DIGITAL DETERRENCE THROUGH FINANCIAL CONTROLS: ANTI-MONEY LAUNDERING LAWS, LAWFARE, AND THE PRC CYBER THREAT

TABLE OF CONTENTS

INTRODUCTION

According to a February 2023 report by the Center for Strategic and International Studies, at least 104 instances of cyber espionage have been publicly attributed to cyber forces from the People's Republic of China (PRC) over the past two and a half decades.[1] The 2024 Annual Threat Assessment by the Office of the Director of National Intelligence reiterated the U.S. Intelligence Community's position that the PRC "remains the most active and persistent cyber threat to U.S. [g]overnment, private-sector, and critical infrastructure networks."[2] This threat endures despite numerous lines of effort within the U.S. federal government to counter the PRC by pressing criminal charges, enacting sanctions, implementing export

1. *Survey of Chinese Espionage in the United States Since 2000*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 2023), https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000 [https://perma.cc/QN4W-FLRM]. This Note will utilize the term "PRC" in reference to the mainland Chinese Communist Party in order to distinguish the country's political leadership from the general Chinese populace. *See generally Understanding the Black Box of Chinese Politics*, ASIA SOC'Y POL'Y INST., https://asiasociety.org/policy-institute/decoding-chinese-politics/introduction-black-box-chinese-policy [https://perma.cc/C5D9-4KNY] (discussing the difference between the Chinese political system and the Chinese state). This is particularly important in the face of the growing anti-China hysteria that has gained steam in Washington over the last few administrations. *See generally* Nina Luo, *The American Victims of Washington's Anti-China Hysteria*, NEW REPUBLIC (May 20, 2021), https://newrepublic.com/article/162429/yellow-peril-rhetoric-selling-war-with-china [https://perma.cc/8RWE-XZL2] (highlighting how political hysteria against China has fueled xenophobic rhetoric and policy harms); Chandran Nair, *Anti-China Rhetoric Is Off the Charts in Western Media*, DIPLOMAT (Feb. 21, 2023), https://thediplomat.com/2023/02/anti-china-rhetoric-is-off-the-charts-in-western-media/ [https://perma.cc/37HJ-QL7E] ("A key feature of mainstream Western media today is the relentless China-bashing. It is off the charts and tiring, often involving regurgitated trivia or fabricated stories with no evidence to support callous statements about the country, demonstrating a deep lack of understanding."); Andreas Kluth, Opinion, *It's Time for a Pause in US Hysteria About China*, BLOOMBERG (Aug. 14, 2023, at 08:30 ET), https://www.bloomberg.com/opinion/ articles/2023-08-14/us-hysteria-over-china-threat-could-drag-down-world-economy [https://perma.cc/43PV-4L3R] (criticizing escalating U.S. fear-driven rhetoric about China that threatens global stability); Devlin Barrett, *Experts Who Warn of Risks Posed by Chinese Students Are Skeptical of Trump Plan*, N.Y. TIMES (May 31, 2025), https://www.nytimes.com/2025/05/31/us/politics/trump-china-student-visas-crackdown-risks.html [https://perma.cc/8G5X-J9LZ] (reporting on politically motivated anti-China investigations targeting Chinese nationals).

2. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 11 (2024) [hereinafter ODNI ASSESSMENT], https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf [https://perma.cc/D3ND-PGPD].

controls, and improving international cooperation.[3] Despite concerted efforts by a plethora of U.S. federal agencies to counteract this threat, existing legal tools have so far yielded limited success in slowing the onslaught of PRC state-sponsored cyber activities.[4] The U.S. government's persistent inability to effectively deter the PRC's Malicious Cyber Activity (MCA) or degrade the capabilities of the PRC cyber forces highlights the urgent need to explore a wider range of legal strategies to address this challenge more effectively.[5]

The traditional legal mechanisms used to deter PRC MCA face significant drawbacks and limitations. Criminal charges, often brought under the Computer Fraud and Abuse Act (CFAA) or wire fraud statutes, face jurisdictional hurdles and come with the

3. *See U.S. Responses to the China Cyber Challenge: Diplomatic Efforts to Establish Norms in Cyberspace: Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States Before the U.S.-China Econ. Sec. Rev. Comm'n.*, 117th Cong. 178-85 (2022) (statement of Adam Segal, Ira A. Lipman Chair in Emerging Techs. & Nat'l Sec., & Dir., Digit. & Cyber Program, Council on Foreign Rels.), https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states [https://perma.cc/3L9C-37KE].

4. Numerous federal agencies, including the Department of Justice (DOJ), Department of Commerce (DOC), Department of Defense (DOD), Department of the Treasury, Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI), have actively engaged in coordinated efforts to counter cyber threats posed by the PRC. *See, e.g.*, Press Release, U.S. Dep't of Just., Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns (Mar. 5, 2025), https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global [https://perma.cc/U87Y-MMDU]; Press Release, U.S. Dep't of Com., Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats (Jan. 14, 2025), https://www.bis.gov/press-release/ commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats [https://perma.cc/PL74-5DVA]; *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 7, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a [https://perma.cc/B64B-NZQH]; C. Todd Lopez, *U.S. Can Respond Decisively to Cyber Threat Posed by China*, U.S. DEP'T OF DEF.: DOD NEWS (Feb. 1, 2024), https://www.defense.gov/News/News-Stories/Article/Article/3663799/us-can-respond-decisively-to-cyber-threat-posed-by-china/ [https://perma.cc/UQ26-NURF]; Press Release, U.S. Dep't of Treasury, Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise, (Jan. 17, 2025), https://home.treasury.gov/news/press-releases/jy2792 [https://perma.cc/DF27-HYJ3].

5. *See* Press Release, H. Comm. on Oversight & Accountability, Hearing Wrap Up: U.S. Must Bolster Efforts to Deter and Defend Against Evolving Cyberthreat from China (May 16, 2024), https://oversight.house.gov/release/hearing-wrap-up-u-s-must-bolster-efforts-to-deter-and-defend-against-evolving-cyberthreat-from-china/ [https://perma.cc/BV78-KWYJ].

challenge of attributing MCA to specific individuals or entities.[6] Sanctions, another measure frequently employed by the U.S. government, have similarly been hampered by logistical difficulties in attributing MCA and the onerous task of updating the list of sanctioned PRC entities in a timely manner.[7]

Export controls aimed at restricting the flow of advanced technologies and talent to the PRC have also shown limitations.[8] International coordination, crucial for effective cybersecurity, has been characterized as "piecemeal," with substantial discrepancies in sanctions, export control systems, and technology stack harmonization among U.S. allies and partners.[9] Civil lawsuits in U.S. venues, while offering a direct pathway for victims to seek compensation, are often hindered by the challenge of identifying cyber actors.[10] The considerable limitations of existing legal mechanisms underscore the need to establish other legal strategies to inhibit the PRC cyber threats.

This Note argues that anti-money laundering (AML) laws have the potential to serve as powerful tools in disrupting and degrading

---

6. *See* Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks*, 113 A.J.I.L. UNBOUND 202, 202-05 (2019); Jake Sepich, *The Evolution of Cyber Attribution*, AM. UNIV. CTR. FOR SEC., INNOVATION & NEW TECH. (Apr. 19, 2023), https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm [https://perma.cc/9ZV4-293Q]; OFF. OF LEGAL EDUC., U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES 1-3, 109-19 (2010), https://www.justice.gov/criminal/file/442156/dl [https://perma.cc/UC78-R93S].

7. *See* Jason Bartlett & Megan Ophel, *Sanctions by the Numbers: Spotlight on Cyber Sanctions*, CTR. FOR A NEW AM. SEC. (May 4, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber [https://perma.cc/6NTH-4VTQ].

8. *See, e.g.*, Sujai Shivakumar, Charles Wessner & Thomas Howell, *Balancing the Ledger: Export Controls on U.S. Chip Technology to China*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 21, 2024), https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china [https://perma.cc/589S-SZE5] (explaining the limitations of export controls in limiting access to key technologies, specifically semiconductors).

9. *Are America's Allies the Holes in its Export-Control Fence?*, ECONOMIST (Oct. 16, 2023), https://www.economist.com/business/2023/10/16/are-americas-allies-the-holes-in-its-export-control-fence [https://perma.cc/MH94-FQ7R]; *see* Michele Savini Zangrandi, *Disentangling Huawei from the US Has Proven Harder than Anticipated*, PETERSON INST. FOR INT'L ECON. (Dec. 4, 2019, at 04:00 ET), https://www.piie.com/blogs/realtime-economic-issues-watch/disentangling-huawei-us-has-proven-harder-anticipated [https://perma.cc/4WXL-3WSM].

10. *Cf.* Amy Hogan-Burney & George Ramsey, *Cybercrime Disruption Through Civil Litigation and Equitable Remedies*, LAWFARE (May 10, 2023, at 09:15 ET), https://www.lawfaremedia.org/article/cybercrime-disruption-through-civil-litigation-and-equitable-remedies [https://perma.cc/863L-CG45] (discussing civil litigation as a tool for disrupting cybercrime).

the support networks that enable and sustain PRC offensive cyber operations.[11] The Bank Secrecy Act (BSA) has been the foundation of U.S. AML laws since its enactment.[12] Subsequent amendments and additions have allowed the AML regulatory regime to evolve and combat new forms of illicit financial activity.[13] The robust nature of the AML framework can be leveraged against PRC cyber actors to disrupt the funding streams that enable PRC cyber actors to attract technical talent, procure vulnerabilities, maintain infrastructure, and launder illicit proceeds.[14] Part I provides an

---

11. *Cf. Countering Threats Posed by the Chinese Communist Party to U.S. National Security: Hearing Before the H. Comm. on Homeland Sec.*, 119th Cong. 45-46 (2025) [hereinafter *Countering Threats Hearing*] (statement of Dr. Rush Doshi, C.V. Starr Senior Fellow for Asian Stud. & Dir. of the China Strategy Initiative, Couns. on Foreign Rels. & Assistant Professor of Sec. Stud., Georgetown Univ.) (noting the threat of PRC cyber activity and the possibility of using AML law to combat PRC activity relating to fentanyl manufacturing).

12. *See The Bank Secrecy Act*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act [https://perma.cc/PWF5-D8VF]; Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1829b, 1951-1960 and 31 U.S.C. §§ 5311-5314, 5316-5336).

13. *See* Alina Laumann, *The History of Anti-Money Laundering—Events, Regulations, and Adaptions in the United States*, KROLL (July 16, 2019), https://www.kroll.com/en/insights/publications/compliance-risk/history-anti-money-laundering-united-states [https://perma.cc/LF5L-4BPC].The most recent amendment, the Anti-Money Laundering Act of 2020 (AMLA), required "federal-level beneficial ownership disclosure and transparency requirements," theoretically enhancing the government's capacity to trace and disrupt financial networks that support PRC cyber operations in blue or gray cyberspace terrain. LIANA W. ROSEN & RENA S. MILLER, CONG. RSCH. SERV., R47255, THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN): ANTI-MONEY LAUNDERING ACT OF 2020 IMPLEMENTATION AND BEYOND (2022), https://crsreports.congress.gov/product/pdf/R/R47255 [https://perma.cc/68YH-LW5L]. Although the Trump Administration promised to not enforce the beneficial ownership requirement, Congress has a long-established track record of expanding the AML framework. *See* David Ljunggren, *US Treasury Department Says It Will Not Enforce Anti-Money Laundering Law*, REUTERS (Mar. 2, 2025, at 20:50 ET), https://www.reuters.com/world/us/us-treasury-department-says-it-will-not-enforce-anti-money-laundering-law-2025-03-03/ [https://perma.cc/8DAK-MJ68].

14. U.S.-CHINA ECON. & SEC. REV. COMM'N, 117TH CONG., 2022 REPORT TO CONGRESS 418-21, https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf [https://perma.cc/A9EH-VLJP] ("China is a global leader in vulnerability exploitation, highlighting the substantial exploitation development talent within China's domestic hacker community. The astounding improvement in Chinese cyber capabilities since 2013 is the product of sustained attention at the highest levels of China's political leadership, major reorganizations of its cyber-related institutions, and substantial investments in its future cybersecurity workforce."). *See generally* FIN. ACTION TASK FORCE, ILLICIT FINANCIAL FLOWS FROM CYBER-ENABLED FRAUD (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

overview of the PRC's cyber force structure and the national objectives it seeks to achieve through state-sponsored cyber operations. Part II examines the existing legal mechanisms employed to combat PRC MCA, including criminal charges, sanctions, export controls, investment restrictions, civil lawsuits, and other regulatory measures. Part III introduces AML laws as an additional tool in the legal and regulatory toolkit used to disrupt, degrade, and deny PRC MCA by focusing on the operations-adjacent cyber support ecosystem precariously tethered to global financial networks. Part IV explores recent domestic legislative proposals and opportunities for collaboration with international partners to enhance AML enforcement efforts.

I. THE CHALLENGE OF PRC MALICIOUS CYBER ACTIVITY

The PRC poses a significant and persistent cyber threat to the United States and its allies through its targeting of "multiple critical infrastructure sectors, including communications, energy, transportation systems, and water."[15] The objectives of PRC cyber actors include espionage, intellectual property theft, public opinion curation, individual financial pursuits, and strategic pre-positioning on U.S. "networks for disruptive or destructive cyberattacks ... in the event of a major crisis or conflict with the United States."[16] These activities not only pose a broader economic threat, but also present an immediate security risk to the United States.[17] Tailoring countermeasures to specific threat actors and specific stages of the cyber exploitation pipeline can enhance their efficacy by exploiting

---

[https://perma.cc/WK9Q-Z9YL] (highlighting how the robust AML framework can be effectively used to target and disrupt illicit financial activities by malicious cyber actors).

15. U.S. DEP'T OF DEF., MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 86 (2024); *see also PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, *supra* note 4.

16. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 4; *see also Countering Hybrid Threats*, NATO (May 7, 2024, at 15:29 ET), https://www.nato.int/cps/en/natohq/topics_156338.htm [https://perma.cc/PCT6-75GN]; *People's Republic of China Cyber Threat*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china [https://perma.cc/X5HZ-BPD2].

17. *See Countering Threats Hearing*, *supra* note 11, at 47 (statement of Dr. Rush Doshi, C.V. Starr Senior Fellow for Asian Stud. & Dir. of the China Strategy Initiative, Couns. on Foreign Rels. & Assistant Professor of Sec. Stud., Georgetown Univ.).

unique vulnerabilities and disrupting particular operational patterns.[18]

Security researcher Max Smeets categorized the cyber kill chain requirements under the "PETIO framework: people, exploits, toolset, infrastructure, and organizational structure."[19] It is important to note that it takes more than just technical operators to function at the scale and tempo that PRC cyber forces would like to operate.[20] A capable cyber force "requires a more comprehensive workforce" to include intelligence personnel, tool developers, infrastructure maintainers, translators, lawyers, and fire support coordination staff.[21] It also requires experienced human managers to conduct appropriate command and control over global infrastructure, which consists of both servers and endpoints.[22] Therefore, the United States' approach to countering PRC MCA through various legal frameworks must be carefully calibrated to address the diverse array of PRC cyber actors and their specific objectives.[23] This Part provides an overview of the distinct cyber actors operating within the PRC and the objectives that they seek to accomplish.

---

18. *See* U.S. DEP'T OF THE TREASURY, 2024 NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILLICIT FINANCING 8 (2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf [https://perma.cc/55N4-9V34] (explaining AML laws can be tailored to "counter national security threats" by providing "robust information sharing with private sector and international partners … [and] disseminating financial intelligence and information").

19. Max Smeets, *Building a Cyber Force Is Even Harder Than You Thought*, WAR ON THE ROCKS (May 12, 2022), https://warontherocks.com/2022/05/building-a-cyber-force-is-even-harder-than-you-thought/ [https://perma.cc/4NWG-7GTK].

20. *See* John Cobb, C*yber Campaign Plans and Other Fairy Tales*, WAR ON THE ROCKS (Dec. 20, 2024), https://warontherocks.com/2024/12/cyber-campaign-plans-and-other-fairy-tales/ [https://perma.cc/4KDB-7N5M]; Esteban Borges, *What Is the Cyber Kill Chain?*, RECORDED FUTURE (Apr. 19, 2024), https://www.recordedfuture.com/threat-intelligence-101/threat-analysis/cyber-kill-chain [https://perma.cc/86WV-Y6PQ] (describing the multi-disciplinary nature of cyber kill chain framework).

21. Smeets, *supra* note 19.

22. See the 2020 Mueller Report for an example of a foreign intelligence agency managing overseas infrastructure. ROBERT S. MUELLER III, SPECIAL COUNSEL, U.S. DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 40 (Mar. 2019) ("GRU officers accessed the DNC's mail server from a GRU-controlled computer leased inside the United States.").

23. *Cf. Countering Hybrid Threats*, *supra* note 16 (discussing NATO's adoption of a diverse toolset to ensure cybersecurity).

