a number of bipartisan measures since 2018, such as the Export Control Reform Act and key provisions in the FY2021 NDAA, that strengthen America's ability to defend against Chinese CEEW and malicious cyber operations more broadly. However, gaps still remain. Properly addressing Chinese CEEW will require sustained effort.

1. **Implement sanctions and other measures to curb Chinese cyber-enabled IP theft.** The United States must impose material costs on the Chinese individuals and entities that have directed or benefitted from cyber-enabled IP theft or perpetrated acts of CEEW. The threat of U.S. sanctions was instrumental in pressuring the Chinese ahead of the Xi-Obama agreement that temporarily reduced Chinese cyber-enabled IP theft.[168] A healthy future for the U.S.-China trade relationship will depend on guarantees from Beijing to adhere to global IP protections. It will also require transparency and reciprocity for U.S. firms operating in China, granting them the same legal standing as domestic firms in IP infringement cases.

2. **Ensure the Continuity of the Economy.** The United States must mitigate or stave off the consequences of CEEW operations, particularly critical infrastructure disruption. China has demonstrated both the intent and capability to put U.S. critical infrastructure at risk. As China increases the scale and sophistication of its cyber capabilities, the United States should expect an increase in targeting of critical assets. While the United States plans well for military contingencies and natural disasters, it lags in planning for CEEW scenarios. In the FY2021 NDAA, Congress passed a provision for Continuity of the Economy (COTE) planning, which directs the U.S. government to develop contingency plans to rapidly restart the economy in the event of a systemic disruption.[169] The legislation directs the U.S. government to focus on key mechanisms and critical industries so that in the event of conflict, the United States can blunt the effects of attempted coercion and maintain freedom of action. More than a year later, the federal government has barely begun. It must rapidly stand up the planning effort and ensure the necessary interagency and budgetary support.

3. **Prepare offensive economic contingency plans.** Whereas COTE planning is defensive in nature, the United States should also consider economic actions that impose costs on attackers. China's approach to conflict will not conform to conventional American views of war. For now, China remains wary of provoking the United States into an armed confrontation, particularly as its military forces still lag those of the United States. China is therefore likely to utilize a combination of cyber-enabled economic coercion and targeted critical-infrastructure disruption to pressure the United States or its allies. As Cooper noted in 2018, "Chinese activity across a range of domains operates in the 'gray zone' below the threshold that would warrant a major and sustained response. China uses asymmetries, ambiguity, and incrementalism to advance its strategic and economic aims without triggering a conflict with the United States or its friends."[170]

   Accordingly, the U.S. government must plan for economic contingencies vis-à-vis China. These plans should be formed alongside, and informed by, the

168. Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," *Council on Foreign Relations*, September 28, 2016. (https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later); "Redline Drawn: China Recalculates its use of Cyber Espionage," *FireEye*, 2016. (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)
169. Mark Montgomery and Annie Fixler, "Congress Poised to Enact Unprecedented Cyber Defense Legislation," *Foundation for Defense of Democracies*, December 8, 2020. (https://www.fdd.org/analysis/2020/12/08/congress-cyber-defense-legislation)
170. Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, September 5, 2018. (https://www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare)

key scenarios that guide U.S. military contingency planning. The United States cannot be caught flat-footed in responding to China's CEEW and broader political warfare.

4. **Establish a plurilateral approach to export controls.** In recent years, the United States has implemented measures to limit Chinese ICT development and the risk these technologies pose to U.S. critical infrastructure. Export controls on semiconductors, for instance, have precipitated a substantial loss in market share for Huawei and other Chinese companies.[171] The Department of Commerce has added Chinese firms to its Entity List, which deprived them of basic American-made technologies necessary to expand their industrial output.[172] However, China will likely resort to CEEW measures to circumvent these restrictions, either through IP theft or by employing a mix of coercion and persuasion to secure the desired technology from a U.S. ally. Thus, for export controls to be effective, they must be plurilateral. Such controls mean little if America's other trading partners allow China access to technology the United States seeks to restrict.

5. **Codify into law measures against high-risk Chinese vendors.** Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," signed on May 19, 2019, is one of the broadest and most powerful tools the United States can wield to combat risks associated with Chinese ICT in U.S. critical infrastructure.[173] The order delegates significant authority to the secretary of commerce to mitigate risks and block transactions involving ICT and related services owned, controlled, or directed by "foreign adversaries," to include China, Russia, Iran, North Korea, Cuba, and Venezuela.

   Despite its importance, this executive order rests on shaky ground. It relies on an emergency declaration under the International Emergency Economic Powers Act, which the sitting president can revoke at any time. Emergency declarations, while expedient, are not a substitute for statutory action when facing an enduring risk to national security. The measures envisioned under the executive order should be made permanent through codification in law. With statutory authorities, the Commerce Department could establish a quasi-"import control" regime around ICT equipment to reduce the risk of cyber-enabled IP theft and critical-infrastructure disruption facilitated by firms under U.S. adversaries' control.

Conclusion

The Chinese approach to CEEW reflects Beijing's perception of its vulnerabilities and strengths. The CCP seeks to establish China as a global center of innovation and economic power but anticipates foreign resistance to that goal. The 14th FYP, issued in March 2021, "highlights a growing urgency to protect China from external vulnerabilities through attaining self-reliance in science and technology," in the words of one China analyst.[174] This is a direct response to U.S. trade and export-control measures that underscore China's weakness in indigenous innovation. Yet the CCP is unlikely to revisit the confrontational approach that spurred this American response. On the contrary, Beijing's strident foreign policy and rhetoric make clear that CEEW will continue to be a mainstay of Chinese statecraft for years to come.

171. Jeanne Whalen, "U.S. Campaign Against Huawei Appears to be Working, as Chinese Tech Giant loses Sales Outside its Home Market," *The Washington Post*, March 31, 2021. (https://www.washingtonpost.com/technology/2021/03/31/impact-us-campaign-against-huawei); Dan Strumpf, "U.S. Restrictions Push Huawei's Revenue Down by Nearly a Third," *The Wall Street Journal*, December 31, 2021. (https://www.wsj.com/articles/u-s-restrictions-push-huaweis-revenue-down-by-nearly-a-third-11640934969)

172. Grant Leach and Cortney O'Toole Morgan, "BIS Adds Over 70 New Entities to the Entity List, Including SMIC," *Global Trade*, January 8, 2021. (https://www.globaltrademag.com/bis-adds-over-70-new-entities-to-the-entity-list-including-smic)

173. U.S. Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May15,2019.(https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain)

174. Lauren Dudley, "China's Quest for Self-Reliance in the Fourteenth Five-Year Plan," *Council on Foreign Relations*, March 8, 2021. (https://www.cfr.org/blog/chinas-quest-self-reliance-fourteenth-five-year-plan)

THE EVOLUTION OF KIM JONG UN'S 'ALL-PURPOSE SWORD'

By Mathew Ha

Introduction

For decades, the Kim regime has used weapons tests, border conflicts, and acts of terrorism to gain attention and raise tensions. The regime then demands economic and political benefits in exchange for reducing the tensions it provoked.[175] Pyongyang has the potential to add cyberattacks to this repertoire. Kim Jong Un reportedly described cyber warfare in 2012 as North Korea's "all-purpose sword," which provides "a capability to strike relentlessly."[176] In the decade since then, Pyongyang has wielded its growing cyber capabilities to reap financial, political, and strategic benefits to prolong the Kim regime's survival.

Over the past four years, Pyongyang's financially motivated cybercrime has become more prolific. North Korean cyberattacks increased by 32 percent

175. Jung H. Pak, "Kim Jong-un's tools of coercion," *The Brookings Institution*, June 21, 2018. (https://www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion)
176. Leekyung Ko, "North Korea as a Geopolitical and Cyber Actor," *New America*, June 6, 2018. (https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline)

year over year in 2020, according to South Korea's National Intelligence Service.[177] The blockchain data firm Chainalysis observed a steady increase in attacks on cryptocurrency exchanges between 2019 and 2021.[178] This may reflect the regime's desperation as it faces one of the most challenging economic crises in decades. North Korea has likely stolen "hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs,"[179] the U.S. intelligence community concluded in April 2021. Pyongyang's hackers steal money directly from international banks and cryptocurrency exchanges, in addition to employing ransomware and cryptocurrency mining tools to generate funds.[180]

Cybercrime is an integral element of the Kim regime's hybrid warfare strategy. Accordingly, Pyongyang's foreign intelligence agency, the Reconnaissance General Bureau, houses its cyber capabilities within Bureau 121,[181] which is responsible not only for cybercrime but also for espionage, reconnaissance, and inciting "social chaos by weaponizing enemy network vulnerabilities."[182]

Within the North Korean military, the General Staff Department — the armed forces' senior leadership organ — has developed cyber capabilities to quickly incapacitate the adversary by disabling command, control, and communications systems.[183] To compensate for its limited resources and conventional military capabilities, Pyongyang seeks to exploit its adversaries' weaknesses.[184] In that vein, it may launch cyberattacks against critical civilian infrastructure such as banks, public transportation, the electric grid, and telecommunications in South Korea (or the United States). Doing so could spark mass chaos, delay evacuations, and complicate Seoul's decision making in a wartime scenario.[185] Such efforts could require only

177. Seulkee Jang, "North Korea recently hacked Pfizer to steal vaccine development-related secrets," *Daily NK* (South Korea), February 24, 2021. (https://www.dailynk.com/english/north-korea-recently-hacked-pfizer-steal-vaccine-development-secrets)
178. Chainalysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," *Chainalysis*, January 13, 2022. (https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high)
179. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 2021, page 16. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf)
180. UN Panel of Experts, "Final report of the Panel of Experts submitted pursuant to resolution 2569 (2021)," S/2022/132, March 1, 2022, page 80. (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf)
181. ROK Ministry of National Defense, "2014 Defense White Paper," December 31, 2014, page 27. (http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201704260250138940.pdf). Academic and industry reports on North Korea's cyber capabilities also refer to Bureau 121 as Unit 121 or Lab 110. A South Korean military report first identified Lab 110 as an expansion and reorganization of Bureau 121. In keeping with the terminology used in U.S. government publications, this chapter uses the name Bureau 121.
182. U.S. Department of the Army, "North Korean Tactics," ATP 7-100.2, July 24, 2020, page 277. (http://www.documentcloud.org/documents/7038686-US-Army-report-on-North-Korean-military.html); Ji Young Kong, Jong In Lim, and Kyoung Gon Kim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," *2019 11th International Conference on Cyber Conflict*, July 2019, page 5. (https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf); Michael Barnhart, Michelle Cantos, Jeffery Johnson, Elias Fox, Gary Freas, and Dan Scott, "Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations," *Mandiant*, March 23, 2022. (https://www.mandiant.com/resources/mapping-dprk-groups-to-government)
183. Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Response," *Center for Strategic and International Studies*, December 2015, pages 5 and 45–50. (https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)
184. David Maxwell and Bradley Bowman, "Maximum Pressure 2.0: A Plan B for North Korea," . *Maximum Pressure 2.0: A Plan for North Korea*, Eds. Bradley Bowman and David Maxwell (Washington, DC: Foundation for Defense of Democracies, 2019). (https://www.fdd.org/analysis/2019/12/3/maximum-pressure-2)
185. Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War With the US," *The Diplomat*, October 10, 2017. (https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us)

rudimentary cyber capabilities, such as DDoS attacks, wipers, or ransomware.[186]

The Kim regime demonstrated this sort of capability in 2013, when the North Korean hacker group Dark Seoul launched destructive attacks against three banks and three media companies in Seoul, which inflicted over $800 million in total damage and sowed confusion across South Korea's financial sector for several days.[187] Fortunately, Seoul has reportedly improved its cyber defenses in recent years. The Korea Internet Safety Agency has successfully blocked numerous North Korean spear-phishing attempts.[188] However, Seoul's ability to thwart a major attack has yet to be tested.

"As the North Korean economy deteriorates further, the regime may seek to divorce itself conclusively from the U.S.-led international financial order."

FDD's 2018 study of North Korea's CEEW strategy concluded that the Kim regime has calibrated its cyber provocations to remain within the gray zone so as not to elicit a military response from South Korea and the United States, focusing instead on financially motivated cybercrime.[189] This chapter examines the evolving tactics and motives of Pyongyang's cybercrime and explores how North Korea's financially motivated cyberattacks and theft of cryptocurrencies mitigate the effect of sanctions.