A. PRC Cyber Force Structure

While all PRC-affiliated cyber entities operate under the broad strategic directives of the Communist Party,[24] their individual motivations, capabilities, and vulnerabilities vary significantly.[25] By developing a comprehensive understanding of the PRC cyber actor landscape and carefully crafting targeted legal strategies, the United States can more effectively disrupt and degrade PRC MCA.[26] A nuanced approach that addresses each entity in a discrete manner should permit a proportional response that helps to mitigate the risk of unintended escalation.[27] PRC cyber forces can broadly be broken down into three groups: the People's Liberation Army (PLA), the Ministry of State Security (MSS), and the private sector.[28]

1. The People's Liberation Army

The PRC's military cyber force has undergone several significant restructurings in the last decade, most notably with the recent dissolution of the Strategic Support Force (SSF) in April 2024.[29] The

---

24. For a discussion on the political decision-making process in the PRC, see SUSAN V. LAWRENCE, CONG. RSCH. SERV., IF12505, CHINA PRIMER: CHINA'S POLITICAL SYSTEM (2025).

25. *See* CTR. FOR STRATEGIC & INT'L STUD., *supra* note 1; Christopher Ashley Ford, *Responding to Modern Cyber Threats with Diplomacy and Deterrence*, U.S. DEP'T OF STATE (Oct. 19, 2020), https://2017-2021.state.gov/responding-to-modern-cyber-threats-with-diplomacy-and-deterrence/ [https://perma.cc/T3HF-MCP8].

26. *See generally* Insikt Group, *From Coercion to Invasion: The Theory and Execution of China's Cyber Activity in Cross-Strait Relations*, RECORDED FUTURE (Nov. 23, 2022), https://www.recordedfuture.com/research/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity [https://perma.cc/FD9W-6NSU] (discussing the PRC's cyber goals).

27. *See* BOOZ ALLEN HAMILTON, SAME CLOAK, MORE DAGGER: DECODING HOW THE PEOPLE'S REPUBLIC OF CHINA USES CYBERATTACKS 2, 7, 12, 23, https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html [https://perma.cc/3R7F-ET6F]; *see also* Manshu Xu & Chuanying Lu, *China-U.S. Cyber-Crisis Management*, 3 CHINA INT'L STRATEGY REV. 97, 99 (2021) ("China-U.S. cyber-crisis management [is] the control and handling of cyber incidents that may trigger tensions, armed conflicts and even wars between China and the United States, with the aim of managing the cyberspace differences and reducing the cyber risk that could trigger a deterioration of bilateral relations, or even a full-scale confrontation between the two countries.").

28. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 419.

29. *See* J. Michael Dahm, *A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force*, CHINA BRIEF Apr. 26, 2024, at 15, 16, https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-

SSF, originally established in 2015 by Xi Jinping, had previously consolidated the PLA's cyber, space, electronic, and psychological warfare capabilities under a single command structure to enhance the PLA's operational effectiveness in the information domain.[30]

Less than a decade later, Xi Jinping "reassigned [the SSF's] subordinate forces, the Aerospace Force and the Cyberspace Force, directly under the Central Military Commission ... [and] added a new Information Support Force."[31] The restructuring may reflect the PLA's renewed drive to achieve "the best possible network and communication systems management to enable the successful prosecution of high-end warfare against the most capable opponent(s)."[32] The Cyberspace Force will retain primacy over offensive and defensive cyber operations, while the ISF will "manage network information systems [and] communications support."[33]

Some national security pundits have suggested that the Chairman of the Central Military Commission, Xi Jinping, would not have taken the dramatic step of directly subordinating the Cyberspace Force under the Central Military Commission if the unit was meeting or surpassing expectations under the SSF construct.[34] This

---

support-force/ [https://perma.cc/K5J3-P7QF].

30. John Costello & Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, *in* CHAIRMAN XI REMAKES THE PLA: ASSESSING CHINESE MILITARY REFORMS 437, 437-38 (Phillip C. Saunders et al. eds., 2019).

31. Andrew Erickson, *What the Pentagon's New Report on Chinese Military Power Reveals About Capabilities, Context, and Consequences*, WAR ON THE ROCKS (Dec. 19, 2024), https://warontherocks.com/2024/12/what-the-pentagons-new-report-on-chinese-military-power-reveals-about-capabilities-context-and-consequences/ [https://perma.cc/356N-RA42].

32. *Id.*

33. Ashu Maan, *A Shift in Command: The Restructuring of China's Strategic Support Force*, CTR. FOR LAND WARFARE STUD. (May 7, 2024), https://web.archive.org/web/20240721072050/https://www.claws.in/a-shift-in-command-the-restructuring-of-chinas-strategic-support-force/ [https://perma.cc/5F6P-WTY5]; *see also* Colin Clark, *China Creates New Information Support Force, Scraps Strategic Support Force in 'Major' Shakeup*, BREAKING DEF. (Apr. 22, 2024, at 12:25 ET), https://breakingdefense.com/2024/04/in-major-shakeup-china-creates-new-information-support-force-scraps-strategic-support-force/ [https://perma.cc/6AMN-MXRB].

34. Matt Bruzzese & Peter W. Singer, *Farewell to China's Strategic Support Force. Let's Meet Its Replacements*, DEF. ONE (Apr. 28, 2024), https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/ [https://perma.cc/S83Z-33WM] ("[I]t suggests that the PLA's much-heralded reforms of 2015, which were meant to turn it into a modern joint force, have not been smooth sailing."); *see also* Gordon Arthur, *China Dissolves Strategic Support Force, Focused on Cyber and Space*, DEF. NEWS (Apr. 23, 2024), https://www.defensenews.com/global/asia-pacific/2024/04/23/china-

shift may indicate some level of dissatisfaction with the SSF's ability to address the complex demands of modern cyber warfare under its previous structure.[35] The reorganization underscores the PRC's strategic emphasis on information dominance as a critical component of its military doctrine.[36] The restructuring seeks to streamline command and control processes and enhance its ability to conduct coordinated cyber operations across multiple theater commands.[37]

2. PRC Intelligence Agencies

The PRC's principal civilian intelligence agency, the Ministry of State Security (MSS), plays a pivotal role in advancing the PRC's strategic objectives through cyber operations. The MSS focuses primarily on espionage, to include intellectual property theft and the acquisition of sensitive political and economic data from foreign entities.[38] The MSS's overarching goal is to enhance the PRC's national security by leveraging cyber capabilities to undermine

---

dissolves-strategic-support-force-focused-on-cyber-and-space/ [https://perma.cc/GX3C-SML2].

35. *See* Maan, *supra* note 33 ("Similarly, the SSF commander General Ju Qiansheng had been missing since 2023 leading to speculation of corruption in SSF akin to the Rocket Force. The SSF had become a bloated organisation due to the integration of various departments and coupled with intensive investment it needed due to being technical in nature may have served as a motivation for corruption.").

36. *See id.*

37. *See* Ying Yu Lin & Tzu-Hao Liao, *RIP, SSF: Unpacking the PLA's Latest Restructuring*, DIPLOMAT (Apr. 23, 2024), https://thediplomat.com/2024/04/rip-ssf-unpacking-the-plas-latest-restructuring/ [https://perma.cc/UZ8B-LDD5] ("[T]his restructuring aims to enhance the PLA's capabilities in an era increasingly defined by information warfare and cyber operations.").

38. *See, e.g.*, *IP and Strategic Competition with China: Part III - IP Theft, Cybersecurity, and AI: Hearing Before the Subcomm. on Cts., Intell. Prop., & the Internet of the H. Comm. on the Judiciary*, 118th Cong. 33 (2023) [hereinafter *IP and Strategic Competition Hearing*] (statement of Dr. Benjamin Jensen, Senior Fellow, Int'l Sec. Program, Ctr. for Strategic & Int'l Stud.); *see also* GREG AUSTIN, KAI LIN TAY & MUNISH SHARMA, GREAT-POWER OFFENSIVE CYBER CAMPAIGNS: EXPERIMENTS IN STRATEGY 72, 85-86 (2022), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/02/great-power-offensive-cyber-campaigns_04-china.pdf [https://perma.cc/BU8D-UZ4L]. The Ministry of Public Security (MPS) also conducts cyber operations with a primary focus on ensuring domestic political stability and centralizing control in the Communist Party. *See* Matthew Brazil, *Foreign Intelligence Hackers and Their Place in the PRC Intelligence Community*, JAMESTOWN FOUND.: CHINA BRIEF, Mar. 29, 2024, at 6, 8, https://jamestown.org/program/foreign-intelligence-hackers-and-their-place-in-the-prc-intelligence-community/ [https://perma.cc/6C9R-F44U].

adversaries and secure technological and economic advantages for the state.[39] Like the PLA, the MSS relies on a complex mix of domestic personnel and a global network of infrastructure.[40] The U.S. and its allies can most effectively employ lawfare tools by systematically targeting the supporting infrastructure that enables PRC cyber operations, to include disrupting command-and-control nodes, severing illicit funding streams, and deterring contractor collaboration, rather than exclusively targeting individual operators.[41]

In addition to state-managed cyber operations conducted by government employees, the MSS increasingly relies on private contractors to execute state-sponsored cyber activities.[42] These

39. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 419, 446-52 ("China's premier spy agency, the Ministry of State Security (MSS), conducts most global cyberespionage operations and targets political, economic, and personally identifiable information to achieve China's strategic objectives."); *see also China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States: Hearing Before the U.S.-China Econ. & Sec. Rev. Comm'n*, 117th Cong. (2022) [hereinafter *China's Cyber Capabilities Hearing*] (statement of Adam Kozy, CEO & Founder, SinaCyber), https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf [https://perma.cc/U9EJ-VK6C] ("[T]he MSS has an advantage of being able to co-opt talent if they wish, especially if an individual's cyber activities conducted during their youth fall under criminal activity."); Chris Buckley & Adam Goldman, *How China's Secretive Spy Agency Became a Cyber Powerhouse*, N.Y. TIMES (Sep. 28, 2025), https://www.nytimes.com/2025/09/28/world/asia/how-chinas-secretive-spy-agency-became-a-cyber-powerhouse.html [https://perma.cc/DNM5-V4J7] ("American and European officials say China's Ministry of State Security, the civilian spy agency often called the M.S.S., in particular, has emerged as the driving force behind China's most sophisticated cyber operations.").

40. *See* AJ Bakari, *Ministry of State Security: China's Intel Machine in High Gear*, GREY DYNAMICS (Feb. 22, 2025), https://greydynamics.com/ministry-of-state-security-chinas-intel-machine-in-high-gear/ [https://perma.cc/Z8G6-MXSL] (explaining the recruitment process for MSS personnel); *see also China's Cyber Capabilities Hearing*, *supra* note 39, at 96 (statement of Adam Kozy, CEO & Founder, SinaCyber) ("[A] candidate who had already been approached by PLA recruiters was enticed to the MSS due to an easier recruitment process, better pay/benefits, and more freedom as non enlisted.").

41. *See generally* U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA (2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF [https://perma.cc/ND2L-N66M] (noting the PRC's extensive cyber capability and the potential value of disrupting it).

42. *See, e.g.*, Press Release, U.S. Dep't of the Treasury, Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure (Mar. 25, 2024), https://home.treasury.gov/news/press-releases/jy2205 [https://perma.cc/UMH3-D34U]; China's Cyber Capabilities Hearing, *supra* note 39, at 89 (statement of Adam Kozy, CEO & Founder, SinaCyber) ("The MSS's model of using a combination of in-house talent and cyber contractors has won the [Chinese Communist Party's] favor for engaging in economic-driven cyber espionage.").

contractors, often cybersecurity firms or independent freelancers, provide the MSS with "plausible deniability" while expanding its operational capacity.[43] A tailored AML response that targets the MSS's unique vulnerabilities, often arising from its comparatively heavy utilization of private-sector proxies, would enhance U.S. efforts to counter Chinese cyber operations.[44]

3. Private Sector Cyber Entities

The PRC has increasingly turned to private contractors to bolster its offensive cyber capabilities.[45] Both the PLA and MSS leverage a complex ecosystem of universities, private firms, and state-aligned actors to achieve strategic objectives.[46] These entities provide zero-days, command and control software, surveillance technologies, and most importantly, human capital.[47] Some of these organizations also directly conduct cyber operations targeting foreign governments, critical infrastructure, and other private sector entities.[48]

---

43. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 453.

44. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CHINESE MINISTRY OF STATE SECURITY-AFFILIATED CYBER THREAT ACTOR ACTIVITY 2 (2020), https://www.cisa.gov/sites/default/files/publications/AA20-258A-Chinese_Ministry_of_State_Security-Affiliated_Cyber_Threat_Actor_Activity_S508C.pdf [https://perma.cc/R47Y-KAS3]; *see also* Matt Brazil & Peter W. Singer, *China Is Turning to Private Firms for Offensive Cyber Operations*, DEF. ONE (June 30, 2024), https://www.defenseone.com/threats/2024/06/china-turning-private-firms-offensive-cyber-operations/397767/ [https://perma.cc/P4D7-KUMK] ("[T]he transfer of what appears to be a substantial portion of work from state security agencies to contractors.").

45. *See* Brazil & Singer, *supra* note 44.

46. COLINE CHAVANE, A THREE-BEAT WALTZ: THE ECOSYSTEM BEHIND CHINESE STATE-SPONSORED CYBER THREATS 30-33 (2024), https://blog.sekoia.io/wp-content/uploads/2024/11/A-three-beat-waltz-The-ecosystem-behind-Chinese-state-sponsored-cyber-threats.pdf [https://perma.cc/JWV3-XUQP]. Companies such as i-Soon (Shanghai Anxun Information Company) and Chengdu 404 exemplify this trend of private contractors operating on behalf of PRC intelligence agencies. *See* Akshaya Asokan, *iSoon Leak Shows Links to Chinese APT Groups*, BANKINFOSECURITY (Mar. 26, 2024), https://www.bankinfosecurity.com/isoon-leak-shows-links-to-chinese-apt-groups-a-24713 [https://perma.cc/6TA6-GR9X]; *see also Shadow Ops Exposed: Inside the Leak of China's i-Soon Cyber Espionage Empire*, SOCRADAR (Feb. 22, 2024), https://socradar.io/shadow-ops-exposed-inside-the-leak-of-chinas-i-soon-cyber-espionage-empire/ [https://perma.cc/B2UP-BURZ].

47. *See* Tom Uren, *How China's Cyber Ecosystem Feeds Off Its Superstar Hackers*, LAWFARE (June 14, 2024, at 08:00 ET), https://www.lawfaremedia.org/article/how-china-s-cyber-ecosystem-feeds-off-its-superstar-hackers [https://perma.cc/EWD8-529G].

48. *See* Press Release, U.S. Dep't of Treasury, Treasury Sanctions Cybersecurity Company Involved in Compromise of Firewall Products and Attempted Ransomware Attacks (Dec. 10,

State-sponsored cyber activities conducted by contractors differ slightly from civilian efforts in both structure and intent. PRC contractors often receive direct tasking from PRC government agents to either exploit specific vulnerabilities or conduct Computer Network Exploitation (CNE) against specific targets.[49] In contrast, ad hoc actors often act independently but within parameters that align with state interests.[50] While official government employees or contractors are tasked with advancing explicit state goals like espionage or intellectual property theft, civilians working on an ad hoc basis may also engage in opportunistic attacks for personal gain so long as they avoid actions that would provoke a crackdown by the state.[51]

The PRC's reliance on private contractors offers several advantages, such as plausible deniability for state-sponsored cyber activities and the ability to scale operations rapidly by tapping into

---

2024), https://home.treasury.gov/news/press-releases/jy2742 [https://perma.cc/2KLP-9XGY]; DEP'T OF JUST., PEOPLE'S REPUBLIC OF CHINA-LINKED ACTORS COMPROMISE ROUTERS AND IOT DEVICES FOR BOTNET OPERATIONS 1-2 (2024), https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF [https://perma.cc/U8RV-EY3U].

49. *See* CHAVANE, *supra* note 46, at 30-32. Recently, Sichuan Silence Information Technology was sanctioned for managing botnets that hijacked hundreds of thousands of devices globally to support PRC espionage campaigns. U.S. Dep't of the Treasury, *supra* note 48. Similarly, Integrity Technology Group facilitated malware distribution networks that enabled large-scale data exfiltration from foreign entities. U.S. DEP'T OF JUST., *supra* note 48.

50. For instance, many groups within the Russian cybercrime community are best categorized as ad hoc actors that operate under certain operational norms such as the "[n]umber [o]ne [r]ule" on Russian cybercrime forums: "Never offer to hack or sell data stolen from Russian entities or citizens." Brian Krebs, *Hacker in Snowflake Extortions May Be a U.S. Soldier*, KREBS ON SECURITY (Nov. 26, 2024), https://krebsonsecurity.com/2024/11/hacker-in-snowflake-extortions-may-be-a-u-s-soldier/ [https://perma.cc/U8KC-MF4L].

51. *See China's Cyber Capabilities Hearing*, *supra* note 39, at 98 (statement of Adam Kozy, CEO & Founder, SinaCyber) ("Immunity in this case is much more likely to represent the MSS and MPS turning a blind eye to these criminal activities rather than providing lifelong immunity. This makes the relationship between blackhat contractors and the MSS a tenuous one, based mostly on those criminals conducting their activities outside of China to prevent a conflict of interest where the MSS and MPS need to protect Chinese citizens from their own operators."); *see also Eight Rules for "Civilian Hackers" During War, and Four Obligations for States to Restrain Them*, INT'L COMM. OF THE RED CROSS (Aug. 2, 2024), https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them [https://perma.cc/3Q8V-3TJH] (demonstrating the additional legal complexities "[i]f civilian hackers act under the instruction, direction or control of a State").

the competitive cybersecurity market.[52] These contractors often operate under the guise of legitimate businesses selling defensive cybersecurity software or services but are deeply embedded in the PRC's broader cyber espionage ecosystem.[53] Moreover, various national security laws can be invoked by the PRC to compel private firms to disclose software vulnerabilities or install backdoors in their products that are sold worldwide.[54]

Although this contractor-driven model may enable enhanced operational effectiveness, it may also generate heightened exposure to AML laws. Some of these firms engage in ancillary cybercrime, often in the form of ransomware attacks, to generate illicit financial flows that could be targeted by AML enforcement mechanisms.[55]

---

52. *See* JAKOB BUND, HAND AND GLOVE: HOW AUTHORITARIAN CYBER OPERATIONS LEVERAGE NON-STATE CAPABILITIES 5-7 (2025), https://www.swp-berlin.org/publications/products/comments/2025C30_AuthoritarianCyberOperations.pdf [https://perma.cc/4MHY-96RV]. For more on why states often choose not to confirm or deny cyber operations, see Joseph M. Brown & Tanisha M. Fazal, *#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations*, 6 EUR. J. INT'L SEC. 401, 407, 409-12, 415 (2021).

53. As an example, i-Soon's leaked internal documents revealed numerous contracts with Chinese government agencies and its role as a subcontractor conducting CNE in a quasi-independent manner rather than merely selling a vulnerability to the PRC. *See* Brian Krebs, *New Leak Shows the Business Side of China's APT Menace*, KREBS ON SECURITY (Feb. 22, 2024), https://krebsonsecurity.com/2024/02/new-leak-shows-business-side-of-chinas-apt-menace [https://perma.cc/EZL2-S2A4]; SOCRADAR, *supra* note 46. This stands in subtle contrast to the United States, where "the government may purchase vulnerabilities to use on an offensive mission[,]" but "does not hire firms to conduct specific offensive operations"; whereas, "[i]n China, the government may hire teams for both offensive and defensive work, including offensive hacking operations." Simon Handler, *The 5x5—China's Cyber Operations*, THE ATL. COUNCIL (Jan. 30, 2023), https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations [https://perma.cc/ES5B-R74A] (quoting Dakota Cary). *See also* Charles W. Mahoney, *Corporate Hackers: Outsourcing US Cyber Capabilities*, 15 STRATEGIC STUD. Q., Spring 2021, at 61, 66-67, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-1/Mahoney.pdf [https://perma.cc/8G2K-JMWY].

54. *See* U.S. DEP'T OF HOMELAND SEC., DATA SECURITY BUSINESS ADVISORY 6 (2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf [https://perma.cc/YRL9-LPRA]; *see also* NATIONAL COUNTERINTELLIGENCE AND SEC. CTR., SAFEGUARDING OUR FUTURE (2023), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf [https://perma.cc/DEG7-5AWS].

55. *See* U.S. Dep't of the Treasury, *supra* note 48 (identifying ransomware from "a Chengdu-based cybersecurity government contractor whose core clients are PRC intelligence services"); *see also* Press Release, Matthew Miller, Dep't Spokesperson, U.S. Dep't of State, Sanctioning PRC Cyber Company Involved in Malicious Botnet Operations, (Jan. 3, 2025) https://2021-2025.state.gov/sanctioning-prc-cyber-company-involved-in-malicious-botnet-operations/ [https://perma.cc/UW3Q-YC93] (indicating that a private PRC company managed

Targeting the supporting infrastructure that underpins these organizations and their operations through AML laws could effectively disrupt their ability to sustain their operations.[56]

B. PRC Cyber Objectives

These PRC cyber forces seek to deliver the following strategic objectives: (1) intelligence collection, (2) overseas strategic prepositioning, (3) economic espionage, and (4) narrative control on sensitive topics. Individual actors also seek personal monetary gain. Better understanding the different objectives that the PRC seeks to achieve through MCA will enable authorities to precisely target the financial networks that support PRC-affiliated cyber actors.[57]

1. Intelligence Collection

The PRC has engaged in a systematic cyber campaign focused on intelligence collection as part of the nation's broader strategic goals.[58] Benjamin Jensen, a senior fellow at the Center for Strategic and International Studies, noted that "a network of operatives linked to the [Chinese Community Party] wage[s] a systematic cyber

---

a botnet used to "target[] multiple U.S. and foreign corporations, universities, government agencies, telecommunications providers, and media organizations").

56. *See* FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM NATIONAL PRIORITIES (June 30, 2021), https://www.occ.treas.gov/news-issuances/bulletins/2021/bulletin-2021-29b.pdf [https://perma.cc/6D8S-SC4Q].

57. *See, e.g.*, Press Release, Dep't of Treasury, U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia (Oct. 14, 2025), https://home.treasury.gov/news/press-releases/sb0278 [https://perma.cc/2JWF-6YUW].

58. PRC leadership believes that not conducting offensive cyber operations would place its "modern intelligence collection organizations at a strategic disadvantage; by not participating, [the PRC] would inevitably miss out on intelligence that is difficult if not impossible to collect using existing traditional means." Lester Godefrey, *Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests*, STUD. INTELLIGENCE, Mar. 2022, at 1, 1, 5. The PRC has sought to conduct "economic espionage while claiming not to renege on the [2015] Xi-Obama agreement" and arguing that "directives like 'Made in China 2025' are for national benefit, rather than the private financial benefit of commerce." *Id.* at 5; *see also* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 418 ("Under General Secretary of the Chinese Communist Party (CCP) Xi Jinping, the country's leaders have consistently expressed their intention to become a 'cyber superpower.'").

espionage campaign designed to gain an intelligence advantage."[59] For instance, the 2015 hack of the U.S. Office of Personnel Management, attributed to PRC forces, compromised the sensitive personal information of approximately 21.5 million individuals, including federal employees and contractors with security clearances.[60] A decade later, PRC forces "may have stolen information from nearly every American" while targeting global telecommunication networks.[61] A laundry list of similar campaigns demonstrates the PRC's commitment to using cyber operations as a tool for strategic intelligence collection to bolster its economic and military capabilities and enhance its global influence.[62]

2. Strategic Pre-Positioning in Anticipation of Kinetic Conflict

The PRC has been actively engaged in cyber pre-positioning efforts in order to establish a strategic advantage in any future conflict.[63] The 2024 ODNI Annual Threat Assessment stated that "PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber attacks against infrastructure."[64] CISA further reported that a "PRC state-sponsored cyber group" engaged in a "pattern of behavior [that] is not consistent with traditional cyber espionage or intelligence gathering operations."[65]

---

59. *IP and Strategic Competition Hearing*, *supra* note 38, at 37 (statement of Dr. Benjamin Jensen, Senior Fellow, Int'l Sec. Program, Ctr. for Strategic & Int'l Studs.).

60. *See* Keith Wagstaff, James Eng & Matthew DeLuca, *OPM: 21.5 Million People Affected by Background Check Breach*, NBC NEWS (July 9, 2015, at 17:12 PT), https://www.nbcnews.com/tech/security/opm-hack-security-breach-n389476 [https://perma.cc/QK4H-6243]. This breach underscores the PRC's ability to infiltrate critical U.S. government databases and highlights the strategic value of such intelligence for future espionage and counterintelligence operations.

61. Adam Goldman, *'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American*, N.Y. TIMES (Sep. 4, 2025), https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html [https://perma.cc/XST9-HSCX].

62. *See* ODNI ASSESSMENT, *supra* note 2, at 11-12.

63. *See* Christine Barry, *Volt Typhoon's Future War*, BARRACUDA (Mar. 14, 2024), https://blog.barracuda.com/2024/03/14/volt-typhoon-future-war [https://perma.cc/RPL4-ME29].

64. *See* ODNI ASSESSMENT, *supra* note 2, at 11.

65. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, *supra* note 4. It goes without saying that the Trump administration's drastic cuts to CISA are likely to "exacerbate digital threats to US networks, which are already under daily fire from nation-state spies and cybercrime gangs." Jessica Lyons, *As CISA Braces for More Cuts, Threat Intel Sharing Takes a Hit*, REGISTER (Apr. 8, 2025, at 01:24

U.S. authorities "assess[ed] with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to [Operational Technology] assets to disrupt functions."[66] These efforts underscore the PRC's commitment to leveraging cyber operations as a tool for strategic advantage in the event of conflict.

3. Economic Competition

The PRC has an extensive history of conducting economic espionage through cyber operations focused on acquiring foreign intellectual property (IP). According to the 2024 ODNI Annual Threat Assessment, the PRC "will continue to ... steal trade secrets and IP to bolster China's indigenous [science and technology] sectors."[67] The PRC's systematic cyber espionage campaign is designed to steal intellectual property from the private sector[68] and U.S. research institutions[69] as part of the PRC's "economic development strategy."[70] Recent attention has centered on areas such as artificial intelligence, electrical engineering, and advanced manufacturing, with prior efforts targeting companies in critical industries like aviation and energy.[71]

UTC), https://www.theregister.com/2025/04/08/cisa_cuts_threat_intel/ [https://perma.cc/PTE6-6GX3].

66. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, *supra* note 4. This Note will steer clear of the convoluted Advanced Persistent Threat (APT) naming conventions that largely serve a marketing function for cyber threat intelligence vendors. *See* Jen Easterly & Ciaran Martin, *Call Them What They Are: Time to Fix Cyber Threat Actor Naming*, JUST SEC. (June 12, 2025), https://www.justsecurity.org/114442/cyber-threat-actor-naming/ [https://perma.cc/EL5H-45EN] ("They obscure attribution, mystify the public, and often glamorize dangerous adversaries.").

67. *See* ODNI ASSESSMENT, *supra* note 2, at 12.

68. *See IP and Strategic Competition Hearing*, *supra* note 38, at 38 (statement of Dr. Benjamin Jensen, Senior Fellow, Int'l Sec. Program, Ctr. for Strategic & Int'l Studs.).

69. *See* Indictment at 1-4, United States v. Xu Zewei, No. 23-cr-523 (S.D. Tex. Nov. 2, 2023).

70. Jenna Lifhits, Note, *Sentencing Economic Espionage in an Era of Great Power Competition*, 22 GEO. J.L. & PUB. POL'Y 353, 354 (2024). The PRC has been called the "world's most egregious actor in terms of cyber espionage targeting private firms and linked to stealing intellectual property." *See IP and Strategic Competition Hearing*, *supra* note 38 (statement of Dr. Benjamin Jensen, Senior Fellow, Int'l Sec. Program, Ctr. for Strategic & Int'l Studs.).

71. *See* Nicole Sganga, *Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies*, CBS NEWS (May 4, 2022, at 00:01 ET), https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-

According to a survey of Chief Financial Officers, "[one] in [five] U.S. corporations has had their IP stolen," with small businesses and startups being particularly vulnerable.[72] Furthermore, Benjamin Jensen, a senior fellow at the Center for Strategic & International Studies, has called the duration and scale of the PRC's IP theft "staggering."[73] The PRC's IP theft campaign has also been linked to its now-defunct "Made in China 2025" plan, which aims to promote the PRC's economic development and dominance in key industries.[74] The scale of IP theft by the PRC has even alarmed the Five Eyes intelligence chiefs.[75] Unfortunately, existing countermeasures appear to have not had any meaningful impact.[76]

---

companies/ [https://perma.cc/NMU4-9NFQ]; *Protecting Our Edge: Trade Secrets and the Global AI Arms Race: Hearing Before the Subcomm. on Cts., Intell. Prop., A.I., & the Internet of the H. Comm. on the Judiciary*, 119th Cong. 10 (2025) [hereinafter *Protecting our Edge Hearing*] (statement of Dr. Benjamin Jensen, Dir. & Senior Fellow, Ctr. for Strategic & Int'l Stud. Futures Lab).

72. *See IP and Strategic Competition Hearing*, *supra* note 38, at 38 (statement of Dr. Benjamin Jensen, Senior Fellow, Int'l Sec. Program, Ctr. for Strategic & Int'l Stud.) (citing Eric Rosenbaum, *1 in 5 Corporations Say China Has Stolen Their IP Within the Last Year, CNBC CFO Survey*, CNBC (Mar. 1, 2019), https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-yer-cnbc.html).

73. *Id.*

74. *See* Yudhijit Bhattacharjee, *The Daring Ruse That Exposed China's Campaign to Steal American Secrets*, N.Y. TIMES MAG. (June 15, 2023), https://www.nytimes.com/ 2023/03/07/ magazine/china-spying-intellectual-property.html [https://perma.cc/FJ55-66Y6]; *An Initiative So Feared that China Has Stopped Saying Its Name*, ECONOMIST (Jan. 16, 2025), https://www.economist.com/china/2025/01/16/an-initiative-so-feared-that-china-has-stopped-saying-its-name [https://perma.cc/EXL7-SZN2].

75. *See* Zeba Siddiqui, *Five Eyes Intelligence Chiefs Warn of China's Theft of Intellectual Property*, REUTERS (Oct. 18, 2023, at 09:46 PT), https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/ [https://perma.cc/G2N7-WRV6]. Whether the PRC's IP theft campaign continues at the same pace is an open question due to the PRC's present-day leadership in many critical technologies. *See* Jennifer Wong Leung, Stephan Robin & Danielle Cave, *ASPI's Two-Decade Critical Technology Tracker: The Rewards of Long-Term Research Investment*, Austl. Strat. Pol'y Inst. (Aug. 28, 2024), https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker/ [https://perma.cc/5TDH-3EZ2] ("These new results reveal the stunning shift in research leadership over the past two decades towards large economies in the Indo-Pacific, led by China's exceptional gains. The US led in 60 of 64 technologies in the five years from 2003 to 2007, but in the most recent five years (2019-2023) is leading in seven. China led in just three of 64 technologies in 2003-2007, but is now the lead country in 57 of 64 technologies in 2019-2023.").

76. *See, e.g.*, Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018, at 09:00 ET), https://www.lawfaremedia.org/article/failure-united-states-chinese-hacking-indictment-strategy [https://perma.cc/TTS2-ZQX7] ("[I]t is hard not to conclude that the Justice

4. Public Opinion Warfare

The PRC has also leveraged cyber capabilities as a key instrument in conducting public opinion warfare, both domestically and abroad, as it aims to shape global narratives and suppress dissent.[77] Beijing's information operations focus on promoting pro-PRC narratives, countering criticism of its policies, and undermining the credibility of foreign governments by exploiting digital platforms to disseminate propaganda and disinformation.[78] Domestically, these efforts are reinforced by an extensive surveillance apparatus that monitors online activity and censors dissenting voices, as the PRC "leads the world in applying" advanced technologies "to monitor its population and repress dissent."[79] The PRC employs its cyber capabilities to target a range of specific regions and groups as part of its information warfare strategy to suppress dissent domestically and advance its geopolitical objectives abroad.[80] On a global scale, the PRC seeks to manipulate international public opinion by

Department's deterrence-by-indictment efforts have failed.").

77. Public Opinion Warfare, also referred to as Information Warfare, is one of the pillars of the PRC's "three warfares" theory. Dean Cheng, *How China Has Integrated Its Space Program into Its Broader Foreign Policy*, CHINA AEROSPACE STUD. INST. (2020), https://www.airuniversity.af.edu/Portals/10/CASI/Conference-2020/CASI%20Conference%20China%20Space%20and%20Foreign%20Policy-%20Cheng.pdf [https://perma.cc/6UJM-9Q6U].

78. *See* ODNI ASSESSMENT, *supra* note 2, at 12.

79. *See id.* at 11.