The chapter also explores how, as the North Korean economy deteriorates further, the regime may seek to divorce itself conclusively from the U.S.-led international financial order. Currently, North Korea's illicit funds must often transit formal financial institutions or U.S.-based cryptocurrency exchanges to reach their final destination.[190] A robust cryptocurrency marketplace disconnected from the U.S.-led banking system could provide Pyongyang with a long-term solution to this vulnerability.

This chapter concludes with policy recommendations designed not only to bolster the U.S. and allied governments' cyber defense and deterrence strategies, but also to strengthen financial safeguards against the exploitation of cryptocurrencies by North Korea and other rogue states.

Tactics and Motives of North Korean Cybercrime

FDD's 2018 study concluded that "the majority of North Korea's current cyber activity is focused on making — or stealing — money or collecting data for the regime."[191] This holds true today. The primary mission of Pyongyang's cyber operators is financial gain, Kim Heung-kwang, a North Korean escapee and a former computer science professor at North Korea's Hamheung Computer Technology University, explained in 2017.[192] ClearSky, a UK- and Israel-based cybersecurity company, similarly concluded that a

186. David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More." *The New York Times*, October 15, 2017. (https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html)
187. Kyoung Jae Park, Sung Mi Park, and Joshua I. James, "A Case Study of the 2016 Korea Cyber Command Compromise," *Hallym University*, accessed June 25, 2018. (https://arxiv.org/ftp/arxiv/papers/1711/1711.04500.pdf)
188. "North Korean hackers behind attacks on cryptocurrency exchanges, South Korean newspaper reports," *Reuters*, December 15, 2017. (https://www.reuters.com/article/us-northkorea-southkorea-cryptocurrency/north-korean-hackers-behind-attacks-on-cryptocurrency-exchanges-south-korean-newspaper-reports-idUSKBN1EA02F)
189. Mathew Ha and David Maxwell, "Kim Jong Un's 'All-Purpose Sword': North Korean Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, October 3, 2018. (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword)
190. "North Korea's Lazarus Group Identified as Exploiters Behind $540 Million Ronin Bridge Heist," *Elliptic*, April 14, 2022. (https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge)
191. Mathew Ha and David Maxwell, "Kim Jong Un's 'All-Purpose Sword': North Korean Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, October 3, 2018. (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword)
192. Kim Jaewon, "A cybersecurity defector warns of North Korea's 'hacker army,'" *Nikkei Asia* (Japan), May 25, 2017. (https://asia.nikkei.com/Politics/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army)

unique characteristic of North Korean hackers is their "dual attack mission" of monetary theft and espionage. Other state-backed cyber actors tend to focus on national security priorities, not financial gain, the researchers noted.[193]

In addition to requiring funds for its nuclear weapons and ballistic missile programs, North Korea needs cash to offset an ongoing domestic economic crisis. In August 2020, the Kim regime made an unprecedented admission that it failed to achieve the goals of its last five-year plan. Pyongyang blamed sanctions, foreign enemies, COVID-19, natural disasters, and poor policy implementation by lower-level leaders, but the admission was a clear sign of distress.[194]

It is true that external factors exacerbated the regime's economic woes. Sanctions are putting pressure on Pyongyang's finances, and Typhoon Bavi in August 2020 hammered North Korea's agricultural sector. It is the regime's response to the COVID-19 pandemic, however, that has been particularly devastating.[195] To prevent a viral outbreak inside North Korea, the regime closed its borders and cut itself off from foreign trade. According to the Korea Trade-Investment Promotion Agency in Seoul, North Korea's trade volume with China dropped by 80.7 percent in 2020.[196] This forced several North Korean factories to close because they rely on materials and inputs from China to keep facilities and power plants running. Alexander Matsegora, Russia's ambassador to North Korea, said that "without imported materials, raw materials and components, many enterprises stopped, and people, accordingly, lost their jobs."[197] As North Korea's economy continues to deteriorate, cybercrime remains a key source of revenue.

Over the last four years, Pyongyang's hackers diversified their methods by experimenting with business email compromise (BEC) and card skimming schemes.[198] BEC schemes involve stealing a company's financial records and client contact information so that hackers can disguise themselves as vendors and receive payment for fraudulent invoices.[199] In card skimming, or "Magecart," schemes, hackers intercept customers' credit card information from retail websites and then sell it on the black market.[200] While this tactic is not new in the cybercrime world, North Korea's first

193. "Operation 'Dream Job' Widespread North Korean Espionage Campaign," *ClearSky Cybersecurity*, August 2020, page 39. (https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf)
194. Shim Kyu Seok, "Kim Jong-un makes rare admission of economic failure," *Korea JoongAng Daily* (South Korea), August 20, 2020. (https://koreajoongangdaily.joins.com/2020/08/20/national/northKorea/North-Korea-economy-failure/20200820185100410.html); David Maxwell and Mathew Ha, "Opening of Eighth Party Congress Shows Kim Jong Un Stays True To his Roots," *Foundation for Defense of Democracies*, January 7, 2021. (https://www.fdd.org/analysis/2021/01/07/eighth-party-congress-kim-jong-un-roots)
195. Evans J. R. Revere, "North Korea's economic crisis: last chance for denuclearization?" *The Brookings Institution*, February 26, 2021 (https://www.brookings.edu/wp-content/uploads/2021/02/fp_20210226_revere_krins.pdf); Min Joo Kim, "Typhoon Bavi approaches North Korea, posing another crisis for Kim Jong Un," *The Washington Post*, August 26, 2020. (https://www.washingtonpost.com/world/asia_pacific/typhoon-bavi-north-korea-coronavirus-kim-jong-un/2020/08/26/43f2a8e2-e75b-11ea-bf44-0d31c85838a5_story.html)
196. Elizabeth Shim, "Report: North Korea's trade with China declined 80% in 2020," *UPI*, February 22, 2021. (https://www.upi.com/Top_News/World-News/2021/02/22/Report-North-Koreas-trade-with-China-declined-80-in-2020/2431614020515)
197. Simon Denyer, "North Korea's economy is ravaged by sanctions and pandemic isolation. Kim is lashing out," *The Washington Post*, February 21, 2021. (https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-economy-crisis/2021/02/19/16d108d8-706b-11eb-8651-6d3091eac63f_story.html)
198. "Operation 'Dream Job' Widespread North Korean Espionage Campaign," *ClearSky Cybersecurity*, August 2020, page 8. (https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf)
199. U.S. Federal Bureau of Investigation, "Business Email Compromise," accessed February 12, 2021. (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise)
200. "What is Magecart?" *SanSec*, accessed July 27, 2021. (https://sansec.io/what-is-magecart); Alex Scroxton, "North Korea behind spate of Magecart attacks," *Computer Weekly*, July 6, 2020. (https://www.computerweekly.com/news/252485702/North-Korea-behind-spate-of-Magecart-attacks)

publicly known successful card skimming operation began in May 2019.[201]

Still, the priority for Pyongyang's hackers remains banks and cryptocurrency exchanges. The U.S. government reported that between 2015 and 2020, North Korea infiltrated banks and cryptocurrency exchanges in over 30 countries.[202] This yielded Pyongyang over $200 million between 2017 and 2019 and an additional $300 million in 2020.[203]

North Korean hackers have two primary ways of stealing funds from traditional financial institutions. First, they may seize control of a bank's financial transfer system run by the Society for Worldwide Interbank Financial Telecommunications, or SWIFT, and then use that control to conduct fraudulent transactions. North Korean hackers employed this method to steal $80 million from the Bank of Bangladesh in 2017.[204] The second tactic involves breaching ATMs. After gaining control, hackers remotely order select ATMs to dispense cash, which Pyongyang's accomplices collect.[205]

To steal from cryptocurrency exchanges, North Korean hackers have launched spear-phishing campaigns against exchange employees. Exchanges are attractive targets because, as FireEye explains, once hackers breach an exchange, "they potentially can move cryptocurrencies out of online wallets, swapping them for other, more anonymous cryptocurrencies or send them directly to other wallets on different exchanges to withdraw them in fiat currencies," such as dollars or euros.[206]

Three attacks on cryptocurrency exchanges in North America, Europe, and Asia between 2020 and 2021 yielded $50 million, according to the March 2022 report of the UN Panel of Experts on North Korea.[207] Chainalysis, meanwhile, concluded that Pyongyang successfully stole nearly $400 million in cryptocurrency from seven intrusions in 2021.[208] In April 2022, the FBI attributed a $620 million cryptocurrency hack to North Korea.[209] In that operation, the hackers used stolen credentials (rather than a software vulnerability) to compromise the blockchain bridge

201. "North Korean hackers are skimming U.S. and European Shoppers," *SanSec*, July 6, 2020. (https://sansec.io/research/north-korea-magecart)
202. U.S. Cybersecurity and Infrastructure Security Agency, Department of the Treasury, Federal Bureau of Investigation, Cyber Command, Joint Cybersecurity Advisory, "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," AA20-239A, August 25, 2020. (https://us-cert.cisa.gov/ncas/alerts/aa20-239a)
203. Eileen Yu, "North Korea reportedly stole $2B in wave of cyber-attacks," *ZDNet*, August 7, 2019 (https://www.zdnet.com/article/north-korea-reportedly-stole-2b-in-wave-of-cyberattacks); Richard Roth and Joshua Berlinger, "North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN Report," *CNN*, February 9, 2021. (https://www.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk)
204. Syed Zain Al-Mahmood, "How Bangladesh's Central Bank Found $100 Million Missing After a Weekend Break," *The Wall Street Journal*, March 11, 2016. (https://blogs.wsj.com/indiarealtime/2016/03/11/how-bangladeshs-central-bank-found-100-million-missing-after-a-weekend-break)
205. Indictment, *United States of America v. Jon Chang Hyok, Kim Il, and Park Jin Hyok*, 2:20-cr-00614-DMG (C.D. Cal. filed December 8, 2020). (https://www.justice.gov/opa/press-release/file/1367701/download)
206. Luke McNamara, "Why is North Korea so interested in Bitcoin?" *FireEye*, September 11, 2017. (https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html). A fiat currency derives value from the authority of the government that issues it rather than from an underlying commodity such as gold.
207. UN Panel of Experts, "Final report of the Panel of Experts submitted pursuant to resolution 2569 (2021)," S/2022/132, March 1, 2022, page 80. (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf)
208. "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," *Chainalysis*, January 13, 2022. (https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high)
209. U.S. Federal Bureau of Investigation, "FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea," April 14, 2022. (https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea)

— the tool for moving cryptocurrencies between different blockchains.[210]

The FBI has suggested that North Korean hackers may prefer targeting cryptocurrency exchanges because they provide "relatively fewer complications" compared to traditional banks.[211] In the past, banks' safeguards have tripped up Pyongyang's operatives. For instance, during the hack of the Bank of Bangladesh, the New York Federal Reserve detected suspicious activity, namely that one of the recipient addresses at a Filipino bank was named "Jupiter," a name it shared with a U.S.-sanctioned oil tanker from Iran. The Fed then paid closer attention to the hackers' payment requests and blocked them. Although the Bank of Bangladesh did lose $80 million, the Fed's intervention prevented the hackers from executing their planned theft of $1 billion.[212]

Another drawback of bank heists is they require a "larger network of criminals to help steal and then launder the money," while cryptocurrency hacks "cut out nearly all the middlemen."[213] Indeed, North Korean hackers require extensive help to steal from ATM machines. For example, in 2017, Japan's National Police Agency reported that up to 260 individuals affiliated with the Japanese yakuza and other international criminal organizations helped Pyongyang's hackers steal up to $16.6 million from 1,700 ATM machines across 17 Japanese prefectures.[214] In February 2021, the U.S. Justice Department revealed that North Korea collaborated with a North American criminal network to support ATM schemes targeting Pakistan's BankIslami and an unnamed Indian bank in 2018.[215]

While North Korea does not need as many accomplices to move its cryptocurrency revenues, hackers must still rely on money launderers to transfer virtual currency into fiat currency. For example, in March 2020, the Justice and Treasury departments respectively indicted and sanctioned two Chinese currency traders, Tian Yinyin and Li Jiadong, for helping North Korean hackers convert over $100 million in stolen cryptocurrency into fiat currency through Chinese banks via several hundred small transactions.[216] To eliminate these middlemen, North Korea would likely need to rely on emerging crypto-based payment and transaction systems.