80. Within its borders, the PRC targets minority groups such as the Uyghurs, using cyber tools to monitor, intimidate, and disrupt their advocacy efforts both domestically and in exile communities. *See PRC Efforts to Manipulate Global Public Opinion on Xinjiang*, U.S. DEP'T OF STATE (Aug. 24, 2022), https://2021-2025.state.gov/prc-efforts-to-maintain-global-public-opinion-on-xinjiang/ [https://perma.cc/K7BT-VAU3]. For a deep dive into the technical tools involved in "enabling the repression of the Uighur population in Xinjiang, China," see George T. Papademetriou, Note, *Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry*, 36 HARV. HUM. RTS. J. 191, 210-11 (2023). The PRC also targets Tibetans. For details on the surveillance of the populace in Tibet, see William Yang, *Report: Government-Linked Hackers in China Target Exiled Tibetan Leaders*, VOA (Apr. 18, 2024, at 11:46 ET), https://www.voanews.com/a/report-government-linked-hackers-in-china-target-exiled-tibetan-leaders/7575410.html [https://perma.cc/2J9H-S6EA]. Regionally, Taiwan is a key focus of PRC cyber operations, with campaigns designed to undermine democratic institutions, gather intelligence, and promote unification narratives favorable to Beijing. *See* Enescan Lorci, *The Nexus of Cybersecurity and National Security: Taiwan's Imperatives Amidst Escalating Cyber Threats*, 9 GLOBAL TAIWAN BRIEF, no. 6, 2024, at 9, 10 (Mar. 20, 2024).

amplifying pro-PRC narratives while discrediting criticism of its policies, particularly regarding human rights abuses.[81]

Internationally, the PRC employs cyber operations "in conjunction with so-called 'non-cyber' measures" to amplify its messaging, expose or intimidate dissidents, "manipulat[e] an adeversary's perception about the utility of future escalatory actions[,] and potentially undermin[e] its will to act."[82] The PRC "focus[es] on promoting pro-China narratives, refuting U.S.-promoted narratives, and countering U.S. and other countries' policies that threaten Beijing's interests, including China's international image, access to markets, and technological expertise."[83] This strategy is further bolstered by the PRC's export of "[s]urveillance technologies" to authoritarian regimes worldwide, enabling other states to replicate its model of digital control while expanding the PRC's influence in global information governance.[84] These operations have contributed to a global decline in internet freedoms, as authoritarian regimes adopt sophisticated tools for monitoring and manipulating public discourse.[85] By combining domestic censorship with international propaganda campaigns, the PRC seeks not only to ensure domestic regime stability but also to shape a global information environment that aligns with its geopolitical interests.[86]

5. Individual Financial Motivation

Select entities within the PRC cyber ecosystem have occasionally leveraged access gained during cyber operations tasked by the

---

81. *See How the People's Republic of China Seeks to Reshape the Global Information Environment*, U.S. DEP'T OF STATE (Sep. 28, 2023), https://2021-2025.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/ [https://perma.cc/SP5R-LLSE].

82. AUSTIN ET AL., *supra* note 38, at 79, 88; *see also* Siena Anstis, *Regulating Transnational Dissident Cyber Espionage*, 73 INT'L & COMP. L.Q. 259, 264 (2023).

83. ODNI ASSESSMENT, *supra* note 2, at 12.

84. *See* Samuel Woodhams, *China, Africa, and the Private Surveillance Industry*, 21 GEO. J. INT'L AFFS 158, 158 (2020).

85. Owen Reger, *The Rise of Digital Authoritarianism: Impacts on Global Democracy and Human Rights*, YALE REV. INT'L STUD. (Feb. 12, 2025) https://yris.yira.org/column/the-rise-of-digital-authoritarianism-impacts-on-global-democracy-and-human-rights/ [https://perma.cc/R738-J2A4].

86. *See* AUSTIN ET AL., *supra* note 38, at 72-89.

government to secure their own personal enrichment.[87] These actors are often private companies and individuals that engage in "side hustle[s]" to profit from ransomware attacks or cryptocurrency theft.[88] Unlike North Korea, where cybercrime directly funds important state initiatives like its nuclear weapons program,[89] the PRC does not view MCA as a direct regime funding mechanism, but PRC-linked cybercriminals do occasionally engage in independent financial schemes that are not explicitly approved by the government.[90]

In summary, the PRC's strategic objectives cascade down to the tactical level, shaping the incentives and operations of its diverse field of cyber actors.[91] While intelligence collection, intellectual property theft, public opinion manipulation, and strategic pre-positioning remain readily traceable to the PRC's overarching strategy, the individual financial motivations that drive many private PRC cyber entities are less publicized but equally integral to the functioning of the broader ecosystem.[92] This landscape

87. *See* AJ Vicens, *Chinese Hackers Are Increasingly Deploying Ransomware, Researchers Say*, CYBERSCOOP (June 26, 2024), https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/ [https://perma.cc/T3PE-RQSF]. Chinese hackers have been implicated in stealing millions in COVID-19 relief funds from the United States. Sarah Fitzpatrick & Kit Ramgopal, *Hacker Linked to Chinese Government Stole Millions in Covid Benefits, Secret Service Says*, NBC NEWS (Dec. 5, 2022, at 06:30 ET), https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636 [https://perma.cc/C9YG-EASS].

88. Patrick Howell O'Neill, *China's Cyber-Spies Make Money on the Side by Hacking Video Games*, MIT TECH. REV. (Aug. 7, 2019), https://www.technologyreview.com/2019/08/07/133840/chinese-hackers-do-double-duty-operations-for-espionage-and-profit/ [https://perma.cc/WQ8F-3MWB].

89. Doreen Horschig, *How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?*, CTR. FOR STRATEGIC & INT'L STUD. (July 31, 2024), https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions [https://perma.cc/366R-QBX5].

90. Although not explicitly approved by the government, the schemes are frequent enough to create the presumption that the PRC has a high degree of tolerance for them. *See* Andy Greenberg, *Inside a Firewall Vendor's 5-Year War with the Chinese Hackers Hijacking Its Devices*, WIRED (Oct. 31, 2024, at 8:45 ET), https://www.wired.com/story/sophos-chengdu-china-five-year-hacker-war/ [https://perma.cc/7Z2S-B98C] (quoting the Sophos CISO, Ross McKerchar, as stating that "researchers" from Sichuan Silence Information Technology were "not averse to making a bit of money on the side").

91. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 418-19.

92. *See Nation-State Cyber Actors: Helping Cybersecurity Defenders Protect Against and Respond to Nation-State Actors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors [https://perma.cc/VU8S-5YYQ]; Vicens, *supra* note 87; Brazil & Singer, *supra* note 44.

requires a U.S. response that aligns a range of legal tools with the multifaceted objectives of PRC cyber forces.[93] Although existing legal mechanisms have generally targeted official PRC state objectives, the individual financial incentives of PRC cyber actors have largely gone unaddressed.[94] Anti-money laundering laws present an additional avenue to confront this overlooked dimension of the threat.[95]

II. LAWFARE CAPABILITIES TO DISRUPT, DEGRADE, AND DENY PRC MALICIOUS CYBER ACTIVITY[96]

The PRC seeks to utilize its cyber capabilities to implement and export a form of digital authoritarianism that can "surveil, repress, and manipulate domestic and foreign populations."[97] In response, the U.S. government and private companies headquartered in the

---

93. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 14, at 419-20.

94. *See Countering Threats Hearing*, *supra* note 11, at 48 (statement of Dr. Rush Doshi, C.V. Starr Senior Fellow for Asian Stud. & Dir. of the China Strategy Initiative, Couns. on Foreign Rels. & Assistant Professor of Sec. Stud., Georgetown Univ.). *But see U.S. Has Responded to Chinese-Linked Cyber Attacks on Telecoms Firms, Sullivan Says*, REUTERS (Jan. 10, 2025, at 10:45 ET), https://www.reuters.com/technology/cybersecurity/us-has-responded-chinese-linked-cyber-attacks-telecoms-firms-sullivan-says-2025-01-10/ [https://perma.cc/VB46-C4DV] (highlighting recent efforts by the United States to target PRC cyber actors' financial incentives).

95. *See* FIN. CRIMES ENF'T NETWORK, *supra* note 56, at 4-6 (describing how government entities can use anti-money laundering laws to "identify and report" certain cybercrimes).

96. Various outlets emphasize different tactical tasks within the cyber domain. *Compare* Erick D. McCroskey & Charles A. Mock, *Operational Graphics for Cyberspace*, *in* IDA RESEARCH NOTES: CHALLENGES IN CYBERSPACE: STRATEGY AND OPERATIONAL CONCEPTS 13, 14, 20-21 (Inst. for Def. Analyses ed., 2019), https://www.ida.org/-/media/feature/ publications/i/id/ida-research-notes-challenges-in-cyberspace-strategy-and-operational-concepts/ida-rn--operational-graphics-for-cyberspace.ashx [https://perma.cc/D6NQ-6UFY] (defining "block," "contain," "disrupt," "isolate," "neutralize," and other tasks in Table 1), *with* MICHAEL SCHWILLE, JONATHAN WELCH, SCOTT FISHER, THOMAS M. WHITTAKER & CHRISTOPHER PAUL, HANDBOOK FOR TACTICAL OPERATIONS IN THE INFORMATION ENVIRONMENT: ONLINE APPENDIXES 12-13 (2021), https://www.rand.org/content/dam/rand/pubs/tools/TLA700/TLA732-1/RAND_TLA732-1.appendixes.pdf [https://perma.cc/4PGD-S6P7] (defining "disrupt," "degrade," "deny," and other tactical tasks in Table B.1), *and* JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS II-7 (2018), https://irp.fas.org/doddir/dod/jp3_12.pdf [https://perma.cc/UPF3-BGK6] (defining "deny," "degrade," "disrupt," "destroy," and "manipulate"), *and* Bruce Sterling, *Deny, Degrade, Disrupt, Deceive, or Destroy*, WIRED (Apr. 5, 2019, at 07:49 ET), https://www.wired.com/beyond-the-beyond/2019/04/deny-degrade-disrupt-deceive-destroy/ [https://perma.cc/69XP-EHME] (explaining the "5 Ds").

97. Woodhams, *supra* note 84, at 158.

U.S. have employed a range of domestic legal mechanisms to counter MCA originating from the PRC, including criminal prosecutions, targeted sanctions, export controls, investment restrictions, and civil lawsuits.[98] These measures aim to disrupt PRC cyber operations by targeting both state-sponsored actors and private entities that have been tasked with achieving PRC objectives.[99] However, these efforts have so far yielded limited success in deterring PRC MCA.[100] PRC cyber intrusions have only grown over the years, underscoring the need for alternative legal strategies to address this challenge.[101]

A. Criminal Charges

The landmark 2014 indictment of five members of the PLA for cyber espionage targeting U.S. critical infrastructure was a watershed moment for the United States as it began utilizing criminal charges against PRC cyber personnel as part of a "name and shame" campaign.[102] This marked the "first time criminal

98. *See* James Dowd, Gregory Lantier & Thomas Sprankling, *Cyberespionage and Civil Suits*, LAW360 (July 14, 2014, at 10:11 ET), https://www.law360.com/articles/555126/cyberespionage-and-civil-suits [https://perma.cc/Z789-GC2S]; Press Release, Bureau of Indus. & Sec., U.S. Dep't of Com., Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications (Dec. 2, 2024), https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semicondctors-military [https://perma.cc/648A-5QXX]; Press Release, U.S. Dep't of Just., Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians (Mar. 25, 2024), https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived [https://perma.cc/HT8C-R3H2]; U.S. DEP'T OF THE TREASURY, *supra* note 42.

99. *See* Press Release, Dep't of the Treasury, *supra* note 57.

100. *See People's Republic of China Cyber Threat*, *supra* note 16 ("China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."); Goldsmith & Williams, *supra* note 76.

101. *See* OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 11 (2025) ("The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's campaign to preposition access on critical infrastructure for attacks during crisis or conflict ... demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure.").

102. Christian Vasquez, *FBI Has Conducted More Than 30 Disruption Operations in 2024*, CYBERSCOOP (Oct. 30, 2024), https://cyberscoop.com/fbi-ransomware-disruption-infrastructure-cybertalks/ [https://perma.cc/C69B-KU8D] (noting the U.S. government's "name and shame" strategy). *See* Press Release, U.S. Dep't of Just., U.S. Charges Five Chinese

charges [were] filed against known state actors for hacking" and signaled a shift towards using public attribution to deter PRC MCA.[103] In 2018, the DOJ escalated its efforts by indicting three members working for an organization linked to the MSS for conducting a global campaign targeting managed service providers and stealing intellectual property from dozens of countries.[104]

In the years that followed, the Department of Justice's efforts have only expanded. In 2020, four PLA members were indicted for their role in the Equifax data breach, which exposed the sensitive personal information of nearly half of all Americans and highlighted the PRC's focus on large-scale data theft.[105] The following year, four MSS-affiliated individuals were indicted for targeting companies in the healthcare and aviation sectors as part of a global espionage campaign.[106]

The federal government has even gone as far as charging employees of private entities like Chengdu 404 Network Technology and accused them of conducting both state-sponsored espionage and financially motivated cybercrime in the form of ransomware attacks.[107] The stated objectives of these indictments are to expose

---

Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/Y4AR-6F6R]. The PRC has also started publicly attributing MCA to U.S. entities. *See* Connor Jones, *China Names Alleged US Snoops Over Asian Winter Games Attacks*, REGISTER (Apr. 15, 2025, at 18:02 UTC), https://www.theregister.com/2025/04/15/china_nsa_winter_games/ [https://perma.cc/43QL-P5S4]; Tim Starks, *Chinese Cyber Center Points Finger at U.S. Over Alleged Cyberattacks to Steal Trade Secrets*, CYBERSCOOP (Dec. 19, 2024), https://cyberscoop.com/chinese-cyber-center-us-alleged-cyberattacks-trade-secrets/ [https://perma.cc/E4D8-J85K].

103. U.S. Dep't of Just., *supra* note 102.

104. *See Wanted by the FBI: APT 10 Group*, FBI (Dec. 20, 2018), https://www.fbi.gov/wanted/cyber/apt-10-group [https://perma.cc/W9SQ-A8HK].

105. *See* Clare Hymes & Stefan Becket, *Justice Department Charges 4 Members of Chinese Military for Massive Equifax Hack*, CBS NEWS (Feb. 11, 2020, at 9:48 ET), https://www.cbsnews.com/news/equifax-hack-chinese-military-members-charged-department-of-justice/ [https://perma.cc/KYC3-6EQP].

106. *See* Press Release, U.S. Dep't of Just., Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research (July 19, 2021), https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion [https://perma.cc/R8E6-2R4Y].

107. *See* Press Release, U.S. Dep't of Just., Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns

PRC-linked actors, disrupt their operations, and deter future attacks by leveraging public attribution to rally international condemnation.[108] While the U.S. is unlikely to prosecute these individuals in absentia, these efforts underscore the U.S. commitment to holding PRC cyber actors accountable and reinforcing norms of state-sponsored cyber operations.[109]

The United States can file criminal charges against an individual or entity engaged in MCA under the Computer Fraud and Abuse Act (CFAA),[110] the federal wire fraud statute,[111] or the Electronic Communications Privacy Act (an update to the Wiretap Act).[112] The CFAA, which has been the bedrock of federal computer crimes law since 1986, criminalizes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" to obtain

---

Against More Than 100 Victims Globally (Sep. 16, 2020), https://www.justice.gov/archives/opa/pr/seven-international-cyber-defendants-including-apt31-actors-charged-connection-computer [https://perma.cc/FS6D-RNTM]; MANDIANT, APT41: A DUAL ESPIONAGE AND CYBER CRIME OPERATION 3 (2019), https://services.google.com/fh/files/misc/apt41-a-dual-espionage-and-cyber-crime-operation.pdf/ [https://perma.cc/F2JS-ZV8W] ("APT41 carries out an array of financially motivated intrusions, particularly against the video game industry, including ... attempting to deploy ransomware."). Cryptocurrencies like Bitcoin have "made it possible to extort huge ransoms from large companies, hospitals and city governments." Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021, at 05:06 ET), https://www.npr.org/2021/06/01/1004874311/how-bitcoin-has-fueled-ransomware-attacks [https://perma.cc/VQ58-HELP].

108. JON BATEMAN, SCOTT COLLARD, JUNE LEE, ARIEL E. LEVITE, LU CHUANYING, GEORGE PERKOVICH, XU MANSHU & FAN YANG, MANAGING U.S.-CHINA TENSIONS OVER PUBLIC CYBER ATTRIBUTION 15-18 (2022) ("U.S. officials almost always invoke the language of deterrence, cost-imposition, and accountability to explain their use of public attribution.").

109. Unlike their Russian counterparts, who are occasionally arrested while traveling abroad or vacationing in Europe, there are very few documented cases of Chinese nationals working in support of a state-sponsored cyber campaign being arrested and extradited for cyber offenses. *See, e.g.*, Steve LeVine, *The U.S. Is Picking Up Vacationing Russian Hackers*, AXIOS (July 31, 2017), https://www.axios.com/2017/12/15/the-us-is-picking-up-vacationing-russian-hackers-1513304545 [https://perma.cc/D4L6-6QEV]. *But see*, AJ Vicens, *Chinese National Arrested for Operating Proxy Service Linked to Billions in Cybercrime*, CYBERSCOOP (May 29, 2024), https://cyberscoop.com/yunhe-wang-911s5-proxy-arrested/ [https://perma.cc/LJ3S-ZLRM] (noting the arrest of a Chinese cybercriminal outside the PRC). This contrast reflects both the protective environment provided by Chinese authorities and the tendency of Russian cybercriminals to expose themselves to international law enforcement by traveling to popular destinations outside Russia. *Contrast* LeVine, *supra*, *with* Vicens, *supra*, *and* BATEMAN ET AL., *supra* note 108, at 15-16 (illustrating the commonality of international arrests of malicious cyber actors from Russia versus those from the PRC).

110. 18 U.S.C. § 1030.

111. 18 U.S.C. § 1343.

112. 18 U.S.C. §§ 2510-2523.

protected information.[113] The Supreme Court has even weighed in on the phrase "exceeds authorized access" to provide clarity on the criminal ramifications of accessing files or data without permission.[114]

Wire Fraud provides another avenue for prosecuting cybercriminals who devise a "scheme or artifice to defraud".[115] To secure a conviction for wire fraud, prosecutors must prove that the defendant intentionally "devise[d] [a] scheme ... to defraud" and used interstate or foreign "wire, radio, or television communication[s]" in furtherance of that scheme.[116] Wire fraud is particularly valuable in cybercrime cases because it does not require proof of unauthorized computer access, making it applicable to a broader range of fraudulent online activities, such as phishing schemes or fraud by an authorized admin.[117]

Lastly, the Wiretap Act addresses the interception of electronic communications and provides both criminal penalties and civil remedies against individuals who intentionally intercept or use such communications without authorization.[118] The statute has frequently been applied in cases involving spyware or malware that captures private communications from compromised devices.[119] Together, these statutes form a robust legal framework for

---

113. *See* 18 U.S.C. § 1030(a)(2).

114. *See* Van Buren v. United States, 141 S. Ct. 1648, 1657-62 (2021) ("If the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals."); Matthew Hank & Rachel Fendell Satinsky, *Supreme Court Narrows the Scope of Claims Available Under the Computer Fraud and Abuse Act*, LITTLER (June 8, 2021), https://www.littler.com/news-analysis/asap/supreme-court-narrows-scope-claims-available-under-computer-fraud-and-abuse-act [https://perma.cc/SYN4-PLBH].

115. 18 U.S.C. § 1343.

116. 18 U.S.C. § 1343.

117. *See generally* PETER G. BERRIS, CONG. RSCH. SERV., R47557, CYBERCRIME AND THE LAW: PRIMER ON THE COMPUTER FRAUD AND ABUSE ACT AND RELATED STATUTES 36 (2023) ("[A] number of other federal statutes also criminalize fraudulent conduct in the cyber context. For example, one frequently used prosecutorial tool is the federal wire fraud statute."); Zachary Cuttito, *The Human Vulnerability: Spear Phishing and Avenues for Prosecuting It*, SYRACUSE L. REV. LEGAL PULSE (Sep. 26, 2024), https://lawreview.syr.edu/the-human-vulnerability-spear-phishing-and-avenues-for-prosecuting-it/ [https://perma.cc/X432-NRSA] (explaining the required elements of wire fraud in a spear phishing campaign); *Van Buren*, 141 S. Ct. at 1661.

118. 18 U.S.C. §§ 2510-2523; *see* Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205, 211-12 (2018).

119. *See* OFF. OF LEGAL EDUC., *supra* note 6, at 59-88.

prosecuting cybercrimes and enable law enforcement to address a wide spectrum of malicious online activities while adapting to evolving technological threats.

B. Targeted Sanctions

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has taken significant actions to disrupt PRC cyber activities by applying sanctions.[120] The United States employs two principal categories of economic sanctions to address foreign threats: primary sanctions and secondary sanctions.[121] Sanctions are grounded in statutory authorities, such as the International Emergency Economic Powers Act (IEEPA), and are implemented through executive orders and regulations administered by OFAC.[122] IEEPA was enacted in 1977 as a peacetime successor to the Trading with the Enemy Act (TWEA), grants the President broad authority to impose economic sanctions during declared national emergencies.[123] Unlike TWEA, which required a congressionally declared war, IEEPA can be invoked in response to "unusual and extraordinary threats" that originate "in whole or substantial part outside the United States" and pose risks to national security, foreign policy, or the economy.[124] Under IEEPA, the President may block transactions, freeze assets, and restrict imports or exports involving foreign entities or individuals engaged in malicious cyber activities

120. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks (Mar. 5, 2025), https://home.treasury.gov/news/press-releases/sb0042 [https://perma.cc/B45W-J872]; Anniek Bao, *U.S. Blacklists over 50 Chinese Companies in Bid to Curb Beijing's AI, Chip Capabilities*, CNBC (Mar. 26, 2025, at 00:56 ET), https://www.cnbc.com/2025/03/26/us-blacklists-50-chinese-companies-in-bid-to-curb-beijings-ai-chip-capabilities.html [https://perma.cc/99JR-BUYJ].

121. *See Overview of US Sanctions*, WILLKIE COMPLIANCE CONCOURSE, https://complianceconcourse.willkie.com/resources/sanctions-us-overview-of-us-sanctions/ [https://perma.cc/MNB4-WW35].

122. *See* 50 U.S.C. §§ 1701-1707; 31 C.F.R. pts. 500-99.

123. *See* CHRISTOPHER A. CASEY & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 2 (2024), https://www.congress.gov/crs-product/R45618 [https://perma.cc/BF2U-AYBK].

124. 50 U.S.C. §§ 1701-1702 (allowing the President to declare a "national emergency" that enables the President to "prevent … [the] use, transfer, withdrawal, transportation, importation or exportation of … any property in which any foreign country or a national thereof has any interest").

(MCA) that threaten national security.[125] IEEPA allows the president to block and prevent U.S. persons from engaging in transactions with "any property in which any foreign country or a national thereof has any interest."[126] When an entity or person is added to the Specially Designated Nationals and Blocked Persons (SDN) List, all of their property and interests in property within U.S. jurisdiction are frozen, and U.S. persons are broadly prohibited from transacting with them.[127] Civil and criminal penalties for violations are set forth in 31 U.S.C. § 1705, and OFAC's enforcement guidelines.[128]

Secondary sanctions frequently have an extraterritorial effect by deterring non-U.S. persons from engaging in certain activities with sanctioned parties, even absent a direct U.S. nexus due to the threat of U.S. enforcement action or criminal charges.[129] These authorities allow the U.S. government to restrict access to the U.S. financial system or impose SDN designation on non-U.S. persons who facilitate significant transactions with sanctioned actors or sectors, as outlined in statutes such as the Countering America's Adversaries Through Sanctions Act.[130] Recent years have seen a marked increase in the use of both primary and secondary sanctions against Chinese entities, such as those targeted for their involvement in human rights abuses in Xinjiang.[131] The Non-SDN Chinese Military-Industrial Complex Companies list, established under Executive Order 14032, further prohibits U.S. persons from trading in certain securities of designated Chinese firms in the defense and surveillance technology sectors.[132] These measures collectively sever targeted entities from the U.S. marketplace and the broader U.S.-dollar-based financial system.

---

125. *See* CASEY & ELSEA, *supra* note 123, at 2.

126. *See* 50 U.S.C. § 1702(a)(1)(B); *see also, e.g.*, 31 C.F.R. §§ 501.701, 515.201, 560.314.

127. *See* 31 C.F.R. §§ 515.306, 501.603, 594.201.

128. *See* 31 U.S.C. § 1705; 31 C.F.R. pt. 501, app. A.

129. *See*, *e.g.*, Ukraine Freedom Support Act, 22 U.S.C. §§ 8922-8923; 50 U.S.C. § 1701 (highlighting IEEPA extraterritoriality).

130. 22 U.S.C. §§ 9401-9412 (outlining the Act's sanctions as applied to Iran).

131. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Accountability Act (July 9, 2020), https://home.treasury.gov/news/press-releases/sm1055 [https://perma.cc/F2FG-GHSR].

132. *See* Exec. Order No. 14,032, 86 Fed. Reg. 30145 (June 3, 2021); 31 C.F.R. § 586.201.

OFAC has also targeted PRC-linked entities and individuals involved in malicious cyber operations that threaten U.S. national security.[133] For example, in March 2024, OFAC sanctioned "a Wuhan, China-based Ministry of State Security front company[,] along with two affiliated individuals, for a cyber campaign targeting U.S. critical infrastructure and government entities.[134] Similarly, in December 2024, OFAC sanctioned Sichuan Silence Information Technology Company and its employee Guan Tianfeng for deploying malware and ransomware during a 2020 campaign that compromised "tens of thousands of firewalls" globally, including some protecting "U.S. critical infrastructure."[135] These sanctions freeze all U.S.-based assets of the designated entities and individuals and prohibit U.S. persons from engaging in transactions with them, effectively cutting off their access to the global financial system.[136]

Separately, the 2016 Global Magnitsky Act "enables the president to designate and sanction individuals responsible for or aiding in particular human rights abuses or corruption."[137] The associated sanctions prevent an entity from conducting transactions with U.S. entities and freeze their U.S. assets; however, it can be applied only to those who have "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of" targeted entities.[138]

Another sanctions-like tool at the disposal of the federal government is section 311 of the Patriot Act.[139] It allows the Department of the Treasury to cut off financial institutions from the global financial system after various procedural requirements are met.[140]

---

133. *See* Exec. Order No. 13,694, 80 Fed. Reg. 18077 (Apr. 1, 2015).

134. *Recent News from Treasury's Office of Foreign Assets Control: March 28*, ABA BANKING (Mar. 28, 2024), https://bankingjournal.aba.com/2024/03/recent-news-from-treasurys-office-of-foreign-assets-control-march-28/ [https://perma.cc/5J8A-YWWK].

135. U.S. Dep't of the Treasury, *supra* note 48.

136. U.S. sanctions often have extraterritorial effects. *See* 50 U.S.C. §§ 1701-1707; *see also* Jiazhen Guo & Carl A. Valenstein, *Update: US Sanctions on Russia Have Extraterritorial Implications*, MORGAN LEWIS (Mar. 3, 2022), https://www.morganlewis.com/pubs/2022/03/update-us-sanctions-on-russia-have-extraterritorial-implications [https://perma.cc/YH44-LUZ3].

137. Mailyn Fidler, *Zero Progress on Zero-Days: How the Last Ten Years Created the Modern Spyware Market*, 102 NEB. L. REV. 713, 750 (2024).

138. Exec. Order No. 13,818, 82 Fed. Reg. 60839, 60840 (Dec. 20, 2017).

139. *See* 31 U.S.C. § 5318A(a)(1).

140. *See id.*

Special Measure number five of the Patriot Act prohibits domestic financial institutions from maintaining bank accounts on behalf of outside banks.[141] When evaluating legal claims by a sanctioned party, an Article III judge can review classified information ex parte and in camera.[142]

Section 232 of the Trade Expansion Act of 1962 provides the President with complementary authority to impose tariffs and import restrictions based on national security determinations.[143] This provision requires the Department of Commerce to conduct investigations within 270 days to assess whether imports "threaten to impair the national security," after which the President has 90 days to determine appropriate responsive measures.[144] Section 232 investigations can be initiated through self-initiation by the Secretary of Commerce, requests from other government agencies, or petitions from interested parties.[145] The statute deliberately provides no specific definition of "national security," granting the executive branch considerable discretionary authority in making such determinations.[146] While IEEPA targets foreign threats through financial and transactional restrictions, Section 232 addresses national security concerns through trade-based remedies, creating a comprehensive framework for executive economic statecraft in cybersecurity contexts.

Sanctions and AML laws each offer distinct advantages and drawbacks to countering PRC MCA. Sanctions allow the U.S. government to publicly attribute and penalize specific individuals or entities involved in cyber operations, effectively freezing their assets and cutting them off from the global financial system.[147] However, sanctions require constant updating by government employees to remain effective, as cyber actors frequently adapt their

---

141. 31 U.S.C. § 5318A(b)(5).

142. *See* FBME Bank Ltd. v. Lew, 209 F. Supp. 3d 299, 309 (D.D.C. 2016).

143. *See* 19 U.S.C. § 1862; BUREAU OF INDUSTRY AND SEC., DEP'T OF COMMERCE, Section 232 Investigations Program Guide (2007), https://www.bis.doc.gov/index.php/documents/section-232-investigations/86-section-232-booklet/file [https://perma.cc/TH4H-TX6U].

144. 19 U.S.C. § 1862(b)(3)(A).

145. *Id.* at § 1862(b)(1)(A).

146. *See* Scott Lincicome & Inu Manak, *Protectionism or National Security? The Use and Abuse of Section 232*, CATO INST. (Mar. 9, 2021), https://www.cato.org/policy-analysis/protectionism-or-national-security-use-abuse-section-232 [https://perma.cc/U7XK-24YV].

147. *See, e.g.*, U.S. DEP'T OF THE TREASURY, *supra* note 42.

methods and organizational structures to evade restrictions.[148] In contrast, AML laws shift the burden of monitoring suspicious activity onto financial institutions, which are required to implement risk-based compliance programs and report when illicit transactions are detected.[149] This decentralized approach enables a more flexible response to evolving threats, as financial institutions are often better positioned to identify irregularities in real-time.[150] However, AML enforcement can be resource intensive for private organizations and may lead to overcompliance or false positives, which could strain legitimate business activities.[151] While both tools are essential in combating PRC MCA, their effectiveness depends on the nature of the threat and the ability to coordinate enforcement across the public and private sectors.

C. Export Controls

U.S. export controls have historically focused on "restricting the export of certain technologies rather than on stymieing particular bad actors."[152] BIS plays a central role in countering PRC cyber activities through the administration of export controls under the Export Administration Regulations (EAR).[153] BIS utilizes tools such as the Entity List to restrict the export, reexport, or in-country transfer of U.S.-origin goods, software, and technology to entities that pose a threat to U.S. national security or foreign policy

148. *See* Vera Rusinova & Ekaterina Martynova, *Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses*, 57 ISR. L. REV. 135, 174 (2024).

149. *See generally Economic Sanctions and Anti-Money Laundering Developments: 2023 Year in Review*, PAUL WEISS (Jan. 22, 2024), https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/economic-sanctions-and-anti-money-laundering-developments-2023-year-in-review?id=49924 [https://perma.cc/7JGV-WBJY] (noting that AML laws require financial institutions to monitor and report suspicious activity through risk-based programs).

150. *See* Maria A. de Dios, Note, *The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy*, 10 BROOK. J. CORP. FIN. & COM. L. 495, 519 (2016) ("The inherently global nature of these illicit activities has necessitated the implementation of a robust AML compliance regime within financial institutions.").

151. *See* Henry Ogbeide, Mary Elizabeth Thomson, Mustafa Sinan Gonul, Andrew Castairs Pollock, Sanjay Bhowmick & Abdullahi Usman Bello, *The Anti-Money Laundering Risk Assessment: A Probabilistic Approach*, 162 J. BUS. RSCH., July 2023, at 1, 1, 10.

152. *See* Fidler, *supra* note 137, at 716.

153. *See generally* 15 C.F.R. §§ 730-774.

interests.[154] "Companies on the Entity List cannot purchase any item subject to Export Administration Regulations" without a license, thereby cutting off access to critical technologies that could enable PRC MCA.[155] In recent years, BIS has expanded its controls to include cybersecurity tools and intrusion software that could be used for malicious purposes; BIS now requires licenses for exports to countries like the PRC when there is knowledge or reason to believe the items will be used to compromise information systems.[156]

Entities on this list are subject to stringent licensing requirements, with a presumption of denial for most export requests.[157] In May 2024, BIS added thirty-seven PRC entities to the Entity List for their involvement in advancing quantum computing and aerospace programs with military applications, as well as for aiding

---

154. 15 C.F.R. § 744.11; *see also* BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., PRINCIPAL STATUTORY AUTHORITY FOR THE EXPORT ADMINISTRATIVE REGULATIONS 8, 11 (2020), https://www.bis.doc.gov/index.php/documents/regulations-docs/2263-legal-authority-for-the-export-administration-regulations-1/file [https://perma.cc/CWA2-KAZM].

155. *See* Papademetriou, *supra* note 80, at 210; BUREAU OF INDUS. & SEC., *supra* note 154, at 11-14, 16-17. As an example, the Entity List contains the 54th Research Institute of China, a "component of the Chinese military" that was charged with the Equifax hack. Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://www.justice.gov/archives/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking [https://perma.cc/2Z5M-YYT2]; 15 C.F.R. § 744 (Supp. No. 4 2025).

156. This is accomplished by the Foreign-Produced Direct Product Rule's extension of U.S. jurisdiction. 15 C.F.R. § 734.13(a). As an example, "the U.S. placed NSO Group on a Commerce Department blacklist." Michael Silberman, Note, *Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability*, 8 GEO. L. TECH. REV. 245, 263 (2024); *see also* Michael T. Borgia & Melissa Burgess, *Commerce Publishes Export Controls for Cybersecurity Intrusion and Surveillance Tools*, DWT PRIV. & SEC. L. BLOG (Nov. 15, 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/11/commerce-department-cybersecurity-export-controls [https://perma.cc/A8D3-LN97] ("The Interim Final Rule effectively requires licenses for the export, reexport, and in-country transfer of certain 'cybersecurity items' to more than 40 countries, including China and Russia, depending on the specific items, recipients, and anticipated uses.").

157. Export Administration Regulations End-User Controls: Imposition of Restrictions on Certain Persons Identified on the List of Specially Designated Nationals and Blocked Persons (SDN List), 89 Fed. Reg. 20107 (Mar. 21, 2024) (to be codified at 15 C.F.R. pt. 744); *see also* STAFF OF THE H. FOREIGN AFFS. COMM., 118TH CONG., BUREAU OF INDUSTRY & SECURITY: 90-DAY REVIEW REPORT 21 (2023) (Hon. Michael McCaul primary author), https://foreignaffairs.house.gov/wp-content/uploads/2023/12/12.4.23%20BIS%20REPORT--FINALDRAFT.pdf [https://perma.cc/43N7-J5VK].

Russian aggression in Ukraine.[158] The BIS also added two PRC firms in December 2024 for enabling human rights abuses through high-tech surveillance targeting Uyghurs and other minority groups.[159] These measures aim to prevent the transfer of sensitive technologies that could be exploited for MCA or human rights violations.