To that end, Pyongyang invited Virgil Griffith, an American cryptocurrency software developer based in Singapore, to present at the DPRK Cryptocurrency Conference in 2019 on the topic of "potential money laundering and sanctions evasion applications of cryptocurrency and blockchain technologies." The U.S. Justice Department later indicted Griffith for providing "highly technical information to North Korea, knowing that this information could be used to help

210. Lily Hay Newman, "Blockchains Have a 'Bridge' Problem, and Hackers Know It," *Wired*, April 3, 2022. (https://www.wired.com/story/blockchain-network-bridge-hacks)
211. U.S. Federal Bureau of Investigation, "Cryptocurrencies a growing target of theft," March 11, 2021. (https://www.fbi.gov/news/stories/north-korean-hacks-show-virtual-currency-vulnerabilities-031121)
212. Krishna N. Das and Jonathan Spicer, "How the New York Fed fumbled over the Bangladesh Bank cyber-heist," *Reuters*, July 21, 2016. (https://www.reuters.com/investigates/special-report/cyber-heist-federal)
213. U.S. Federal Bureau of Investigation, "Cryptocurrencies a growing target of theft," March 11, 2021. (https://www.fbi.gov/news/stories/north-korean-hacks-show-virtual-currency-vulnerabilities-031121); UN Panel of Experts, "Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019)," S/2019/691, August 30, 2019. (https://undocs.org/S/2019/691)
214. "Suspected ringleader of huge, coordinated ATM scam entered N. Korea," *Kyodo News* (South Korea), April 5, 2020. (https://english.kyodonews.net/news/2020/04/2b45db5e313b-suspected-ringleader-of-huge-coordinated-atm-scam-entered-n-korea.html)
215. U.S. Department of Justice, Press Release, "Three North Korean Military Hackers Indicted in Wide-ranging Scheme to Conduct Cyberattacks and Financial Crimes Across the Globe," February 17, 2021. (https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and)
216. Indictment, *United States of America v. Tian Yinyin and Li Jiadong*, 1:20-cr-00052-TJK (D.D.C. filed May 7, 2019). (https://www.courtlistener.com/recap/gov.uscourts.dcd.215736/gov.uscourts.dcd.215736.1.0.pdf)

North Korea launder money and evade sanctions."[217] Griffith pleaded guilty and was sentenced to five years in federal prison.[218]

Cryptocurrency as an Engine of Sanctions Resistance

The Kim regime may shift its cryptocurrency strategy from an emphasis on acquiring cash to building resistance against sanctions. Rather than converting digital currency into fiat currency, Pyongyang could build large reserves of numerous cryptocurrencies to spend in a cryptocurrency exchange independent of the U.S.-led financial system. For the moment, that goal is mostly aspirational. Yet North Korea is adept at identifying its enemies' structural weaknesses. The lax governance and regulatory structure surrounding digital currency is ripe for exploitation. This strategy would align with the ideological tenets of *juche*, the regime's doctrine of self-reliance, by providing Pyongyang with greater financial autonomy.

However, North Korea's ability to leverage cryptocurrency for these objectives will likely be contingent upon technological advances by other rogue states with more robust economies. Alone, North Korea cannot challenge the U.S.-led financial order.

Fortunately for Pyongyang, Moscow and Beijing are already exploring ways to reduce their dependence on the dollar through digital currency. In March 2021, Russian Foreign Minister Sergey Lavrov recommended during a visit to China that "we [Russia and China] need to reduce sanctions risks by bolstering our technological independence by

On September 6, 2018, in Los Angeles, California, First Assistant U.S. Attorney Tracy Wilkison announces charges against a North Korean national for a range of cyberattacks. (Mario Tama/Getty Images)

switching to payments in our national currencies and global currencies that serve as an alternative to the dollar."[219] That need has only increased since Russia's invasion of Ukraine and the West's imposition of sanctions. China, Russia, and even Iran have started creating their own national digital currencies and blockchain platforms. Moscow, Beijing, and others are looking for ways to operate "economies outside the U.S.-led financial system" to "reduce Washington's ability to impose sanctions," as FDD scholars observed in 2019.[220]

Separately, according to the UN Panel of Experts, North Koreans based in Hong Kong developed a blockchain-enabled digital currency in 2018 called Marine Chain Token for use in shipping-related transactions. The Panel hypothesized that the Marine Chain platform was funded by stolen cryptocurrencies, pointing to the platform's ties to North Korean operatives "who

217. U.S. Department of Justice, U.S. Attorney's Office for the Southern District of New York, Press Release, "Manhattan U.S. Attorney Announces Arrest of United States Citizen for Assisting North Korea in Evading Sanctions," November 29, 2019. (https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-united-states-citizen-assisting-north-korea)
218. "U.S. hacker sentenced to 5 years in North Korea sanctions case," *NBC News*, April 12, 2022. (https://www.nbcnews.com/news/world/north-korea-virgil-griffith-cryptocurrency-rcna24169)
219. Gabrielle Tetrault-Farber and Andrew Osborn, "Russia's top diplomat starts China visit with call to reduce U.S. dollar," *Reuters*, March 22, 2021. (https://www.reuters.com/article/us-russia-china-usa/russias-top-diplomat-starts-china-visit-with-call-to-reduce-u-s-dollar-use-idUSKBN2BE0XH)
220. Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies*, July 11, 2019. (https://www.fdd.org/analysis/2019/07/11/crypto-rogues)

have extorted Bitcoin from online companies."[221] In a 2021 indictment against three North Korean hackers, the Justice Department added that the Marine Chain Token enabled Pyongyang to evade sanctions and "secretly obtain funds from investors" abroad who purchased partial ownership of shipping vessels.[222]

> **"If China succeeds in establishing an alternative system, North Korea will quickly try to attach itself to that system."**

However, these advances still fall far short of Beijing's and Moscow's achievements. China began developing its own digital currency and payment systems as early as 2014[223] and has made significant progress.[224] China's most recent five-year plan noted the significance of blockchain applications for supply chain management, e-governance, fintech, and other purposes. President Xi Jinping seeks "a new industrial advantage" through blockchain. As a result, Chinese companies are filing more blockchain patents than their U.S. counterparts.[225] Beijing's leadership intends to leverage this new digital currency not only to support its commercial and trade activities, but also "to displace the U.S. dollar as a global reserve currency," FDD scholars concluded in 2019.[226]

If China succeeds in establishing an alternative system, North Korea will quickly try to attach itself to that system because Pyongyang conducts over 80 percent of its trade with Beijing.[227] Despite significant decreases in the volume of bilateral trade — which in 2021 was down 40 percent from the previous year and 90 percent compared to pre-pandemic levels[228] — China remains North Korea's main trading partner.[229]

China's cooperation with North Korea in this emerging fintech space may have its limits if Beijing concludes that a visible role for North Korea would deter other nations from participating in a Chinese-led system, for which Beijing has global ambitions. Nonetheless, China is unlikely to reject North Korea's participation entirely, because preventing instability inside North Korea is a long-term strategic objective for Beijing.[230]

---

221. UN Panel of Experts, "Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019)," S/2019/691, August 30, 2019, page 29. (https://undocs.org/S/2019/691)
222. U.S. Department of Justice, Press Release, "Three North Korean Military Hackers Indicted in Wide-ranging scheme to commit cyberattacks and financial crimes across the globe," February 17, 2021. (https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and)
223. Nathaniel Popper and Cao Li, "China charges ahead with a national digital currency," *The New York Times*, March 1, 2021. (https://www.nytimes.com/2021/03/01/technology/china-national-digital-currency.html)
224. Yaya Fanusie and Emily Jin, "China's Digital Currency: Adding Financial Data to Digital Authoritarianism" *Center for a New American Security*, January 26, 2021. (https://www.cnas.org/publications/reports/chinas-digital-currency); Nathaniel Popper and Cao Li, "China charges ahead with a national digital currency," *The New York Times*, March 1, 2021. (https://www.nytimes.com/2021/03/01/technology/china-national-digital-currency.html)
225. Trevor Logan and Theo Lebryk, "America and its military need a blockchain strategy," *C4ISRNET*, April 5, 2021. (https://www.c4isrnet.com/opinion/2021/04/05/america-and-its-military-need-a-blockchain-strategy)
226. Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies*, July 11, 2019. (https://www.fdd.org/analysis/2019/07/11/crypto-rogues)
227. Fan Yifei, "On Digital Currencies, Central Banks Should Lead," *Bloomberg*, September 1, 2016. (http://www.bloomberg.com/opinion/articles/2016-09-01/on-digital-currencies-central-banks-should-lead); Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies*, July 11, 2019. (https://www.fdd.org/analysis/2019/07/11/crypto-rogues)
228. Bo-eun Kim, "North Korea-China Trade on Restoration Path, but Pyongyang Faces Challenges," *The Korea Times* (South Korea), April 10, 2022. (https://www.koreatimes.co.kr/www/nation/2022/04/103_327021.html)
229. Michael Lee, "China-North Korea Trade Soars but Still Falls Short of Pre-Covid Levels," *Korea JoongAng Daily* (South Korea), March 22, 2022. (https://koreajoongangdaily.joins.com/2022/03/22/national/northKorea/North-Korea-China-customs/20220322180517311.html)
230. Eleanor Albert, "The China-North Korea Relationship," *Council on Foreign Relations*, June 25, 2019. (https://www.cfr.org/backgrounder/china-north-korea-relationship)

Recommendations

As North Korean cyber operations evolve, the U.S. government must bolster American defenses and strengthen deterrence measures. The Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security has distributed numerous technical alerts on North Korean malware to help private-sector entities harden their networks. The U.S. government has also sought to impose costs on North Korea's hackers and programmers through sanctions and criminal indictments. However, the measures have been insufficient. The United States and its allies must consider innovative ways to change the regime's calculus. The first four recommendations below originally appeared in FDD's 2018 report on North Korean CEEW but have been updated with current information.[231] What follows are three additional recommendations for how the U.S. government should address the risks and opportunities presented by the accelerating global adoption of cryptocurrencies and blockchain technology.

1. **Escalate economic measures targeting the financial networks that launder North Korean funds.** Over the long-term, North Korea may reduce or eliminate its need for financial middlemen to launder funds and convert digital currency into fiat currency. In the meantime, however, this is a strategic weakness. The U.S. Treasury Department should sanction the individuals, companies, and banks that facilitate financial transactions on behalf of Pyongyang's hackers and the Kim regime in general. Washington's earlier sanctions and indictments related to North Korean cyber operations were largely symbolic because they did not target the key nodes supporting North Korean cyber operations. To be effective, sanctions should target the foreign partners, front companies, and overseas financial institutions that work with North Korea.[232] For example, the Justice Department case against Tian Yinyin and Li Jiadong revealed that nine Chinese banks helped launder North Korea's stolen cryptocurrency. Treasury should confirm that these banks have blocked additional suspicious transactions and are no longer complicit in such activity. If Treasury finds any further issue, it should impose additional penalties, fines, and sanctions.