The Export Control Reform Act of 2018 further strengthened BIS's authority by mandating controls on "emerging and foundational technologies" critical to U.S. national security, including those relevant to cybersecurity and artificial intelligence.[160] These measures have been complemented by BIS's collaboration with international partners under multilateral frameworks like the Wassenaar Arrangement to harmonize export controls on dual-use technologies, such as cyber-surveillance tools.[161] Additionally, BIS has targeted PRC entities involved in military modernization and human rights abuses through its Entity List designations, including firms implicated in surveillance activities against minority groups.[162] These actions demonstrate how export controls serve as proactive tools for degrading PRC cyber capabilities by limiting their access to advanced technologies essential for offensive cyber operations.[163]

---

158. *See* Press Release, Bureau of Indus. & Sec., U.S. Dep't of Com., Commerce Adds 37 PRC Entities to Entity List for Enabling PRC Quantum and Aerospace Programs, Aiding Russian Aggression in Ukraine (May 9, 2024), https://www.bis.gov/press-release/commerce-adds-37-prc-entities-entity-list-enabling-prc-quantum-aerospace-programs-aiding-russian [https://perma.cc/PF7R-REXA].

159. Press Release, U.S. Dep't of Com., Commerce Adds 8 Entities to the Entity List for Enabling Human Rights Abuses (Dec. 10, 2024), https://www.bis.gov/press-release/commerce-adds-8-entities-entity-list-enabling-human-rights-abuses [https://perma.cc/KY2Q-J3HB].

160. *See* 50 U.S.C. § 4817.

161. *See* Borgia & Burgess, *supra* note 156. However, Russia's membership has decreased the utility of this arrangement since its invasion of Ukraine. *See id.*

162. *See* U.S. Dep't of Com., *supra* note 159 ("Of the two PRC entities added, one was added because it enables human rights violations, including high-technology surveillance targeted at the general population of the people of China, Uyghurs, and members of other ethnic and religious minority groups.").

163. The regulatory and oversight structures governing sensitive information in the life sciences, such as the registration and screening of laboratories handling select agents under the Bioterrorism Response Act, might offer a potential model for regulating cybersecurity in the future, as both fields grapple with challenges involving dual-use technologies, relatively low production costs, and the widespread availability of critical information online. *See generally* NAT'L RSCH. COUNCIL (US) COMM. ON RSCH. STANDARDS & PRACS. TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, BIOTECHNOLOGY RESEARCH IN AN AGE OF

D. Investment Restrictions

The United States has recently implemented robust investment controls to prevent U.S. capital from advancing the PRC's cyber and military capabilities. President Biden issued an executive order on August 9, 2023, that declared a national emergency to address the threat posed by PRC advancements in fields deemed critical to national security, such as semiconductors, quantum information technologies, and artificial intelligence.[164] Under this order, the Department of the Treasury, in coordination with the Department of Commerce, finalized the Outbound Investment Rule, which, starting in 2025, prohibits U.S. persons from participating in certain transactions with PRC entities involved in these sectors and requires notification for others.[165] These restrictions aim to sever financial support for PRC companies that contribute to military-civil fusion or cyber operations while closing loopholes that previously allowed U.S. investors to indirectly fund PRC technological advancements.[166] The Outbound Investment Rule also imposes compliance obligations on U.S.-controlled foreign entities, requiring U.S. persons to take "all reasonable steps" to ensure their subsidiaries do not engage in prohibited transactions.[167] The expanded U.S. outbound investment rules now cover passive investments in certain non-U.S. pooled funds likely to invest in sensitive Chinese technology companies, addressing indirect financial flows supporting

---

TERRORISM (2004), https://www.ncbi.nlm.nih.gov/books/NBK222057/ [https://perma.cc/58ZL-D366] (discussing regulatory structures for sensitive life sciences information, which could be a potential model for cybersecurity regulation).

164. Exec. Order No. 14,105, 88 Fed. Reg. 54867 (Aug. 9, 2023).

165. *See* 31 C.F.R. pt. 850 (2025); *Outbound Investment Security Program*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/outbound-investment-program [https://perma.cc/SLZ8-HMTA].

166. *See Final Outbound Investment Rule Released*, DAVIS POLK (Nov. 4, 2024), https://www.davispolk.com/insights/client-update/final-outbound-investment-rule-released [https://perma.cc/J579-BUPH]; *Client Insight: Biden Administration Finalizes Regulations Restricting Outbound U.S. Investment into China*, GUNDERSON DETTMER (Nov. 13, 2024), https://www.gunder.com/en/news-insights/insights/client-insight-biden-administration-finalizes-regulations-restricting-outbound-us-investment-into-china [https://perma.cc/LB3W-PT94].

167. 31 C.F.R. § 850.302; *see U.S. Outbound Investment Regulations to Take Effect on January 2, 2025*, SQUIRE PATTON BOGGS: TRADE PRACTITIONER (Nov. 1, 2024), https://www.tradepractitioner.com/2024/11/u-s-outbound-investment-regulations-to-take-effect-on-january-2-2025/ [https://perma.cc/JXF9-2PAR].

national security risks.[168] Together, these investment controls reflect a growing recognition that U.S. financial flows can indirectly enhance PRC cyber capabilities and underscore the need for comprehensive economic measures to safeguard national security.

E. Research, Data, and Personnel Restrictions

The United States has implemented a range of research, data, and personnel restrictions to unilaterally counter PRC MCA by leveraging legal and regulatory frameworks to limit the flow of sensitive information and expertise. The Export Control Reform Act of 2018 and its subsequent amendments grant BIS the authority to regulate U.S. persons' activities that support foreign military, security, or intelligence services, including those of the PRC, even when no physical export of goods or technology occurs.[169] These restrictions prevent U.S. researchers, engineers, or consultants from providing technical assistance or expertise that could enhance PRC cyber capabilities.[170] Additionally, the Trump administration has threatened U.S. visa restrictions on Chinese students "studying in

168. *See* 31 C.F.R. §§ 850.210(a)(6), 850.303; JAMES H. BARKER, LES P. CARNEGIE, DAMARA L. CHAMBERS, ZACHARY N. EDDINGTON, RUCHI G. GILL, CATHERINE HEIN, RAGAD ALFARAIDY, ASIA Y. CADET, MONICA CALCE, SARA CASTIGLIA, JULIE LEE CHOI, MATTHEW J. CRAWFORD, ELLIOT W. HECHT & CHRISTINE KALPIN, FINAL US OUTBOUND INVESTMENT RULES TO BE EFFECTIVE JANUARY 2, 2025: KEY QUESTIONS ANSWERED 3 (Nov. 8, 2024), https://www.lw.com/en/practices/admin/upload/ SiteAttachments/Final-US-Outbound-Investment-Rules-Effective-January-2025-Key-Questions-Answered.pdf [https://perma.cc/QRA9-SY9E] (noting that the regulation prevents "the acquisition of a limited partner (LP) or equivalent interest in a non-US venture capital fund, private equity fund, fund of funds, or other pooled investment fund if" the transaction involves "persons on certain sanctions- and export controls-related denied persons lists").

169. *See* 50 U.S.C. §§ 4801-4852; Kevin J. Wolf, Shiva Aminian, Anne E. Borkovic, Jingli Jiang, Jaelyn Edwards Judelson, Susan M.C. Kovarovics, Kimberly M. Myers & Thomas Krueger, *BIS Has New Authorities to Impose Controls over Activities of US Persons in Support of Foreign Military, Security, or Intelligence Services*, AKIN (Jan. 5, 2023), https://www.akingump.com/en/insights/alerts/bis-has-new-authorities-to-impose-controls-over-activities-of-us-persons-in-support-of-foreign-military-security-or-intelligence-services [https://perma.cc/C6SU-XXVA].

170. *See, e.g.*, Paul Triolo, *Restrictions on Trade with China Harm U.S. Leadership in Technology*, *in* GETTING CHINA RIGHT AT HOME: ADDRESSING THE DOMESTIC CHALLENGES OF INTENSIFYING COMPETITION 24-28 (Jessica Chen Weiss ed., 2025), https://acf.sais.jhu.edu/assets/files/getting-china-right-at-home.pdf [https://perma.cc/A6B5-KLKM].

'critical fields.'"[171] Conference attendance by Chinese researchers in areas like cybersecurity and artificial intelligence is also increasingly scrutinized by the PRC to prevent the transfer of cutting-edge knowledge that could be exploited for offensive cyber operations.[172] These measures echo longstanding controls in fields like biotechnology and nuclear research, in which strict oversight mechanisms have been employed to prevent dual-use technologies from falling into the hands of adversaries.[173] By restricting access to critical expertise and data, these policies aim to degrade PRC MCA capabilities while safeguarding U.S. technological leadership.

F. Civil Lawsuits

Civil lawsuits provide an additional mechanism for deterring PRC MCA by enabling private entities in the U.S. to seek damages and injunctive relief under statutes like the CFAA, state computer fraud laws, and common law causes of action. The CFAA allows private parties to bring civil claims when unauthorized access to a protected

---

171. *See* Edward Wong, *U.S. Will 'Aggressively' Revoke Visas of Chinese Students, Rubio Says*, N.Y. TIMES (May 28, 2025), https://www.nytimes.com/2025/05/28/us/politics/china-student-visas-revoke.html [https://perma.cc/Z89A-HCBM]. Relatedly, the Biden administration had signaled a tougher stance by threatening visa restrictions on individuals involved in the development or deployment of spyware targeting journalists and dissidents, potentially foreshadowing heightened accountability for state-linked cyber operations. *See* Aamer Madhani & Frank Bajak, *US Rolls Out Visa Restriction Policy on People Who Abuse Spyware To Target Journalists, Activists*, AP NEWS (Feb. 6, 2024, at 02:30 MT), https://apnews.com/article/biden-commercial-spyware-visa-blinken-a725b3f22cc2a9420be4f35af8a78096 [https://perma.cc/EAQ4-Q659].

172. *See* Chris Bing, *China's Government Is Keeping Its Security Researchers from Attending Conferences*, CYBERSCOOP (Mar. 8, 2018), https://cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/ [https://perma.cc/G49E-6TBC]; Yoko Kubota, *China Tells Its AI Leaders to Avoid U.S. Travel Over Security Concerns*, WALL ST. J. (Mar. 1, 2025, at 00:01 ET), https://www.reuters.com/world/china-tells-its-ai-leaders-avoid-us-travel-over-security-concerns-wsj-reports-2025-03-01/ [https://perma.cc/VPX9-F77V] (reporting official instructions for Chinese AI researchers to refrain from travel abroad due to security fears and control of knowledge transfer).

173. *See* CARL STOIBER, ALEC BAER, NORBERT PELZER & WOLFRAM TONHAUSER, HANDBOOK ON NUCLEAR LAW 137-44 (2003), https://www.pub.iaea.org/mtcd/publications/pdf/pub1160_web.pdf [https://perma.cc/H8TU-H2RY]; NAT'L RSCH. COUNCIL (US) COMM. ON RSCH. STANDARDS & PRACS. TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, *supra* note 163.

computer causes at least $5,000 in damage within a one-year period.[174]

In *WhatsApp Inc. v. NSO Group Technologies Ltd.*, the U.S. District Court for the Northern District of California held that NSO Group violated the CFAA by using WhatsApp servers to deploy spyware onto users' devices, with intent demonstrated by NSO Group's redesign of its Pegasus spyware to evade detection after WhatsApp implemented security fixes.[175] Additionally, breach of contract claims have proven effective in cases in which a defendant has violated the terms of a service agreement, such as prohibitions on reverse engineering or decompiling software.[176] In *WhatsApp*, the court presumed that NSO Group agreed to WhatsApp's terms by creating accounts necessary to access its server infrastructure, and therefore violated the agreement when it engaged in command and control of its malware through those servers.[177] State laws like California's Comprehensive Computer Data Access and Fraud Act offer another opportunity for private parties to assert a claim of unauthorized computer access, complementing federal statutes like the CFAA.[178] Common law claims such as invasion of privacy and unjust enrichment also allow plaintiffs to recover damages for interference with their digital property or profits derived from unauthorized access.[179] These legal tools can theoretically enable private parties to hold PRC-linked cyber actors accountable and deter future MCA by raising the financial and reputational costs of cyber intrusions. However, challenges remain in demonstrating harm under statutes like the CFAA, as courts increasingly require

174. *See* 18 U.S.C. § 1030(g).

175. *See* No. 19-cv-07123, 2024 WL 5190365, at *7 (N.D. Cal. Dec. 20, 2024).

176. *See, e.g.*, SAS Inst., Inc. v. World Programming Ltd., 874 F.3d 370, 380-82 (4th Cir. 2017).

177. *See WhatsApp Inc.*, 2024 WL 5190365, at *8; *US Judge Finds Israel's NSO Group Liable for Hacking in WhatsApp Lawsuit*, REUTERS (Dec. 23, 2024, at 15:19 ET), https://www.reuters.com/technology/cybersecurity/us-judge-finds-israels-nso-group-liable-hacking-whatsapp-lawsuit-2024-12-21/ [https://perma.cc/69CD-LJBL].

178. *See WhatsApp Inc.*, 2024 WL 5190365, at *8.

179. *See* Ying Hu, *Mainstreaming Unjust Enrichment and Restitution in Data Security Law*, 13 U.C. IRVINE L. REV. 855, 857 n.2, 859-61 (2023) ("In recent years, an increasing number of unjust enrichment claims concerning data breach have survived motions to dismiss.").

plaintiffs to show tangible technological damage or loss rather than mere data exfiltration.[180]

Bringing a civil suit against PRC cyber actors also presents significant legal and procedural challenges, particularly in establishing jurisdiction, overcoming forum non conveniens defenses, and addressing issues of standing and sovereign immunity. Jurisdiction can be difficult to establish in transnational cybercrime cases, especially if operations are conducted remotely through leased cloud servers or anonymized networks.[181] Additionally, courts may dismiss cases under the doctrine of forum non conveniens if they determine that a foreign court is more appropriate for resolving the dispute, though this requires showing "that an adequate alternative forum exists" and "that 'private' and 'public' interest factors weigh heavily in favor of dismissal."[182] The Alien Tort Statute, which allows noncitizens to bring tort claims for violations of international law, could theoretically provide a basis for claims against PRC-linked entities; however, its application is limited by the Supreme Court's rulings restricting extraterritoriality and requiring a clear nexus to U.S. territory.[183]

Standing also poses a challenge, as plaintiffs must demonstrate a concrete injury that is traceable to the defendant's actions and

---

180. *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1659-1660 (2021); *US Supreme Court Appears to Limit Civil Liability Under the CFAA*, LAW OFFICES OF DONOGHUE & PICKER (Mar. 6, 2023), https://jdbplaw.com/us-supreme-court-appears-to-limit-civil-liability-under-the-cfaa/ [https://perma.cc/A35Q-XTN2].

181. *See* Alexandra Perloff-Gilest, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191, 226 (2018) ("The jurisdictional rules developed for the nineteenth-century world of Westphalian nation-states are in many ways at odds with the network architecture of modern computing and the inherently cross-border character of transnational cyber offenses."); *cf.* Kellen Dwyer, Kim Peretti & Emily Skahill, *How to Fight Foreign Hackers with Civil Litigation*, LAWFARE (May 13, 2022, at 08:01 ET), https://www.lawfaremedia.org/article/how-fight-foreign-hackers-civil-litigation [https://perma.cc/PC6V-JRAH].

182. *Personal Jurisdiction/Forum Non Conveniens—The World in U.S. Courts: Spring 2018*, ORRICK (May 1, 2018), https://www.orrick.com/en/Insights/2018/05/The-World-in-US-Courts-Spring-2018-Personal-Jurisdiction-Forum-Non-Conveniens [https://perma.cc/RB7X-ZWKE].

183. *See* William S. Dodge & Oona A. Hathaway, *Answering the Supreme Court's Call for Guidance on the Alien Tort Statute*, JUST SEC. (June 3, 2022), https://www.justsecurity.org/81730/answering-the-supreme-courts-call-for-guidance-on-the-alien-tort-statute/ [https://perma.cc/4KRX-WBZN].

likely to be redressable by the court.[184] Courts have historically scrutinized claims based on speculative harms, such as the risk of future identity theft following data breaches, making it harder for victims of PRC MCA to establish standing.[185]

Sovereign immunity further complicates litigation against state-linked actors. While the Foreign Sovereign Immunities Act provides exceptions for commercial activities or terrorism-related acts to its general protection of foreign governments from suit in U.S. courts, they may not apply cleanly to cyber operations, leaving victims with limited recourse.[186] Private contractors linked to state-sponsored cyber campaigns may invoke derivative sovereign immunity defenses to evade, or at least complicate, civil litigation.[187]

Finally, attribution remains a significant hurdle in civil litigation against PRC actors. Offensive cyber operations often involve layers of obfuscation, including third-party proxies or contractors, making it difficult to directly link malicious activity to specific entities or countries.[188] The sheer number of PRC-linked organizations engaged in cyber operations, many of which can quickly dissolve and reconstitute under new names or structures, is fed by "an ecosystem

---

184. *See Second Circuit Rules Individuals Have Standing to Sue for 'Increased Risk' of Identity Theft*, COOLEY (Apr. 30, 2021), https://cdp.cooley.com/second-circuit-rules-individuals-have-standing-to-sue-for-increased-risk-of-identity-theft/ [https://perma.cc/JBW9-YBAC].

185. *See id.* ("*McMorris* poses clear hurdles for data breach class actions in the Second Circuit because it will be difficult for plaintiffs to plead sufficient facts showing that the purpose of any given cyberattack was to target *their* data.").

186. *See* Adam L. Silow, Note, *Bubbles Over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability*, 12 J. NAT'L SEC. L. & POL'Y 659, 666-73 (2022).

187. This is suggested in *WhatsApp Inc. v. NSO Group Technologies Ltd.*, where the Ninth Circuit rejected the NSO Group's claim of immunity but highlighted the complexities of litigating against quasi-state actors. 17 F.4th 930, 933, 940 (9th Cir. 2021); *see also* Phineas Rueckert & Karine Pfenniger, *Israel Maneuvered to Prevent Disclosure of State Secrets Amid WhatsApp vs NSO Lawsuit*, FORBIDDEN STORIES (July 25, 2024), https://forbiddenstories.org/actualites_posts/israel-maneuvered-to-prevent-disclosure-of-state-secrets-amid-whatsapp-vs-nso-lawsuit/ [https://perma.cc/Q2EK-TD7X] (highlighting legal maneuvers by NSO Group and the State of Israel "to prevent state secrets from being shared in legal proceedings."). There is an added twist when the U.S. government is a prospective buyer of the same offensive cyber tools that exploit vulnerabilities in software developed by U.S. tech companies. *See* Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. TIMES (Nov. 15, 2022), https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html [https://perma.cc/WFF7-8GLY] (suggesting that a purchase by the U.S. government of these same offensive cyber tools being utilized against U.S. tech companies may have unexpected legal ramifications).

188. *See* Sepich, *supra* note 6.

that includes multiple national-level collegiate and professional hacking competitions."[189] While civil lawsuits have proven effective in disrupting botnets and obtaining injunctive relief against well-known cybercrime collectives,[190] their utility in addressing PRC MCA is likely limited unless they are supported by broader diplomatic and enforcement efforts targeting state-sponsored cyber campaigns.

III. ANTI-MONEY LAUNDERING LAWS: ANOTHER TOOL IN THE TOOLKIT

Utilizing AML laws against PRC cyber threats may help to disrupt the supporting ecosystem that underpins complex cyber operations. Effective offensive cyber operations rely on a web of technical and financial networks to procure vulnerabilities,[191] evade detection,[192] maintain persistence, and, if financially motivated, launder proceeds from the crime.[193] By enforcing AML statutes under 18 U.S.C. §§ 1956-1957, which criminalize money laundering and impose stringent reporting requirements on financial institutions, U.S. officials can target the financial conduits of PRC cyber actors and disrupt their operational capabilities.[194]

---

189. Dakota Cary & Eugenio Benincasa, *Capture the (Red) Flag: An Inside Look into China's Hacking Contest Ecosystem*, ATL. COUNCIL (Oct. 18, 2024), https://www.atlanticcouncil.org/in-depth-research-reports/report/capture-the-red-flag-an-inside-look-into-chinas-hacking-contest-ecosystem/ [https://perma.cc/DW8W-UFEN] (describing how the PRC cyber ecosystem spreads around talent and maintains operational continuity); *see also* Brian Krebs, *Ransomware Gangs and the Name Game Distraction*, KREBS ON SECUTITY (Aug. 5, 2021), https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/ [https://perma.cc/6V8M-4W9J] (describing an example of a ransomware group changing its name and branding to frustrate attribution and law enforcement).

190. *See* Hogan-Burney & Ramsey, *supra* note 10.

191. *See* Matthias Dellago, Andrew C. Simpson & Daniel W. Woods, *Exploit Brokers and Offensive Cyber Operations*, Summer 2022, CYBER DEF. REV. at 31, 32-33.

192. Jose Ignacio Fernandez del Campo Aguado, *Defense Evasion: Advanced Techniques Undermining Cybersecurity*, AQUA (Sep. 8, 2024), https://www.aquasec.com/cloud-native-academy/cloud-attacks/defense-evasion/ [https://perma.cc/8UZW-JFQA].

193. *See* Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SEC. L & POL'Y 595, 610-11 (2016).

194. *See* 18 U.S.C. §§ 1956-1957; *see also* Matthew S. Morgan, *Money Laundering: The American Law and Its Global Influence*, LAW & BUS. REV. AMERICAS, Summer 1997, at 24, 30-36.

Moreover, AML actions conducted in cooperation with international partners are likely to enable a wider net to be cast and improve global standards for financial transparency.[195] This international dimension is crucial given the PRC cyber forces' targeting of a multitude of foreign governments, corporations, and individuals.[196] AML laws can enable U.S. authorities, in collaboration with international partners, to track and dismantle the financial networks that sustain PRC-sponsored cyber activities.[197] By harnessing the investigative and regulatory tools provided by AML statutes, U.S. authorities can improve national security by tamping down on the financial dimensions of PRC MCA.[198]

A. Historical Flexibility of Domestic AML Laws

The history of AML laws in the United States demonstrates frequent evolution to address emerging threats. The Currency and Foreign Transactions Reporting Act of 1970, commonly referred to as the Bank Secrecy Act (BSA), was the first major legislative effort.[199] It required financial institutions to maintain records and "report cash transactions over $10,000 using the Currency Transaction Report," laying the groundwork for modern AML frameworks.[200]

Since 1970, a multitude of new AML laws have been constructed to combat new threats. The Money Laundering Control Act of 1986 built upon the BSA by criminalizing money laundering itself and introducing civil forfeiture for assets tied to illicit financial

195. *See* KATHRYN JUDGE & ANIL K. KASHYAP, ANTI-MONEY LAUNDERING: OPPORTUNITIES FOR IMPROVEMENT 23-24 (2024).

196. *See* ODNI ASSESSMENT, *supra* note 2, at 11.

197. *See U.S. Takes Action to Further Disrupt PRC Cyber Activities*, U.S. DEP'T OF STATE (Mar. 25, 2024), https://2021-2025.gov/u-s-takes-action-to-further-disrupt-prc-cyber-activities/ [https://perma.cc/2SRB-FPD2].

198. *See generally* Edoardo Saravalle, Note, *Recasting Sanctions and Anti-Money Laundering: From National Security to Unilateral Financial Regulation*, 2022 COLUM. BUS. L. REV. 550, 588-93 (2022) (explaining that U.S. sanctions and AML operate as powerful extra-territorial regulatory tools whose effectiveness depends on regulatory capacity and political will).

199. *See History of Anti-Money Laundering Laws*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws [https://perma.cc/NN9N-NVGE] (indicating that the BSA was the first major AML legislative effort in the United States).

200. *Id.*

activities,[201] a tool that could be applied to disrupt PRC-linked financial networks supporting MCA.

The Annunzio-Wylie AML Act of 1992 "strengthened the sanctions for BSA violations" and introduced safe harbor provisions for financial institutions reporting suspicious activities,[202] incentivizing private sector cooperation to help identify funds used in illicit activity such as PRC MCA.

In the wake of 9/11, the USA PATRIOT Act of 2001 expanded AML requirements for financial institutions by prohibiting them from "engaging in business with foreign shell banks" and "criminaliz[ing] the financing of terrorism," both of which reflected the growing recognition of financial networks as enablers of national security threats.[203]

The most recent statutory AML update, the Anti-Money Laundering Act of 2020 (AMLA), attempted to modernize the BSA by requiring disclosure of beneficial ownership information through the Corporate Transparency Act,[204] a provision that could be particularly relevant for identifying shell companies supplying private servers located in the U.S. that support PRC MCA. Collectively, these demonstrate how the U.S. AML framework has been continuously adapted over time to meet the needs of new challenges.[205] By targeting financial flows linked to MCA, AML laws may provide an additional mechanism to disrupt PRC cyber actors who rely on laundering illicit funds through global financial systems.

---

201. *See id.*

202. *See id.*; 31 U.S.C. § 5318(g)(3)(A) ("Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency ... shall not be liable to any person under any law or regulation of the United States ... for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure.").

203. *See* FIN. CRIMES ENF'T NETWORK, *supra* note 199.

204. *See* ROSEN & MILLER, *supra* note 13, at 1. Unfortunately, the Corporate Transparency Act may now be of little practical value, as the Trump administration announced in March 2025 that "it would not enforce an anti-money laundering law that obliges millions of business entities to disclose the identities of their real beneficial owners." Ljunggren, *supra* note 13.

205. *See generally* FIN. CRIMES ENF'T NETWORK, *supra* note 199 (demonstrating how AML laws have evolved over time to address emerging threats).

B. How AML Provisions Can Be Applied to Cyberspace

The existing U.S. AML framework possesses both the flexibility and the reach to confront the evolving landscape of PRC MCA. AML laws have been expanded numerous times over the years to provide authorities with powerful tools to monitor and disrupt illicit financial flows.[206] Under 18 U.S.C. § 1956, it is illegal to knowingly conduct a "financial transaction" with "the proceeds of specified unlawful activities" (SUAs) for the purpose of concealing proceeds of an SUA, promoting an SUA, evading taxes, or evading reporting requirements.[207] The inclusion of computer fraud and abuse as an SUA underscores Congress's recognition of the need to provide authorities with additional legal avenues to prosecute MCA.[208] For example, offensive cyber infrastructure purchases or ransomware payments facilitated through PRC-linked actors could be prosecuted under § 1956 if the proceeds are funneled through U.S. financial institutions or used to promote further unlawful activity.[209] The statute also applies extraterritorially to transactions involving U.S. financial institutions, even if they originate abroad, making it particularly relevant for targeting PRC-linked actors who often launder funds through layered international transactions.[210]

---

206. *Id.*

207. 18 U.S.C. § 1956(a)(1).

208. *See* 18 U.S.C. §§ 1030, 18 U.S.C. § 1956(c)(7)(D).

209. Efforts that parallel the AML regime's coordinated efforts to detect, disrupt, and prosecute ransomware-related financial flows could also be applied toward financial networks facilitating PRC-linked cyber operations by leveraging suspicious activity reporting, economic sanctions, and money laundering statutes. *See* FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 2-4 (2021), https://www.fincen.gov/sites/default/files/ advisory/ 2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf [https://perma.cc/YME4-JEUW].

210. *See* Michael F. Zeldin, *Money Laundering: Legal Issues*, *in* CURRENT LEGAL ISSUES AFFECTING CENTRAL BANKS 209, 214 (Robert C. Effros ed., 1994), https://www.elibrary.imf.org/downloadpdf/display/book/9781557753069/ch018.pdf [https://perma.cc/5HEX-5EWF] (explaining that "§ 1956(f) provides for extraterritorial jurisdiction[,]" which could be particularly relevant for targeting PRC-linked actors who frequently launder funds through layered international transactions involving financial intermediaries). A federal district court in New York found an individual criminally liable for administering a specialty cryptocurrency as part of an unlicensed money transmission business because an extraterritorial effect was implied in 18 U.S.C. § 1960. United States v. Budovsky, No. 13cr368, 2015 WL 5602853, at *2-3 (S.D.N.Y. Sep. 23, 2015). This finding was due to a sufficient nexus between the organization and its American customers of the service even though the digital

In *United States v. 280 Virtual Currency Accounts*, North Korean operatives conducted wire fraud (an SUA) by stealing individual crypto accounts and then attempted to launder stolen cryptocurrency through financial institutions using false Know Your Customer (KYC) data and chain-hopping techniques to obscure the funds' origins.[211] At the end of a winding trail of transactions, the North Koreans tried to wash the crypto using Chinese over-the-counter crypto brokers.[212] This violated the prohibition in § 1956(a)(2) against international money laundering schemes in which funds are transferred across borders with the intent to promote or conceal a SUA.[213]

Additionally, individuals are prohibited from attempting to "conceal, falsify, or misrepresent" the source of assets in monetary transactions involving entities identified as primary money laundering concerns.[214] AML laws allow authorities to intervene at multiple stages of the money laundering process.[215]

Frequent coordination among law enforcement agencies and financial institutions is often essential in identifying suspicious transactions and disrupting these schemes before they can fully materialize.[216] One example of this is the U.S. Secret Service's Cyber Fraud Task Forces, which bring together private financial institutions and law enforcement at the federal, state, and local level to share information, detect cyber-enabled financial crimes, and coordinate rapid incident response efforts.[217]

---

transaction was conducted on computers in Costa Rica. *See id.* at *5; *see also* U.S. DEP'T OF THE TREASURY, *supra* note 18, at 2-3, 38.

211. No. 20-2396, 2024 WL 2049002, at *1-2 (D.D.C. May 8, 2024).

212. *Id.* at *2. The FBI was able to freeze and recover a portion of the stolen funds. *See Chainalysis in Action: Justice Department Demands Forfeiture of 280 Cryptocurrency Addresses Associated with North Korea Exchange Hackers*, CHAINALYSIS (Aug. 28, 2020), https://www.chainalysis.com/blog/lazarus-group-north-korea-doj-complaint-august-2020/ [https://perma.cc/XH7R-D69L].

213. *See* 18 U.S.C. § 1956(a)(2).

214. *See* 31 U.S.C. § 5335(b).

215. *See* FIN. ACTION TASK FORCE, *supra* note 14.

216. *See, e.g.*, *DOJ and FBI Phoenix Seize $112M in Proceeds from Crypto-Related Scams*, TRM LABS, https://www.trmlabs.com/case-study/doj-and-fbi-phoenix-crypto-seizure [https://perma.cc/72QZ-2UFM].

217. *See Preparing for a Cyber Incident*, U.S. SECRET SERV., https://www.secretservice.gov/investigations/cyberincident [https://perma.cc/4PGY-Q4HJ] (describing Cyber Fraud Task Forces as partnerships between law enforcement and private industry focused on "prevention, detection, mitigation, and investigation of cyber incidents").

The BSA, its amendments, and subsequent administrative rulemakings[218] impose stringent obligations on financial institutions "to implement and maintain an AML program, including policies, procedures, and controls to assure ongoing compliance with the applicable provisions of the Bank Secrecy Act."[219]

Ultimately, the statutory and regulatory language that governs U.S. AML requirements is broad enough to place obligations on entities in such a manner that could help U.S. authorities identify and prevent transactions that support PRC MCA. The definition of a "financial institution" under the BSA is notably broad, encompassing not only traditional banks but also entities such as money services businesses, casinos, securities brokers, and even car dealerships engaged in large cash transactions.[220] This expansive definition ensures that a wide array of economic activities fall under AML oversight.[221] Financial institutions are required to file Currency Transaction Reports for cash transactions exceeding $10,000 and Suspicious Activity Reports (SARs) for transactions that may involve criminal activity or violate federal law, with strict prohibitions against notifying customers of SAR filings to preserve investigative integrity.[222] The BSA also mandates robust record-keeping requirements to maintain a clear audit trail of customer accounts and transactions, which are critical for reconstructing financial activities during investigations.[223]

Regulations and prior enforcement actions have forced financial institutions to implement AML programs that adhere to the Five Pillars outlined by FinCEN: internal controls; independent testing; designation of a compliance officer; ongoing training; and customer

218. *See* 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210.

219. T.D. Bank, N.A., No. 2024-02, Consent Order at 4 (Dep't of the Treasury Oct. 10, 2024).

220. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

221. *See* 31 U.S.C. § 5312(a)(2) (defining "financial institution" to encompass a wide range of organizations).

222. 31 U.S.C. § 5313(a); 12 C.F.R. § 21.11(a), (k); T.D. Bank, N.A., *supra* note 219.

223. *See* 31 C.F.R. § 1010.410; FED. FIN. INSTS. EXAMINATION COUNCIL, BSA/AML MANUAL, https://bsaaml.ffiec.gov/manual/Introduction/01 [https://perma.cc/E6RE-BKWH] (explaining that statutory recordkeeping requirements under the BSA are critical to reconstructing transaction histories and supporting investigations into illicit financial activity).

due diligence, including KYC protocols.[224] These programs must be risk-based and tailored to the institution's size, geographic operational areas, clientele, and services offered.[225] For example, institutions must assess customer risk profiles during onboarding and monitor accounts for unusual activity that could indicate money laundering or other illicit behavior.[226] Failure to comply with these requirements can result in severe penalties, including fines and imprisonment for willful violations.[227] The Secretary of the Treasury can develop rules and minimum standards for "(A) the development of internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs."[228]

A risk-based approach ensures appropriate scrutiny of cross-border transactions and compliance with SAR and Currency or Monetary Instruments Report requirements for transporting monetary instruments exceeding $10,000 into or out of the United

---

224. *See* T.D. Bank, N.A., *supra* note 219, at 4-5, 5 n.12, 40 (illustrating how FinCEN leverages enforcement actions, such as consent orders, to publicly communicate and clarify the agency's interpretation of AML compliance obligations). U.S. AML requirements for financial institutions are governed by very broad statutory language. *See* 31 U.S.C. § 5318(h). FinCEN guidance helps financial institutions define AML program and reporting requirements. *See* 31 C.F.R. § 1020.210(a)(2) (identifying AML program requirements at a financial institution to include "at a minimum: (i) A system of internal controls to assure ongoing compliance; (ii) Independent testing for compliance to be conducted by bank personnel or by an outside party; (iii) Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance; (iv) Training for appropriate personnel; and (v) Appropriate risk-based procedures for conducting ongoing customer due diligence").