2. **Pressure China to dismantle North Korean cyber infrastructure.** Pyongyang dispatches hackers abroad — particularly, although not exclusively, to China — to access more robust internet infrastructure capable of supporting more complex operations.[233] Operating abroad also increases plausible deniability for the Kim regime. By contrast, relying on personnel and computer networks based solely in North Korea would create a "significant operational weakness" and leave Pyongyang vulnerable to cyberattacks that would "limit current North Korean cyber operational freedom," according to Recorded Future.[234] Washington should therefore urge China to repatriate all North Korean hackers. If Beijing and other foreign governments fail to dismantle Pyongyang's illicit cyber infrastructure, the White House should consider deploying the North Korean Sanctions and Policy Enhancement Act, which grants Treasury the authority to designate individuals and entities who "have knowingly engaged in, directed, or provided material support to conduct significant activities in undermining cybersecurity."[235]

231. Mathew Ha and David Maxwell, "Kim Jong Un's 'All-Purpose Sword': North Korean Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, October 3, 2018. (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword)
232. Mathew Ha, "New U.S. sanctions on North Korea are insufficient," *Foundation for Defense of Democracies*, September 17, 2019. (https://www.fdd.org/analysis/2019/09/17/new-us-sanctions-on-north-korea-are-insufficient)
233. Will Ripley, "North Korean defector: 'Bureau 121' hackers operating in China, *CNN*, January 7, 2015. (https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang)
234. Insikit Group, "North Korea's ruling elite are not isolated," *Recorded Future*, July 25, 2017. (https://go.recordedfuture.com/hubfs/north-korea-internet-activity.pdf)
235. North Korea Sanctions and Policy Enhancement Act of 2016, Pub. L. 114-122, 130 Stat. 93. (https://www.congress.gov/bill/114th-congress/house-bill/757/text)

3. **Publicize information about cryptocurrency hacks.** Cryptocurrency exchanges have become regular targets of cyber criminals but often do not share the details of those hacks. Without this information, researchers, law enforcement, and government officials have limited ability to decode criminal methodologies. The United States, South Korea, and other partner countries should therefore issue breach-notification rules. They should also establish a framework for sharing information about attacks that combines regulatory and government authorities with virtual currency exchanges and providers.[236]

4. **Conduct information operations against Pyongyang.** In 2017, Cyber Command reportedly launched DDoS attacks on suspected North Korean networks to limit the regime's cyber operations.[237] While the Defense Department should continue to employ such tactics as part of its "defend forward" strategy,[238] cyber measures alone will not impose sufficient costs. Washington should leverage North Korean elites' access to the global internet to expose them to foreign media and other restricted information.[239] The Kim regime fears uncensored information that could compromise its ideological grip on the North Korean populace, such as evidence of its atrocities, corruption, and economic malpractice. Over the long term, creating a rift between these elites and Kim's inner circle could lay the groundwork for a change in leadership and, in the short term, may convince Kim to restrict North Korean cyber operations because their cost is too great.[240]

More broadly, the United States must develop policies to cope with the long-term risks that cryptocurrencies and blockchain technology may pose to the U.S.-led global financial system and the role of the dollar in international trade. A March 2022 executive order on digital currencies directs the Treasury Department, the Federal Reserve, the Consumer Financial Protection Bureau, and other agencies to study these issues.[241] This is a critical first step toward safeguarding financial stability, innovation, and consumer protection.

5. **Commission research on public blockchains.** While the Chinese and Russian governments have advanced their study and early implementation of various blockchain tools to harden their network defenses, Beijing and Moscow have invested less in public blockchain systems, preferring private blockchains in which a single entity controls the chain and knows the identity of all participants.[242] A public blockchain is decentralized, anonymous, and open to anyone's participation if the individual verifies data added to this blockchain.[243] According

236. Mathew Ha and David Maxwell, "Kim Jong-un's 'All-Purpose Sword': North Korean Cyber-enabled Economic Warfare," *Foundation for Defense of Democracies*, October 3, 2018. (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword)
237. Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump signed presidential directive ordering actions to pressure North Korea," *The Washington Post*, September 30, 2017. (https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html)
238. U.S. Department of Defense, "Summary — Department of Defense Cyber Strategy 2018," 2018. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)
239. Insikit Group, "North Korea's Ruling Elite Are Not Isolated," *Recorded Future*, July 25, 2017. (https://www.recordedfuture.com/north-korea-internet-activity); Mathew Ha, "North Korea is relying on the internet more, creating an opening for the U.S.," *Fifth Domain*, February 26, 2020. (https://www.fifthdomain.com/thought-leadership/2020/02/26/north-korea-is-relying-on-the-internet-more-creating-an-opening-for-the-us)
240. David Maxwell and Mathew Ha, "Information and Influence Activities," *Maximum Pressure 2.0: A Plan for North Korea*, Eds. Bradley Bowman and David Maxwell (Washington, DC: Foundation for Defense of Democracies, 2019). (https://www.fdd.org/analysis/2019/12/3/maximum-pressure-2)
241. U.S. Executive Order 14067, "Ensuring Responsible Development of Digital Assets," March 9, 2022. (https://www.govinfo.gov/content/pkg/FR-2022-03-14/pdf/2022-05471.pdf)
242. Trevor Logan and Theo Lebryk, "America and its military need a blockchain strategy," *C4ISRNET*, April 5, 2021. (https://www.c4isrnet.com/opinion/2021/04/05/america-and-its-military-need-a-blockchain-strategy)
243. "Difference between Public and Private blockchain," *Geeks for Geeks*, May 11, 2022. (https://www.geeksforgeeks.org/difference-between-public-and-private-blockchain)

to the Blockchain Council, a U.S.-based group of experts, public blockchains are more secure than private networks because it is difficult for a single bad actor to compromise enough of the decentralized network to corrupt the data within the blockchain.[244] The United States should become a leader in public blockchain technology, which not only adheres to American liberal norms and values but also is garnering more use within the consumer marketplace.[245]

6. **Foster more public-private cooperation and innovation in cryptocurrency, blockchain, and fintech.**[246] A core finding of the U.S. Cyberspace Solarium Commission is the need for greater public-private collaboration on cybersecurity.[247] The U.S. government should sponsor business incubator programs that promote blockchain-based solutions for regulatory challenges related to cryptocurrencies' impact on global finance and banking.[248] Specifically, Congress should appropriate funding for the National Science Foundation to help companies working on blockchain and other distributed ledger technologies. A report from the Center for a New American Security assessed that leading the development of blockchain applications would position Washington to maintain the value of coercive economic tools, including sanctions.[249]
7. **Conduct studies within the U.S. intelligence community and other agencies to forecast trends in the use of cryptocurrency, blockchain and fintech by U.S. adversaries.** The Biden administration should task the intelligence community with studying adversarial ambitions to undermine the existing financial order using cryptocurrencies, blockchain, and other fintech. The objective should be to identify future threats along with the long-term implications of current trends. Beijing has stated that it intends to design a universal digital payment network over the next 10 years to support digital currency transfers and payments worldwide.[250] Understanding threats to America's long-term national and financial security must be a priority.

Conclusion

To counter the North Korean cyber threat, the United States and its allies must employ a tailored approach that focuses both on the immediate needs of cyber defense and deterrence and future challenges posed by illicit financial networks and their state sponsors. With proactive measures, America and its allies can ensure that cryptocurrencies and blockchain technology become assets to protect the integrity of the global financial order.

244. Toshendra Kumar Sharma, "Public vs. Private Blockchain: A Comprehensive Comparison," *Blockchain Council*, accessed July 27, 2021. (https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison)
245. Trevor Logan and Theo Lebryk, "America and its military need a blockchain strategy," *C4ISRNET*, April 5, 2021. (https://www.c4isrnet.com/opinion/2021/04/05/america-and-its-military-need-a-blockchain-strategy)
246. Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies*, July 11, 2019. (https://www.fdd.org/analysis/2019/07/11/crypto-rogues); Peter Harrell and Elizabeth Rosenberg, "Economic Dominance, Financial Technology, and the Future of U.S. Economic Coercion," *Center for a New American Security*, April 2019, page 36. (https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Economic_Dominance-final.pdf?mtime=20190423154936)
247. U.S. Cyberspace Solarium Commission, "Final Report," March 2020, pages iv and 96. (https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report)
248. Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies*, July 11, 2019. (https://www.fdd.org/analysis/2019/07/11/crypto-rogues)
249. Peter Harrell and Elizabeth Rosenberg, "Economic Dominance, Financial Technology, and the Future of U.S. Economic Coercion," *Center for a New American Security*, April 2019, pages 25 and 36–37. (https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Economic_Dominance-final.pdf?mtime=20190423154936)
250. William Foxley, "China's Blockchain-based service network to integrate central bank digital currency," *CoinDesk*, January 17, 2021. (https://www.coindesk.com/chinas-blockchain-based-service-network-to-integrate-central-bank-digital-currency)

THE DANGERS OF IRAN'S CYBER AMBITIONS

By Annie Fixler

Introduction

Tehran has not engaged in spectacular cyberattacks against the United States over the past four years — even after the Trump administration imposed devastating sanctions on Iran and launched a drone strike that killed Major General Qassem Soleimani, commander of the Islamic Revolutionary Guard Corps (IRGC) Quds Force.[251] This is a puzzling departure from precedent and obscures the broader trend of Tehran's improving cyber capabilities.

Iran's 2011–2013 campaign of DDoS attacks against the U.S. financial system — in which hackers took down bank websites by flooding them with traffic — marked one of the earliest examples of CEEW by any nation.[252]

251. Annie Fixler, "The Cyber Threat from Iran after the Death of Soleimani," *CTC Sentinel*, February 2020. (https://ctc.usma.edu/cyber-threat-iran-death-soleimani)

252. U.S. Department of Justice, Press Release, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conduction Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016. (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged); Annie Fixler and Frank Cilluffo, "Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, November 9, 2018. (https://www.fdd.org/analysis/2018/11/06/evolving-menace)

Since then, Tehran appears to have recalibrated its tactics to mirror some of the more successful operations of other U.S. adversaries. The Islamic Republic now engages in disinformation operations, conducts supply chain attacks, and penetrates U.S. critical infrastructure. Some of these activities may constitute CEEW, while others position Iran for future attacks.

Washington should not assume that Tehran's tactical changes indicate the United States has deterred Iran from launching destructive attacks. Deterrence is not static. It requires regular maintenance. Underestimating a committed adversary is dangerous, and a misdiagnosis risks underinvestment in intelligence gathering, leading to strategic surprise. It is possible that U.S. sanctions, indictments, and counter-cyber operations have deterred Iran from further attacks.[253] It is also possible that Iranian hackers are attempting dramatic attacks but failing.

"Underestimating a committed adversary is dangerous, and a misdiagnosis risks underinvestment in intelligence gathering, leading to strategic surprise."

Alternatively, the regime may have elected not to expend limited resources on destructive attacks but to maintain the capability to employ them later on. After all, cyber-espionage can always be a steppingstone to more aggressive operations, and it can be difficult to parse motive from a few lines of code. In late 2019, for example, Microsoft warned that Iranian hackers were trying to breach industrial control systems (ICS) — that is, computer systems that control critical infrastructure — to conduct physically disruptive attacks in the United States.[254] Other private security researchers cautioned that reconnaissance and espionage were equally likely motivations.[255] Given the uncertainty, the United States cannot afford to dismiss the Iranian cyber threat.

Iran's hackers are persistent. For example, in 2018, the Department of Justice charged the Iranian government with sponsoring a multi-year campaign to pilfer data from hundreds of universities, companies, and government entities in the United States and around the world.[256] The following year, researchers discovered the same hackers using the same tactics and network infrastructure to target more than 60 universities in the United States.[257]

Iranian hackers have repeatedly caused damage despite their less sophisticated capabilities compared to America's other cyber adversaries. And Tehran's skills are improving. The Islamic Republic is demonstrating a "growing expertise" in its cyber operations, the U.S. intelligence community concluded in its February 2022 annual threat assessment.[258] Likewise, Microsoft observed a "gradual evolution of the tools, techniques,

253. Ellen Nakashima and Paul Sonne, "U.S. Military Carried Out Secret Cyberstrike on Iran to Prevent it from Interfering with Shipping," *The Washington Post*, August 28, 2019. (https://www.washingtonpost.com/national-security/us-military-carried-out-secret-cyber-strike-on-iran-to-prevent-it-from-interfering-with-shipping/2019/08/28/36202a4e-c9db-11e9-a1fe-ca46e8d573c0_story.html)
254. Kate O'Flaherty, "Iranian Hackers Are Going After A Disturbing New Physical Target," *Forbes*, November 21, 2019. (https://www.forbes.com/sites/kateoflahertyuk/2019/11/21/iranian-hackers-could-be-going-after-a-disturbing-new-physical-target/?sh=62e5fa137d2a)
255. Nicole Lindsey, "Iranian Hackers APT33 Now Threatening ICS Security," *CPO Magazine*, December 5, 2019. (https://www.cpomagazine.com/cyber-security/iranian-hackers-apt33-now-threatening-ics-security)
256. U.S. Department of Justice, Press Release, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," March 23, 2018. (https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary)
257. Sean Lyngaas, "'Cobalt Dickens' Group is Phishing Universities at Scale Again, Researchers Say," *CyberScoop*, September 11, 2019. (https://www.cyberscoop.com/cobalt-dickens-iran-universities-hacking-secureworks). The exact number of successful breaches remains unclear.
258. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 7, 2022, page 15. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf)

and procedures employed by malicious network operators based in Iran" throughout 2021.[259]

In recent years, Tehran has demonstrated improvements in its social engineering and technical skills that raise concerns for future Iranian cyber operations, CEEW or otherwise. Rather than focus exclusively on thwarting or deterring current Iranian operations, the United States and its allies must take steps to prevent Iran from becoming a more capable adversary in the future.

Domestic Repression as a Cyber Training Ground

The Islamic Republic's cyber capabilities were born in reaction to the mass protests following the fraudulent 2009 Iranian presidential election.[260] The protesters' use of the internet and social media for mobilization and information sharing was the regime's first brush with the power that cyberspace provided to the Iranian people.

Iran's Ministry of Intelligence has thus "recruited highly educated people and turned their cyber talents into tools to exploit, harass, and repress their fellow citizens and others deemed a threat to the regime,"[261] according to FBI Director Christopher Wray. This development threatens the United States because the techniques deployed against Iranian dissidents "foreshadow the tactics and tools that will be employed against other targets," scholars Collin Anderson and Karim Sadjadpour concluded in a study four years ago. They noted that "most victims of Iranian cyber operations are in Iran or the large Iranian diaspora," but the Advanced Persistent Threat (APT) groups responsible for internal surveillance are often also responsible for global espionage.[262]

In September 2020, Washington imposed sanctions on Iran's APT39 and its front company Rana Intelligence Computing Company, which were operating on behalf of the Iranian Ministry of Intelligence. The U.S. Treasury Department explained that Rana's operations were "both internal to Iran and global in scale," with its victims comprising "hundreds of individuals and entities from more than 30 different countries across Asia, Africa, Europe, and North America," including 15 U.S. companies.[263]

Like the line between domestic and internationally focused APTs, the distinction between espionage-focused APTs and destructive APTs may also be blurring. Private cybersecurity firms have warned that Iranian APTs associated with espionage maintain destructive malware in their arsenal.[264]

The overlap between those engaged in domestic and international operations is not surprising. The tactics needed to surveil or harass domestic opponents can apply to international espionage targets. For example, the Department of Justice indicted two Iranian hackers in September 2020 for a "coordinated cyber intrusion campaign — sometimes at the behest of the government of the Islamic Republic of Iran." These hackers "brazenly infiltrated computer systems" around the world, explained then-U.S. Attorney for the District of New Jersey Craig Carpenito. They sought to steal sensitive data while also attempting "to intimidate

259. "Evolving Trends in Iranian Threat Actor Activity — MSTIC Presentation at CyberWarCon 2021," *Microsoft*, November 16, 2021. (https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021)
260. Collin Anderson and Karim Sadjapour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington, DC: Carnegie Endowment for International Peace, 2018), pages 10–12. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
261. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry," September 17, 2020. (https://home.treasury.gov/news/press-releases/sm1127)
262. Collin Anderson and Karim Sadjapour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington, DC: Carnegie Endowment for International Peace, 2018), pages 9 and 39. (https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf)
263. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry," September 17, 2020. (https://home.treasury.gov/news/press-releases/sm1127)
264. Andy Greenberg, "Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount," *Wired*, June 28, 2019. (https://www.wired.com/story/iran-hackers-us-phishing-tensions)

perceived enemies of Iran, including dissidents fighting for human rights in Iran and around the world."[265]

Tehran clearly seeks to shape the domestic information environment. For example, to prevent activists from organizing and sharing information, the regime has repeatedly throttled internet connectivity during protests.[266] In November 2019, Tehran ordered internet service providers to disrupt internet access across the country as demonstrations against fuel price spikes spiraled into political protests against the regime.[267] Similarly, Iran's Khuzestan Province experienced internet disruptions in July 2021 during protests sparked by water shortages.[268] In both cases, Tehran aimed to limit the ability of protestors to share information with the outside world about the regime's suppression of dissent.

Human rights and digital rights organizations attribute Tehran's ability to cut internet access to Iranian efforts over the past decade to filter web content and to build a sovereign internet infrastructure known as the National Information Network, or SHOMA in Persian.[269] In March 2021, the IRGC announced yet another initiative to purge the internet of "vulgarities."[270] The effort implemented Supreme Leader Ali Khamenei's instructions that the internet "should not be put at the discretion of the enemy."[271]

Advancements in Disinformation Operations

Tehran has long engaged in online influence operations to "launder information and push distorted narratives, especially with respect to Iran and Saudi Arabia," the congressionally mandated Cyberspace Solarium Commission concluded in December 2021.[272] The Commission noted that Iranian disinformation operations have become more frequent, but "its tactics remained technically unsophisticated." Indeed, Iran's skills do not match those of Russia, but over the past four years, Tehran's hackers have demonstrated a growing understanding of the U.S. information environment and the social engineering needed to target Americans.

Fortunately, the four Iranians responsible for a 2014–2015 cyber-espionage operation targeting U.S. intelligence officials appear to have had limited success

265. U.S. Department of Justice, Press Release, "Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and Middle East," September 16, 2020. (https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states)
266. Matt Burgess, "Iran's Total internet Shutdown is a Blueprint for Breaking the Web," *Wired*, July 10, 2020. (https://www.wired.co.uk/article/iran-news-internet-shutdown); "Iran: Tightening the Net 2020," *Article19*, September 2020. (https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf); Isabel Debre, "Iran Shut Down Internet in Southeast Province Amid Protests, Harsh Crackdown," *The Times of Israel* (Israel), February 28, 2021. (https://www.timesofisrael.com/iran-shuts-down-internet-in-southeast-province-amid-protests-harsh-crackdown)
267. "Internet Disrupted in Iran Amid Fuel Protests in Multiple Cities," *Netblocks*, November 15, 2019. (https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b); Delia Paunescu, "Why did Iran Shut Off the Internet for the Entire Country?" *Recode*, November 21, 2019. (https://www.vox.com/recode/2019/11/21/20975920/iran-internet-protests-reset-podcast)
268. "Mobile Internet Disrupted in Iran Amid Khuzestan Water Protests," *Netblocks*, July 21, 2021. (https://netblocks.org/reports/mobile-internet-disrupted-in-iran-amid-khuzestan-water-protests-1yPjK9AQ)
269. Lily Hay Newman, "How the Iranian Government Shut Off the Internet," *Wired*, November 17, 2019. (https://www.wired.com/story/iran-internet-shutoff)
270. "IRGC Forms Group to Monitor Internet in Iran," *Al-Monitor*, March 25, 2021. (https://www.al-monitor.com/originals/2021/03/irgc-forms-group-monitor-internet-iran)
271. Adena Nima, "What Khamenei's Nowruz Message Means for Iran," *Eurasia Review*, March 25, 2021. (https://www.eurasiareview.com/25032021-what-khameneis-nowruz-message-means-for-iran-oped); "IRGC Forms Group to Monitor Internet in Iran," *Al-Monitor*, March 25, 2021. (https://www.al-monitor.com/originals/2021/03/irgc-forms-group-monitor-internet-iran)
272. U.S. Cyberspace Solarium Commission, "Countering Disinformation in the United States: CSC White Paper #6," December 2021, page 8. (https://cybersolarium.org/white-papers/countering-disinformation-in-the-united-states/)

because of their poor English-language skills.[273] The hackers worked with a former U.S. counterintelligence agent (whom the Justice Department later charged with espionage) and were therefore presumably valuable Iranian operatives. But their grammar revealed them as imposters.

By contrast, when Microsoft revealed a 2020 Iranian operation targeting more than 100 people planning to attend the Munich Security Conference, a prestigious gathering in Germany, the company noted the attackers used "perfect English."[274] One may infer Iranian hackers now have a better command of the English language.

Two Facebook operations highlight Iran's growing understanding of how to leverage social media platforms.[275] Social engineering can convince a target to download malware, hand over credentials, or believe a false narrative. In 2018, Facebook shut down accounts for "coordinated inauthentic behavior" when Iranian hackers tried to convince victims to follow pages and consume disinformation.[276] Three years later, Facebook revealed another operation involving "sophisticated fake online personas" with "profiles across multiple social media platforms to make them appear more credible."[277]

Microsoft also observed that Iranian threat actors are displaying more persistence.[278] Whereas actors previously sent bulk unsolicited emails with malicious attachments, they are now using much more time-consuming and individualized tactics.[279]

"Having witnessed Russia's success at sowing discord during the 2016 election, Iranian hackers attempted a combined hacking and disinformation operation against American citizens."

These improvements were evident in a disinformation operation during the 2020 U.S. presidential election. Having witnessed Russia's success at sowing discord during the 2016 election, Iranian hackers attempted a combined hacking and disinformation operation against American citizens, according to U.S. government statements and a Justice Department indictment.[280] The indictment does not directly

273. U.S. Department of Justice, Press Release, "Former U.S. Counterintelligence Agent Charged with Espionage on behalf of Iran; Four Iranians Charged with a Cyber Campaign Targeting her Former Colleagues," February 13, 2019. (https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber); U.S. Department of Justice, Press Release, "Two Iranians Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," November 18, 2021. (https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed)
274. Zach Whittaker, "Microsoft says Iranian Hacker Targeted 'High Profile' Conference Attendees," *TechCrunch*, October 28, 2020. (https://techcrunch.com/2020/10/28/microsoft-iran-hackers)
275. Annie Fixler, "Iran's Social engineering Capabilities Mature," *Foundation for Defense of Democracies*, July 23, 2021. (https://www.fdd.org/analysis/2021/07/23/irans-social-engineering-capabilities-mature)
276. Nathaniel Gleicher, "Taking Down More Coordinated Inauthentic Behavoir," *Meta*, August 21, 2018. (https://about.fb.com/news/2018/08/more-coordinated-inauthentic-behavior)
277. Mike Dvilyanski and David Agranovich, "Taking Action Against Hackers in Iran," *Meta*, July 21, 2021. (https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran)
278. "Evolving Trends in Iranian Threat Actor Activity — MSTIC Presentation at CyberWarCon 2021," *Microsoft*, November 16, 2021. (https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021)
279. Bill Toulas, "Microsoft Warns of the evolution of Six Iranian Hacking Groups," *Bleeping Computer*, November 16, 2021. (https://www.bleepingcomputer.com/news/security/microsoft-warns-of-the-evolution-of-six-iranian-hacking-groups/?&web_view=true)
280. Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes Iran was behind Threatening Emails sent to Democrats," *The Washington Post*, October 22, 2020. (https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida); U.S. National Intelligence Council, Intelligence Community Assessment, "Foreign Threats to the 2020 US Federal Elections," March 10, 2021. (https://www.intelligence.gov/assets/documents/702%20Documents/declassified/ICA-declass-16MAR21.pdf); U.S. Federal Bureau of Investigation, "Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad," January 26, 2022. (https://www.ic3.gov/Media/News/2022/220126.pdf)

Director of National Intelligence John Ratcliffe arrives to a closed-door briefing on election security for the Senate Select Committee on Intelligence on September 23, 2020, in Washington, DC. (Drew Angerer/Getty Images)

attribute the operation to the Iranian government and only alleges that the hackers worked for a company that provides services to the Iranian regime. However, a U.S. intelligence community assessment concluded with high confidence that Supreme Leader Khamenei likely authorized a "whole of government effort" to interfere in the U.S. election.[281]

Because of the hackers' mistakes, American law enforcement quickly uncovered an effort to intimidate registered Democrats by impersonating the Proud Boys, a right-wing extremist group.[282] The subsequent Justice Department indictment revealed, however, that the operation was more sophisticated than early reporting indicated. The hackers first attempted to compromise voter registration websites in multiple states. Successfully breaching one, the hackers downloaded 100,000 voter records. They then used the information to target registered Democrats with the voter intimidation emails.[283] These emails included the name and address of the recipient and did not contain grammatical errors that compromised their credibility. The hackers also sent messages and videos to Republican lawmakers and members of the media, again pretending to be Proud Boys volunteers, claiming that Democrats were hacking election records and creating fraudulent ballots.[284]

The operation revealed an understanding of the fissures in American society. "The message to Republicans echoed baseless claims Trump had already voiced — that Democrats were prepping to steal the election. The message to Democrats was that thuggish Trump supporters were trying to bully their way to victory," *The Washington Post* explained.[285]

In addition to Tehran's own disinformation operations, the convergence of Iranian, Russian, and Chinese disinformation campaigns provides an avenue for the Islamic Republic to achieve an outsized impact.[286] As scholar Clint Watts has observed:

> By opportunistically reinforcing each other's information manipulation efforts, the cumulative

281. U.S. National Intelligence Council, Intelligence Community Assessment, "Foreign Threats to the 2020 US Federal Elections," March 10, 2021, page 6. (https://www.intelligence.gov/assets/documents/702%20Documents/declassified/ICA-declass-16MAR21.pdf)
282. Christopher Bing and Jack Stubbs, "'Dumb Mistake' Exposed Iranian Hand Behind Fake Proud Boys U.S. Election Emails — Sources," *Reuters*, October 22, 2020. (https://www.reuters.com/article/us-usa-election-cyber-iran-exclusive/exclusive-dumb-mistake-exposed-iranian-hand-behind-fake-proud-boys-u-s-election-emails-sources-idUSKBN2772YL)
283. Tonya Riley, "State Department Offers $10M for Information on Iranian Election Interference," *CyberScoop*, February 2, 2022. (https://www.cyberscoop.com/state-department-offer-10-million-information-iranian-election-interference)
284. *United States of America v. Seyed Mohammad Hosien Mousa Kazemi and Sajjad Kashian*, 21 Cr. 644 (S.D.N.Y. filed 2021). (https://www.justice.gov/opa/press-release/file/1449226/download)
285. Joseph Marks, "Four Takeaways from the Iranian Election Interference Indictments," *The Washington Post*, November 19, 2021. (https://www.washingtonpost.com/politics/2021/11/19/four-takeaways-iranian-election-interference-indictments)
286. Jessica Donati, "U.S. Adversaries Are Accelerating, Coordinating Coronavirus Disinformation, Report Says," *The Wall Street Journal*, April 21, 2020. (https://www.wsj.com/articles/u-s-adversaries-are-accelerating-coordinating-coronavirus-disinformation-report-says-11587514724); Andrew Whiskeyman and Michael Berger, "Axis of Disinformation: Propaganda from Iran, Russia, and China on COVID-19," *Fikra Forum*, February 25, 2021. (https://www.washingtoninstitute.org/policy-analysis/axis-disinformation-propaganda-iran-russia-and-china-covid-19); Michael Lupin, Liyuan Lu, Behrooz Samadbeygi, and Mehdi Jedinia, "Iran, China Amplify Each Other's Allegations of US Coronavirus Culpability," *Voice of America*, March 24, 2020. (https://www.voanews.com/middle-east/voa-news-iran/iran-china-amplify-each-others-allegations-us-coronavirus-culpability)

> sum of their [Russia, Iran, and China] efforts is greater than its individual parts. It also allows each country to concentrate on its comparative advantages. Russia's tremendous capacity for content production and programming in multiple languages offers China and Iran cost savings and extended reach. China's Twitter attacks on America provide the Kremlin an information warfare proxy. Iran's haughty, aggressive anti-American claims allow Russia and China to advance narratives they'd rather not put forth under their own names.[287]

This amplification of each other's messages does not prove coordination. However, the potency of mutually reinforcing disinformation efforts by adversaries is concerning. If U.S. adversaries recognize the benefits of "opportunistically reinforcing" each other's operations, they may begin to apply it to CEEW campaigns.

Lessons From Attacks on Iran's Neighbors

Iranian cyber operations against its regional adversaries "could be a testing ground for attacks against U.S. targets," as *The Washington Post* put it, citing Adam Meyers of cybersecurity firm CrowdStrike.[288] As U.S. sanctions intensified and tensions soared in the Persian Gulf in the summer of 2019,[289] Iran launched cyberattacks against Bahrain. While Tehran's animosity toward Manama pales in comparison to its rivalries with Riyadh and Jerusalem, Bahrain is home to the U.S. Navy's Fifth Fleet and Naval Forces Central Command. Among other targets, Iranian hackers hit Bahrain's Electricity and Water Authority, Aluminum Bahrain, and national oil company Bapco. The attacks disrupted the operation of these critical-infrastructure entities by destroying (or "wiping") data vital to their function.[290] A few months later, IBM's threat researchers disclosed a destructive Iranian campaign targeting industrial and energy firms across the Middle East.[291] Saudi Arabia detected similar activity.[292]

Data destruction has no intelligence value but can have a strategic or psychological value. For example, in late 2020, the Israeli cybersecurity firm ClearSky observed an Iranian APT conducting what appeared to be criminal ransomware operations against Israeli targets.[293] The firm concluded, however, that because the hackers leaked data and posted threatening messages, they were engaged not in ransomware but in information operations aimed at sowing fear in the Israeli public.[294]

Separately, the hacker group MuddyWater — which the U.S. government subsequently called "a subordinate element within the Iranian Ministry of Intelligence and Security"[295] — launched a series of ransomware attacks

287. Clint Watts, "Triad of Disinformation: How Russia, Iran, & China Ally in a Messaging War against America," *Alliance for Securing Democracy*, May 15, 2020. (https://securingdemocracy.gmfus.org/triad-of-disinformation-how-russia-iran-china-ally-in-a-messaging-war-against-america)
288. Joseph Marks, "Four Takeaways from the Iranian Election Interference Indictments," *The Washington Post*, November 19, 2021. (https://www.washingtonpost.com/politics/2021/11/19/four-takeaways-iranian-election-interference-indictments)
289. For more information on the summer 2019 tensions, see: Behnam Ben Taleblu, "Making Sense of Iranian Escalation," *FDD's Long War Journal*, May 20, 2019. (https://www.longwarjournal.org/archives/2019/05/making-sense-of-iranian-escalation.php)
290. Catalin Cimpanu, "New Iranian data wiper malware hits Bapco, Bahrain's national oil company," *ZDNet*, January 9, 2020. (https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company); Bradley Hope, Warren P. Strobel, and Dustin Volz, "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran," *The Wall Street Journal*, August 7, 2019. (https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488)
291. Limor Kessem and IBM Security X-Force Team, "New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East," *IBM Security Intelligence*, December 4, 2019. (https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east)
292. Jenna McLaughlin, "Saudis Warn of new Destructive Cyberattack that Experts Ties to Iran," *Yahoo! News*, January 7, 2020. (https://news.yahoo.com/days-before-suleimani-strike-saudis-warned-of-new-destructive-cyber-attack-013125981.html)
293. "Pay2Kitten — Fox Kitten 2," *ClearSky Cybersecurity*, December 17, 2020. (https://www.clearskysec.com/pay2kitten)
294. "2021 Global Threat Report," *CrowdStrike*, 2021, page 43. (https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf)
295. U.S. Cyber Command, Press Release, "Iranian intel cyber suite of malware uses open source tools," January 12, 2022. (https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools)

on Israeli companies in the fall of 2020.[296] ClearSky assessed that the attack did not aim to extract a ransom for locked data. Rather, the operation resembled Russia's 2017 NotPetya attack on Ukraine, in which hackers disguised their wiper malware (which destroys data) as ransomware (which merely encrypts the data until the victim pays a ransom).[297]

Using ransomware to disguise espionage, destruction, or influence operations helps obscure the attackers' motivation. It may also hinder attribution by creating the impression that the attackers are criminals operating independently from a nation state.

"Learning from other hackers, Iranian APTs have also begun experimenting with supply chain attacks against Iran's neighbors."

Learning from other hackers, Iranian APTs have also begun experimenting with supply chain attacks against Iran's neighbors. In such attacks, the hacker penetrates dozens or hundreds of companies by breaching a trusted vendor, managed service provider, or other third party with direct network access to the victim's systems.

In one operation, Tehran breached a logistics company in Israel, Amital Data, along with other companies in the transportation, logistics, and import sectors. From there, the hackers used Amital's list of clients and login information to breach another 40 firms.[298] While the attack's financial cost remains unclear, targeting the transportation sector is worrisome from a strategic perspective because a military cannot move troops and supplies if the nation's transportation sector is compromised.

The Iranian government's most headline-grabbing cyber operations over the past four years targeted Israeli water facilities.[299] While a June 2020 attack appears to have hit a small agricultural facility with no real-world effects, an unsuccessful April 2020 attack targeting Israel's drinking water could have resulted in a public health crisis.[300] Israel took the operation so seriously that it reportedly responded by launching a cyber operation that knocked a major Iranian port offline.[301]

By launching cyberattacks against its neighbors, Tehran may also be trying to exacerbate tensions between the United States and its allies. For example, when the United States is in delicate nuclear negotiations with Iran, Washington has largely ignored Iranian cyberattacks in

296. "Cybersecurity Groups: Iranians Targeted Top Israeli Firms in Ransomware Attack," *The Times of Israel* (Israel), October 16, 2020. (https://www.timesofisrael.com/cybersecurity-groups-iranians-targeted-top-israeli-firms-in-ransomware-attack)
297. "Operation Quicksand: MuddyWater's Offensive Attack Against Israeli Organizations," *ClearSky Cybersecurity*, October 2020. (https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf). In May 2021, SentinelOne similarly disclosed that it had discovered data-destroying malware targeting Israel that an APT had disguised as ransomware. See: Amitai Ben Shushan Ehrlich, "From Wiper to Ransomware: The Evolution of Agrius," *Sentinel Labs*, May 25, 2021. (https://labs.sentinelone.com/from-wiper-to-ransomware-the-evolution-of-agrius); Dan Goodin, "A Never-Before-Seen Wiper Malware is Hitting Israeli Targets," *Wired*, May 27, 2021. (https://www.wired.com/story/never-before-seen-wiper-malware-hitting-israeli-targets)
298. Stuart Winer, "Cyberattack Hits Israeli Companies, with Iran Reportedly the Likely Culprit," *The Times of Israel* (Israel), December 13, 2020. (https://www.timesofisrael.com/israels-supply-chain-targeted-in-massive-cyberattack); Meir Orbach and Golan Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack," *CTech*, December 13, 2020. (https://www.calcalistech.com/ctech/articles/0,7340,L-3881337,00.html)
299. "Cyber Attacks again hit Israel's Water System, Shutting Agricultural Pumps," *The Times of Israel* (Israel), July 17, 2020. (https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps); Joby Warrick and Ellen Nakashima, "Foreign Intelligence Officials say Attempted Cyberattack on Israeli Water Utilities Linked to Iran," *The Washington Post*, May 8, 2020. (https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html)
300. Mehul Srivastava, Najmeh Bozorgmehr, and Katrina Manson, "Israel-Iran Attacks: 'Cyber Winter is Coming,'" *Financial Times* (UK), May 31, 2020. (https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967)
301. Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *The Washington Post*, May 18, 2020. (https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html)

the Middle East. The absence of an American response may worsen friction between the United States and its Israeli and Arab allies, which already see Washington as too accommodating to Tehran.

Leveraging Common Techniques Against U.S. Critical Infrastructure

The U.S. intelligence community has repeatedly assessed that Iran can "conduct attacks on critical infrastructure."[302] In November 2021, a joint advisory from the FBI, the U.S. Department of Homeland Security, the UK's National Cyber Security Centre, and the Australian Cyber Security Centre warned that "Iranian government-sponsored APTs" are targeting the U.S. transportation and healthcare sectors.[303]

Cybersecurity firm Dragos has observed two Iranian APTs attempting to compromise the ICS of U.S. utilities.[304] Dragos concluded, however, that because Iran lacks "ICS-specific capabilities," the hackers were likely focused "exclusively on information gathering at this time."[305]

Yet Iran does not need ICS-specific capabilities to disrupt critical infrastructure. When U.S. pipeline operator Colonial Pipeline suffered a ransomware attack on its information technology systems in May 2021 at the hands of a Russian ransomware gang, the company "proactively disconnected" components of its gas pipeline "to ensure the systems' safety," explained the Department of Homeland Security.[306] Colonial Pipeline's CEO later testified before Congress that responders "halt[ed] operations throughout the pipeline … to help ensure that malware did not spread to the Operational Technology (OT) network, which controls our pipeline operations."[307] Ransomware effectively shut off a pipeline providing nearly half of all fuel to the East Coast.

Iranian hackers use common tools to conduct their operations, wielding an "opportunistic approach" to cyber operations, the U.S. intelligence community concluded last year.[308] They are attempting, for example, to exploit the widely reported Log4j vulnerability to gain access and exfiltrate data.[309] They are not the first hackers to do so, but the vulnerability is so prevalent across thousands of systems that it is a ripe avenue for attack.

The November 2021 U.S.-UK-Australian joint advisory noted that Iranian APTs are exploiting vulnerabilities as many as three years old and target systems that have not patched a severe vulnerability

302. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, page 14. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf)
303. Sean Lyngaas, "US warns that Iranian government-sponsored hackers are targeting key US infrastructure," *CNN*, November 17, 2021. (https://www.cnn.com/2021/11/17/politics/us-iran-hackers-warning/index.html); U.S. Cybersecurity and Infrastructure Security Agency, "Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities," November 17, 2021. (https://www.cisa.gov/uscert/sites/default/files/publications/AA21-321A-Iranian%20Government-Sponsored%20APT%20Actors%20Exploiting%20Vulnerabilities%20FINAL.pdf)
304. "North American Electric Cyber Threat Perspective," *Dragos*, January 2020. (https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf)
305. "Magnallium," *Dragos*, accessed June 15, 2022. (https://www.dragos.com/threat/magnallium)
306. U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, Joint Cybersecurity Advisory, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," AA21-131A, May 11, 2021. (https://us-cert.cisa.gov/ncas/alerts/aa21-131a)
307. Joseph Blount, "Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure," *Testimony Before the House Committee on Homeland Security*, June 9, 2021. (https://homeland.house.gov/imo/media/doc/2021-06-09-HRG-Testimony-Blount.pdf)
308. Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, page 15. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf)
309. Ravie Lakshmanan, "Iranian Hackers Exploit Log4j Vulnerability to Deploy PowerShell Backdoor," *The Hacker News*, January 13, 2020. (https://thehackernews.com/2022/01/iranian-hackers-exploit-log4j.html)

in Microsoft Exchange.[310] This vulnerability earned headlines in 2021 for its severity and scale.[311] In July 2021, Sky News, a British television station, obtained a cache of documents that purported to be assessments by IRGC hackers of possible cyber targets, including Western cargo ships, fuel pumps, building management systems, and maritime communications networks. The hackers "appeared to rely on open source research rather than any privileged information," Sky News reported. Private cybersecurity firm Mandiant concluded that the Iranian hackers focused on "simple, opportunistic attacks."[312]

Using unsophisticated techniques that are easy to spot does not mean an APT group is amateur. For example, Microsoft noted that the Iranian APT group was "deliberate" and "operationally, very sophisticated."[313] The group may not need to use custom malware or sophisticated techniques to be successful because its victims have weak defenses. In a separate report, Microsoft revealed that Iranian hackers had used "password spraying" — attempting multiple guesses of predictable passwords to break into an account — against U.S. and Israeli defense companies. The report noted that basic security measures can protect against this technique.[314]

Iranian hackers are dangerous because they are opportunistic, adopt the successful strategies and tools of other hackers, and exploit the weak defenses of their targets.

Right-Sizing Concerns About Cooperation With Other U.S. Adversaries

In November 2018, the Department of Justice indicted two Iranian hackers for a nearly three-year ransomware campaign that generated $6 million in revenue and cost victims — including the cities of Atlanta and Newark, the Port of San Diego, and six hospitals and other healthcare-related companies — more than $30 million.[315] More recently, in May, researchers linked an Iranian government-backed group to financially motivated data exfiltration, ransomware, and extortion.[316] It is not clear, however, if the hackers were raising funds for the government or themselves. Tehran could learn from these experiences and begin using ransomware not only to disguise other motives but also to raise funds to bankroll a range of malign activity.

The North Korean regime provides an example of this phenomenon. As the North Korea chapter of this monograph explains, financially motivated cyberattacks lie at the core of Pyongyang's cyber strategy and have enabled the regime to remain solvent despite robust U.S. and UN sanctions. Were Iran to face a severe economic recession, Tehran could mimic Pyongyang's

310. U.S. Federal Bureau of Investigation, U.S. Cybersecurity and Infrastructure Security Agency, Australian Cyber Security Centre, and UK National Cyber Security Center, "Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities," November 17, 2021. (https://www.cisa.gov/uscert/sites/default/files/publications/AA21-321A-Iranian%20Government-Sponsored%20APT%20Actors%20Exploiting%20Vulnerabilities%20FINAL.pdf)
311. U.S. Cybersecurity and Infrastructure Security Agency, "Remediating Microsoft Exchange Vulnerabilities," 2021. (https://www.cisa.gov/uscert/remediating-microsoft-exchange-vulnerabilities); Kristine Phillips, "Biden Administration Blames China for Microsoft Hacking as DOJ Indicts Chinese Nationals in Cyberattacks," *USA Today*, July 19, 2021. (https://www.usatoday.com/story/news/politics/2021/07/19/microsoft-exchange-hack-january-came-china-us-says/8011021002)
312. Deborah Haynes, "Iran's Secret Cyber Files," *Sky News* (UK), July 26, 2021. (https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871)
313. Sean Lyngaas, "APT33 has Shifted Targeting to Industrial Control Systems Software, Microsoft says," *CyberScoop*, November 22, 2019. (https://www.cyberscoop.com/apt33-microsoft-iran-ics)
314. Maggie Miller, "Microsoft Reports Iranian Hackers Targeting US, Israeli Defense Companies," *The Hill*, October 11, 2021. (https://thehill.com/policy/cybersecurity/576250-microsoft-reports-iranian-hackers-targeting-us-israeli-defense-companies)
315. U.S. Department of Justice, Office of Public Affairs, Press Release, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," November 28, 2018. (https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public)
316. AJ Vicens, "Analysis of Well-Known Iranian Hacking Group Points to More Purely Financial Attacks," *CyberScoop*, May 12, 2022. (https://www.cyberscoop.com/iranian-hacking-cobalt-mirage-phosphorous-charming-kitten-ransomware)

strategy, acquire North Korean malware, and learn best practices through bilateral agreements.

However, this strategy poses risks for the Islamist regime. A study at Columbia University concluded that Tehran is unlikely to launch financially motivated attacks against global financial institutions, because doing so would "damage Iran's credibility as an economic partner."[317]

Russia and Iran, meanwhile, have signed several cybersecurity cooperation agreements over the past five years.[318] In January 2021, the two countries signed an accord to coordinate their cyber activities, exchange technology, cooperate on training, and coordinate within international institutions.[319] Iran's Foreign Ministry said the agreement covers cooperation on detection of cyber intrusions and coordination "to ensure national and international security."[320]

Previous cyber cooperation agreements between Tehran and Moscow have not led to any observable tactical coordination on offensive operations. But because Iranian hackers are far less skilled than their Russian counterparts, any knowledge transfer would improve Tehran's cyber capabilities.

Still, recognition of Russia and Iran's history of mutual suspicion and the enduring tension between them should temper handwringing about Russian and Iranian cooperation, although the two powers appear to be growing closer following Moscow's invasion of Ukraine.[321] While Russia finally delivered its S-300 air defense system to Iran after the implementation of the 2015 Iran nuclear deal,[322] Moscow has not sold Tehran its more advanced S-400 system despite making it available to Turkey and other buyers.[323] In the cyber realm, distrust at the operator level — that is, among the actual hackers — may also be high after reports that Russian hackers commandeered Iranian cyber-espionage infrastructure to launch their own operations.[324]

By contrast, Beijing and Tehran have historically recognized the value of a strong bilateral relationship.[325]

317. Erika Banuelos, Clara Brackbill, Kirill Buskirk, Haakon Husoy, Jiwon Ma, Meg Mannix, Daniel Sorek, and Sam Weaver, "Assessing Iran's Cyber Strategy: Risks to the Financial Sector," *Columbia University School of International and Public Affairs*, April 2021. (https://www.sipa.columbia.edu/academics/capstone-projects/why-and-when-do-states-target-financial-institutions)
318. John Hardie and Annie Fixler, "Russia-Iran cooperation poses challenges for US cyber strategy, global norms," *C4ISRNET*, February 8, 2021. (https://www.c4isrnet.com/thought-leadership/2021/02/08/russia-iran-cooperation-poses-challenges-for-us-cyber-strategy-global-norms)
319. "Russia, Iran Sign Agreement on Cyber Security Cooperation," *TASS* (Russia), January 26, 2021. (https://tass.com/politics/1248963); "МИД раскрыл детали соглашения Ирана и России об информационной безопасности [The Ministry of Foreign Affairs revealed the details of the agreement between Iran and Russia on information security]," *Izvestia* (Russia) January 26, 2021. (https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti)
320. Islamic Republic of Iran Ministry of Foreign Affairs, "Iran, Russia Sign Information Security Cooperation Pact," January 26, 2021. (https://en.mfa.ir/portal/NewsView/625777)
321. "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East," *Council on Foreign Relations*, March 15, 2021. (https://www.cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east); Zeke Miller and Josh Boak, "White House: Iran set to deliver armed drones to Russia," *Associated Press*, July 11, 2022. (https://apnews.com/article/russia-ukraine-biden-iran-jake-sullivan-4a9f1b2749893d8f1ed9f039869cf119)
322. For a history of the S-300 sale, see: Patrick Megahan and Behnam Ben Taleblu, "Making Sense of Iranian S-300s," *The Hill*, June 3, 2015. (https://thehill.com/blogs/congress-blog/homeland-security/243784-making-sense-of-iranian-s-300s)
323. "Iran Placed No Order to Buy Russia's S-400 Missile System: Advisor," *Tehran Times* (Iran), November 14, 2020. (https://www.tehrantimes.com/news/454624/Iran-placed-no-order-to-buy-Russia-s-S-400-missile-system-advisor)
324. Jack Stubbs and Christopher Bing, "Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say," *Reuters*, October 21, 2019. (https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK)
325. Scott W. Harold and Alireza Nader, "China and Iran: Economic, Political, and Military Relations," *RAND Corporation*, May 2, 2012. (https://www.rand.org/pubs/occasional_papers/OP351.html); U.S.-China Economic and Security Review Commission, Staff Research Report, "China-Iran Relations: A Limited but Enduring Strategic Partnership," June 28, 2021. (https://www.uscc.gov/sites/default/files/2021-06/China-Iran_Relations.pdf)

As a significant purchaser of Iranian crude oil and a critical trade partner,[326] China has provided Iran with telecommunications and surveillance equipment, often in defiance of U.S. sanctions. Chinese telecommunications giants Huawei and ZTE have provided surveillance equipment to the Iranian government to monitor texts, calls, and emails for nearly a decade.[327] Washington has penalized companies for sanctions evasion and obstruction of justice related to these sales.[328] However, prior agreements, high-level visits, goodwill gestures, and even equipment sales between the two countries appear not to have led to a change in Iranian offensive cyber activities.[329]

Finally, it is worth noting that Iran has long shared China's and Russia's goal of challenging norms of a free and open internet, although coordination between these countries is loose at best.[330] The Islamic Republic, along with human rights abusers such as Belarus, Myanmar, Syria, and Venezuela, cosponsored a 2019 UN resolution proposed by Russia and China that would legitimize domestic repression.[331] Within the Chinese- and Russian-led Shanghai Cooperation Organization, which last year granted Iran full membership,[332] Tehran seeks cooperation to combat the influence of foreign social media organizations.[333] And within the annual Caspian Media Forum, Iran is working with other members to combat "imposed external values alien to" the region.[334] This collaboration in international forums sets the stage for further cooperation.

326. Erika Holmquist and Johan Englund, "China and Iran — an Unequal Friendship," *Swedish Defense Research Agency*, May 2020. (https://www.foi.se/rest-api/report/FOI-R--4976--SE)
327. Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012. (https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322); Steve Stecklow, "Exclusive: Newly Obtained Documents Show Huawei Role in Shipping Prohibited U.S. Gear to Iran," *Reuters*, March 2, 2020. (https://www.reuters.com/article/us-huawei-iran-sanctions-exclusive-idUSKBN20P1VA)
328. James Vincent, "ZTE Receives Record $1.2 Billion Fine for Breaking US Sanctions," *The Verge*, March 8, 2017. (https://www.theverge.com/2017/3/8/14852182/zte-embargo-iran-north-korea-record-fine); Arthur Cyr, "China's Huawei Faces a Showdown, in Court," *Chicago Tribune*, April 8, 2020. (https://www.chicagotribune.com/suburbs/lake-county-news-sun/opinion/ct-lns-cyr-china-shutdown-st-0411-20200408-5axthwyj7zdv3cpo6otqeoeuwm-story.html)
329. Islamic Republic of Iran Presidential Administration, "Full Text of Joint Statement on Comprehensive Strategic Partnership between I.R. Iran, P.R. China," January 23, 2016. (http://president.ir/en/91435); "Iran, China to Expand ICT Cooperation," *Financial Tribune* (Iran), June 15, 2015, (https://financialtribune.com/articles/sci-tech/18983/iran-china-to-expand-ict-cooperation); Zak Doffman, "Cyber Warfare Threat Rises as Iran and China Agree 'United Front' Against U.S.," *Forbes*, July 6, 2019. (https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/?sh=b82162b42ebd)
330. James Marchant and Bronwen Robertson, "Chaos & Control: The Competing Tensions of Internet Governance in Iran," *Internet Policy Observatory*, January 2015, page 46. (https://repository.upenn.edu/cgi/viewcontent.cgi?article=1014&context=internetpolicyobservatory): UN General Assembly, "Countering the use of information and communications technologies for criminal purposes," A/C.3/74/L.11/Rev.1, November 5, 2019. (https://undocs.org/en/A/C.3/74/L.11/Rev.1); Justin Sherman and Mark Raymond, "The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom," *The Washington Post*, December 4, 2019. (https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom); Shannon Vavra, "The U.N. Passed a Resolution that gives Russia Greater Influence over Internet Norms," *CyberScoop*, November 18, 2019. (https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms)
331. Justin Sherman and Mark Raymond, "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom." *The Washington Post*, December 4, 2019. (https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom)
332. Bradley Bowman, Ryan Brobst, and Zane Zovark, "Iran Joining the Shanghai Cooperation Organization," *Foundation for Defense of Democracies*, September 22, 2021. (https://www.fdd.org/analysis/2021/09/22/iran-joining-shanghai-cooperation-organisation)
333. "Iran Calls for International Cooperation against Cyber Terrorism," *Iran Front Page* (Iran), June 9, 2018. (https://ifpnews.com/iran-calls-for-international-cooperation-against-cyber-terrorism)
334. "Astrakhan to Host 1st Caspian Media Forum," *Republican Information Agency* (Russia), September 2, 2015. (https://www.riadagestan.com/mobile/news_en/society/astrakhan_to_host_1st_caspian_media_forum_)

Recommendations

FDD's 2018 monograph on Iranian CEEW offered policymakers 10 recommendations to better understand the Iranian cyber threat, strengthen U.S. and allied defense capabilities, and impose costs on Tehran for its malicious cyber activities.[335] Washington has still not done enough on these three fronts.

2018 Recommendations

Understand The Iranian Cyber Threat Landscape

1. Analyze Tehran's cyber escalatory ladder.
2. Analyze Tehran's cyber investments, industrial base, and partnerships with other rogue actors in order to target these assets as needed.

Strengthen Defense

3. Bolster information sharing with U.S. allies to improve allied defenses.
4. Develop a joint R&D agenda with U.S. allies to address common threats from Iran and other malicious cyber actors.
5. Conduct joint cyber wargames with allies in the Middle East to demonstrate U.S. resolve to defend allies.
6. Announce that the United States will defend its key allies from significant Iranian cyberattacks.

Impose Costs On Tehran

8. Sanction key Iranian leaders for authorizing cyberattacks.
9. Use cyber-enabled information warfare capabilities to exploit and sharpen divisions between the regime and the Iranian public.
10. Hold at risk Iranian assets using cyber and kinetic means.

While punishing Iran remains important, it will always be a reactive policy to address Tehran's capabilities. The maturation of Iranian cyber capabilities over the past four years requires greater attention to understand the trajectory of the Iranian cyber threat. The Islamic Republic has demonstrated its intent to attack American allies. The United States should take the following steps to prevent Tehran from becoming a more capable cyber power.

1. **Undermine Tehran's control over the Iranian people's access to information.** Capabilities that the regime deploys against its own citizens can quickly present a threat to U.S. national security. Protests in Iran against government policies and against the theocracy itself continue.[336] Thus, the regime will likely resort to violence and even sever access to the global internet. This presents an opportunity for the United States to help the Iranian people evade censorship. For example, Washington should devise a land-based or satellite solution as an alternative to SHOMA so the Iranian people have better access to information.[337] This could serve as a test case for supplying freedom of information to other oppressed people, including in China, Russia, and North Korea.

2. **Sow divisions between hackers working for different parts of the Iranian government.** The structure of the Iranian hacker community is one of a loose contractor model in which quasi-independent hacker groups take commissions from the Iranian government to conduct operations. The cybersecurity firm Recorded Future reports that feuds between the IRGC and the Ministry of Intelligence are likely causing hackers to align more closely with one faction or the other. Infighting

335. Annie Fixler and Frank Cilluffo, "Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, November 9, 2018. (https://www.fdd.org/analysis/2018/11/06/evolving-menace)
336. Saeed Ghasseminejad, Behnam Ben Taleblu, and Eliora Katz, "Evolution Toward Revolution: The Development of Street Protests in the Islamic Republic of Iran," *Columbia Journal of International Affairs*, October 29, 2020, Volume 73, Issue 2, pages 147–161. (https://jia.sipa.columbia.edu/evolution-toward-revolution-development-street-protests-islamic-republic-iran)
337. For how the United States can effectively aid protestors, see: Behnam Ben Taleblu and Saeed Ghasseminejad, "Towards a Bipartisan Iran Protest Policy Playbook," *Radio Farda*, November 21, 2019. (https://en.radiofarda.com/a/towards-a-bipartisan-iran-protest-policy-playbook/30284555.html)

between regime factions may present its adversaries with an opportunity to undermine Iranian capabilities. Unconfirmed reports indicate that other Iranian hackers were responsible for a leak about an Intelligence Ministry-affiliated group,[338] forcing it to "re-tool and focus on new campaigns going forward, potentially delaying any current or planned hacking efforts," according to the business and technology news site *ZDNet*.[339]

Washington should exploit divisions within Iran's intelligence agencies and hacker community to instigate internecine fighting. Tactics might include posing as one group to leak the tools of another or spreading disinformation about how Khamenei favors one group over another. The goal would be to exacerbate rivalries so that the hackers betray their own.

3. **Sanction Iranian universities and cyber centers of excellence.** Just as Washington has sanctioned Iranian universities that recruit promising students into science and technology departments, thereby feeding Tehran's nuclear and missile programs, Washington should sanction academic institutions that support Iranian cyber capabilities, such as Shahid Beheshti University and Sharif University of Technology.[340] Such measures can undermine or restrain the systems that produce the next generation of malicious Iranian cyber actors. The sanctions would damage the institutions' reputations and could even hamper their ability to recruit students and engage in cutting-edge scientific research.

4. **Enhance intelligence sharing with Israel and Iran's Arab neighbors and increase global cyber diplomacy.** Understanding the tactics Iran deploys against its neighbors would provide insights into future attacks against America. Therefore, Washington should continue and, where possible, increase intelligence cooperation with regional allies, particularly Israel, which is the most capable cyber actor in the Middle East. Greater diplomatic engagement with all U.S. allies about cybersecurity and norms would complement enhanced intelligence sharing, undermine Iranian efforts to use cyber operations to divide U.S. allies, and enhance the deterrent capabilities of U.S. partners.

5. **Analyze cooperation, technology transfer, and training between Iran and its allies.** The United States should study the collaboration between Iran and other U.S. adversaries and whether Iranian capabilities are improving thanks to help from other cyber powers. While Tehran will eagerly announce diplomatic exchanges, memoranda of understanding, and multi-year investment deals with other countries, Iranian cyber cooperation requires further study. This should be a priority of the U.S. intelligence community.

Conclusion

There is no shortage of steps Congress and the administration must take to enhance U.S. resilience and to thwart and deter cyberattacks. However, defense alone is insufficient. Similarly, deterrence is insufficient. The United States and its allies must actively prevent their adversaries from becoming more capable cyber actors whom they cannot combat or deter.

338. Insikt Group, "Despite infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure," *Recorded Future*, April 9, 2020, page 5. (https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf)
339. Catalin Cimpanu, "New Leaks of Iranian Cyber-Espionage Operations Hit Telegram and the Dark Web," *ZDNet*, May 8, 2019. (https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web)
340. For more on the role of these universities in support of Iran's cyber capabilities, see: Annie Fixler and Frank Cilluffo, "Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, November 9, 2018. (https://www.fdd.org/analysis/2018/11/06/evolving-menace)

Acknowledgments

This study stands on the shoulders of the groundbreaking work of the authors of FDD's 2018 monographs on cyber-enabled economic warfare (CEEW), as well as the scholarship of numerous others. We are grateful for the insights shared by experts and reviewers who helped the authors of this updated study refine the analysis presented herein. It has been our honor to work with this group of authors, who have each offered unique recommendations on how to understand and thwart the future campaign strategies of U.S. adversaries. We would also like to thank the world class FDD editing team of David Adesnik, John Hardie, and Tzvi Kahn, who took a scalpel to every sentence to ensure the final product would not only add critical scholarship to the CEEW field but also be compelling and engaging for the reader. We also owe a debt of gratitude to Erin Blumenthal and Daniel Ackerman, who have worked with us since the 2018 monographs to visualize and communicate the concept of CEEW. Their creativity has enlivened the scholarship. None of this work would be possible without the ongoing encouragement of our supporters — those philanthropies and philanthropists who recognize that research like ours helps defend our country's future.

Cover Illustration by Daniel Ackerman/FDD

About the Authors

Samantha F. Ravich, Ph.D.

Monograph Editor

Dr. Samantha Ravich is the chair of FDD's Center on Cyber and Technology Innovation. She serves on the U.S. Secret Service's Cyber Investigation Advisory Board and was as a commissioner on the Cyberspace Solarium Commission, vice chair of the President's Intelligence Advisory Board, and co-chair of the Artificial Intelligence Working Group of the Secretary of Energy Advisory Board.

Annie Fixler

Monograph Editor

Annie Fixler is a research fellow at FDD and deputy director of FDD's Center on Cyber and Technology Innovation, working on issues related to cyber-enabled economic warfare, the national security implications of cyberattacks on economic targets, adversarial strategies and capabilities, U.S. cyber resilience, and offensive and defensive tools of economic coercion.

Mathew Ha

Mathew Ha is an analyst at Valens Global, a private firm focused on creative solutions to complex national security challenges. Prior to joining Valens, Mathew was a research associate at FDD focusing on North Korean illicit finance, human rights, the U.S.-South Korea alliance, and inter-Korean relations.

RADM (Ret.) Mark Montgomery

Mark Montgomery is the senior director of FDD's Center on Cyber and Technology Innovation and an FDD senior fellow. He also directs CSC 2.0, an effort to continue the work of the Cyberspace Solarium Commission, where he served as executive director. Previously, Mark served as policy director for the Senate Armed Services Committee.

Ryan Tully

Ryan Tully served as senior director for European and Russian affairs at the National Security Council (NSC). Previously, Ryan was the senior advisor for arms control and the deputy senior director for the Weapons of Mass Destruction Directorate at the NSC. He has served in multiple roles on Capitol Hill and as an information dominance warfare officer in the U.S. Navy Reserve.

Logan Weber

Logan Weber holds an MA in international affairs from the George H.W. Bush School of Government and Public Service at Texas A&M University. Prior to graduation, Logan worked as a research advisor at the Atlantic Council, the Scowcroft Institute, and the Belfer Center, contributing to scholarship on global trade and national security, the disruptive role of cryptocurrencies, and weaponized cyber capabilities.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

About FDD's Center on Cyber and Technology Innovation (CCTI)

CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org