225. *See* Anti-Money Laundering and Countering the Financing of Terrorism Programs, 89 Fed. Reg. 55428, 55431 (July 3, 2024) ("The risk assessment process would need to identify, evaluate, and document the financial institution's risks, including consideration of … the ML/TF risks of the financial institution, based on its business activities, including products, services, distribution channels, customers, intermediaries, and geographic locations."); *FinCEN Issues Proposed Rule To Strengthen and Modernize Financial Institutions' AML/CFT Programs*, FIN. CRIMES ENF'T NETWORK (June 28, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-strengthen-and-modernize-financial-institutions [https://perma.cc/ZPJ2-A4VL] (describing a proposed FinCEN rule that has not yet been finalized as of October 2025).

226. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 223.

227. *See* 31 U.S.C. §§ 5321-5322; Alisa Abramova, *AML Laws and Regulations in the US 2024—What Has Changed?*, THE SUMSUBER (Nov. 26, 2024), https://sumsub.com/blog/aml-guide-usa/ [https://perma.cc/4ZWZ-TM54].

228. 31 U.S.C. § 5318(h)(1).

States.[229] Furthermore, the collective knowledge standard under the BSA further ensures that an institution's liability is assessed based on the organization's overall awareness of suspicious activity rather than the knowledge of individual employees alone.[230] As financial crimes evolve with advancements in technology like cryptocurrency mixers and decentralized finance platforms, FinCEN has proposed rules to modernize AML compliance frameworks while preserving their foundational principles of transparency and accountability.[231]

The significant AML obligations imposed on financial institutions can play a critical role in disrupting the various PRC cyber entities that conduct MCA. A "one-size-fits-all" approach that ignores the unique attributes of different entities within the PRC cyberspace ecosystem risks misallocating resources and failing to effectively disrupt the specific operational and financial networks that sustain these diverse threat actors.[232] By requiring institutions to file SARs and implement robust customer due diligence measures, AML frameworks can help identify and prevent the misuse of financial systems to fund or conceal cyber operations.[233] Like U.S. export controls, pressuring PRC cyber forces with aggressive AML enforcement could "force them to re-establish supplier relationships outside the United States, which is undoubtedly disruptive."[234] AML enforcement may also, in a manner similar to export controls, "serve as powerful signals to potential investors, which would raise the cost of financing and limit firms' ability to reinvest profits."[235]

On the surface, it would appear difficult to target either PLA or MSS cyber forces with AML countermeasures due to their purely domestic funding sources, but a closer inspection reveals that these

229. *See* 31 C.F.R. § 1010.340 (detailing reporting requirements for anyone who transports currency or monetary instruments exceeding $10,000).

230. *See* United States v. Bank of New England, N.A., 821 F.2d 844, 855-56 (1st Cir. 1987). *See generally* CHARLES DOYLE, CONG. RSCH. SERV., RL33315, MONEY LAUNDERING: AN OVERVIEW OF 18 U.S.C. § 1956 AND RELATED FEDERAL CRIMINAL LAW (2017) (providing an overview of federal AML law).

231. *See* FIN. CRIMES ENF'T NETWORK, *supra* note 225.

232. *See Unlocking Compliance Excellence: Embracing a Risk-Based Approach to AML*, FIN. CRIME ACAD. (July 15, 2025), https://financialcrimeacademy.org/risk-based-approach-to-aml-compliance [https://perma.cc/4W6H-JCVM].

233. *See* U.S. GOV. ACCOUNTABILITY OFFICE, GAO-24-106301, ANTI-MONEY LAUNDERING: BETTER INFORMATION NEEDED ON EFFECTIVENESS OF FEDERAL EFFORTS 14 (2024).

234. *See* Papademetriou, *supra* note 80, at 212.

235. *Id.*

units employ a host of ancillary personnel and suppliers, exposing a targetable vulnerability.[236] Therefore, while the PLA and MSS might not appear to be heavily exposed to the global financial network at first glance, their dependence on a vast support ecosystem firmly intertwines them with the financial industry.[237] This leaves them exposed to innovative and precise use of AML laws.

C. Limitations of the Current AML Framework

U.S. AML laws have the potential to greatly benefit the fight against PRC MCA, but they are not without their limitations. There are both challenges and risks in leveraging an AML framework against PRC MCA, as financial institutions are likely to struggle to identify transactions linked to state-sponsored operations that increasingly utilize private-sector proxies with criminal appendages.[238]

1. Difficulties Applying Existing AML Laws Against Cyber Threats

While AML laws offer a highly adaptable framework, their effective application against PRC MCA is hampered by the frequently blurred lines between public and private actors within the PRC cyber ecosystem, making it difficult to identify and target the responsible entities. While AML frameworks have been successfully adapted to address ransomware and cryptocurrency schemes, such as those linked to North Korean cyber actors, PRC

236. *See* Handler, *supra* note 53 ("Chinese security services still have a marked preference for using contracted hacking teams. These groups often raise money from committing criminal acts, in addition to work on behalf of intelligence agencies.") (quoting Dakota Cary).

237. *See* CHAVANE, *supra* note 46, at 21-23; *see also* EUGENIO BENINCASA, BEFORE VEGAS: THE "RED HACKERS" WHO SHAPED CHINA'S CYBER ECOSYSTEM 60 (2025), https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/before-vegas-cyberdefense-report.pdf [https://perma.cc/3KAP-KBR6] ("The MSS has made growing use of private-sector proxies, working through front companies established specifically for cyber operations as well as legitimate businesses.").

238. *Cf. Reviewing the Bureau of Industry and Security, Part I: U.S. Export Controls in an Era of Strategic Competition: Hearing Before the Subcomm. on Oversight & Accountability of the H. Comm. on Foreign Affs.*, 118th Cong. 16-18 (2023) (statement of Hon. Nazak Nikakhtar) (paralleling the challenge that export controls face in distinguishing military from civilian use due to the difficulty in obtaining intelligence on PLA diversion).

MCA often involves complex and layered structures in mainland China and other friendly territories that obscure the financial trail.[239] The use of shell companies to purchase infrastructure, such as servers and domain registrations, while layering transactions across multiple entities would complicate attribution and enforcement.[240] This obfuscation strategy mirrors the tactics employed by some ransomware groups, where funds are laundered through decentralized platforms, making it difficult for investigators to trace monetary flows back to their origin.[241] Encouraging financial institutions and federal authorities to utilize AML laws to target PLA MCA would require a high degree of intelligence sharing to identify PLA personnel, technical infrastructure, and supporting organizations.[242]

However, implementing AML measures against PRC cyber entities is fraught with significant challenges. The decentralized nature of China's contractor ecosystem, where private firms and freelance actors often operate in close coordination with state agencies, makes it difficult to identify and disrupt illicit financial flows effectively.[243] Additionally, many of these entities benefit from the legal cover provided by the state, which shields them from international scrutiny and enforcement actions under the guise of

---

239. *See* United States v. 280 Virtual Currency Accts., No. 20-2396, 2024 WL 2049002 (D.D.C. 2024); Piotr Malachinski & Marine Pichon, *The Hidden Network: How China Unites State, Corporate, and Academic Assets for Cyber Offensive Campaigns*, ORANGE CYBERDEFENSE (Nov. 24, 2024), https://www.orangecyberdefense.com/global/blog/cert-news/the-hidden-network-how-china-unites-state-corporate-and-academic-assets-for-cyber-offensive-campaigns [https://perma.cc/D32B-TKBD] (reiterating that "China's offensive cyber capabilities are, in fact, supported by a complex and multi-layered ecosystem" to procure infrastructure, vulnerabilities, personnel, and remote access).

240. *See* Indictment at 1, 24, United States v. Yin Kecheng, No. 23-cr-99 (D.D.C. Mar. 16, 2023).

241. *See* U.S. DEP'T OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 16 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [https://perma.cc/FF87-CVAQ].

242. *See* FIN. CRIMES ENF'T NETWORK, *supra* note 209, at 9 ("When filing a SAR regarding suspicious transactions that involve cyber events (including ransomware), financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators.").

243. *See* Christopher K. Tong, *China Turns to Private Hackers as It Cracks Down on Online Activists on Tiananmen Square Anniversary*, UNIV. MARYLAND, BALTIMORE COUNTY: MAG. (June 7, 2024), https://umbc.edu/stories/china-private-hackers-tiananmen-square-anniversary/ [https://perma.cc/RKU6-BV6U] (describing the decentralization among PRC cyber actors).

compliance with PRC intelligence and security mandates.[244] Despite these obstacles, specifically targeting AML laws at the financial infrastructure that enables PLA, MSS, and private sector cyber forces should help to expose, isolate, and disrupt their operations.[245]

Another challenge lies in the immense pressure AML laws place on financial institutions to detect and report suspicious activity. Financial institutions are required to file various reports when they identify transactions that may involve illicit activity, but the technical complexity of PRC MCA makes it extremely difficult for these institutions to identify such transactions without accurate intelligence provided by the government.[246] "The forensics required to connect dots, let alone meet a legal burden of proof, are difficult and often inconclusive."[247] These difficulties are compounded by the extraterritorial limitations of U.S. AML laws, which struggle to sway PRC financial institutions unless they frequently engage with the U.S.-based financial system.[248]

Lastly, the dispersed nature of private cyber contractors in the PRC creates a difficult whack-a-mole problem for enforcement. Even if one entity is sanctioned or prosecuted, others can quickly take its place under different names or structures. While AML laws remain a critical tool for countering cyber-enabled financial crime, effectively applying them against PRC MCA will require enhanced international cooperation, better integration of cybersecurity intelligence into AML programs, and updated regulatory guidance tailored to the unique challenges posed by state-sponsored cyber threats.

---

244. *See id.*

245. *See Countering Threats Hearing*, *supra* note 11, at 50-53.

246. *Cf.* OFF. OF THE INSPECTOR GEN., FED. DEPOSIT INS. CORP., SHARING OF THREAT AND VULNERABILITY INFORMATION WITH FINANCIAL INSTITUTIONS at i-iii (Aug. 29, 2023), https://www.fdicoig.gov/sites/default/files/reports/2023-08/EVAL-23-002%20REDACTED%20FINAL_0.pdf [https://perma.cc/B2JV-BP8V] (describing current FDIC information-sharing practices); *Overlapping Risks, Part 1: Anti-Money Laundering and Cybersecurity*, FIN. INDUS. REGUL. AUTH. UNSCRIPTED (Oct. 27, 2020), https://www.finra.org/media-center/finra-unscripted/aml-cybersecurity [https://perma.cc/2PE2-DX45].

247. Fidler, *supra* note 137, at 753 (describing an attribution problem with sanctions for spyware use).

248. *See* Joel Slawotsky, *U.S. Extraterritorial Jurisdiction in an Age of International Economic Strategic Competition*, 52 GEO. J. INT'L LAW 427 (2021).

2. Risks of Using AML Laws to Target PRC Cyber Threats

The deployment of the AML framework to combat PRC MCA may introduce significant risks and unforeseen externalities. First, it would provide greater impetus for the PRC to hedge against a dollar-dominated economy, thereby expediting an ongoing bifurcation of global financial and data systems.[249] By imposing AML policies unilaterally and extraterritorially, the U.S. risks further pushing nonaligned nations toward implementing alternative monetary systems that bypass U.S. influence.[250] The PRC has been actively seeking ways to reduce its reliance on the U.S. dollar, including promoting the internationalization of the renminbi and developing alternative payment systems such as the Cross-Border Interbank Payment System (CIPS).[251] Targeting PRC MCA through AML laws may accelerate this trend, as the PRC would likely view such actions as economic coercion.[252] This could lead to further fragmentation of global financial systems, with neutral or third-party countries potentially ignoring or circumventing U.S.-imposed AML restrictions to maintain economic ties with the PRC.

Many countries and non-U.S. domiciled financial institutions may view unilateral U.S. sanctions or AML measures as overreach, particularly if they are seen as being applied extraterritorially

249. *See* Zongyuan Zoe Liu, *China Wants To Ditch the Dollar*, NOEMA MAG. (Jan. 11, 2024), https://www.noemamag.com/china-wants-to-ditch-the-dollar/ [https://perma.cc/6257-TEJH] (indicating that potential sanctions are pushing "China's state-owned financial institutions and enterprises ... [to] inoculate themselves against potential international sanctions in the event of a military conflict with the West over Taiwan.").

250. *See* ROBERT GREENE, CHINA'S DOLLAR DILEMMA 1 (2024), https://carnegie-production-assets.s2.amazonaws.com/static/files/Greene_China%20Dollar_final.pdf [https://perma.cc/4RAU-MZCC]; *see also* MARCO CIPRIANI, LINDA S. GOLDBERG & GABRIELE LA SPADA, FINANCIAL SANCTIONS, SWIFT, AND THE ARCHITECTURE OF THE INTERNATIONAL PAYMENT SYSTEM 26 (2023), https://newyorkfed.org/medialibrary/media/research/staff_reports/sr1047.pdf [https://perma.cc/C668-8JLP] ("The use of the SWIFT system as a tool for financial sanctions by the European Union, the United Kingdom, Canada, and the United States has encouraged other large countries around the world to consider building systems of their own.").

251. *See* Barry Eichengreen, *Sanctions, SWIFT, and China's Cross-Border Interbank Payments System*, CTR. FOR STRATEGIC & INT'L STUD. (May 20, 2022), https://www.csis.org/analysis/sanctions-swift-and-chinas-cross-border-interbank-payments-system [https://perma.cc/X4LZ-C75V].

252. *See* GREENE, *supra* note 250, at 1 ("[P]rominent voices in China are calling to reduce the Chinese financial system's exposure to the dollar.").

without multilateral consensus.[253] This creates significant economic incentives for third-party countries or offshore financial institutions to ignore these restrictions in favor of maintaining profitable relationships with PRC entities.[254] The result could be a weakening of global AML enforcement as financial institutions seek ways to avoid compliance costs while continuing to engage with markets in the PRC.

A more immediate risk is the increased compliance burden on financial institutions. The cost of adhering to escalating AML regulations is already significant, with compliance costs in 2023 reaching $61 billion in the U.S. and Canada alone.[255] These costs are likely to rise further if financial institutions are required to screen transactions related to PRC cyber activities.[256] The imposition of additional AML requirements effectively transfers the cost of geopolitical competition onto private sector financial entities, as they bear the brunt of increased screening and reporting obligations.[257] As these costs escalate, they may reduce the competitiveness of U.S. financial institutions globally, especially if other nations do not impose similar requirements.[258] Offshore financial

253. *See* CLAY LOWERY & VIJAYA RAMACHANDRAN, UNINTENDED CONSEQUENCES OF ANTI-MONEY LAUNDERING POLICIES FOR POOR COUNTRIES 33-43 (2015), https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf [https://perma.cc/2TVA-DVER].

254. *See* DREW THOMPSON, DON'T MAKE US CHOOSE SIDES: SOUTHEAST ASIAN PERSPECTIVES OF U.S. STRATEGY AND PRESENCE IN THE REGION 9-13 (2024), https://lkyspp.nus.edu.sg/docs/default-source/cag/don't-make-us-choose-sides_march2024.pdf [https://perma.cc/H5S6-VHGA].

255. *See* FORRESTER RSCH., TRUE COST OF FINANCIAL CRIME COMPLIANCE STUDY, 2023 UNITED STATES AND CANADA 5 (2023), https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada?trmid=BSGENL24.CRPORT.PR.CS3P-1118106 [https://perma.cc/Z392-MRCC].

256. *See id.* at 7-10.

257. *See* Press Release, Marcy Theobald, LexisNexis Risk Sols., Geopolitical Risks Driving Financial Crime Compliance Costs According to LexisNexis Risk Solutions Research (Sep. 27, 2022), https://risk.lexisnexis.com/global/en/about-us/press-room/press-release/20220927-geopolitical-risks-driving-financial-crime [https://perma.cc/V4X7-MEXK] ("Financial services institutions surveyed across EMEA indicate that 71% of respondents identified geopolitical risk as the top external trend impacting costs, followed closely by increasing anti-money laundering (AML) regulations (70%) and evolving criminal threats (69%).")

258. *See* MATTEO CROSIGNANI, LINA HAN, MARCO MACCHIAVELLI & ANDREÉ F. SILVA, SECURING TECHNOLOGICAL LEADERSHIP? THE COST OF EXPORT CONTROLS ON FIRMS 27 (2024), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1096.pdf [https://perma.cc/484Z-VURW] (concluding that export controls result in a "reduction in banks'

institutions operating in jurisdictions with weaker regulatory frameworks may engage in a form of regulatory arbitrage created by strict U.S. AML rules.[259] By offering services that bypass these restrictions, such institutions could attract business from entities seeking to avoid compliance costs, further undermining global efforts to combat money laundering.[260]

An unintended consequence of stringent AML enforcement is often financial exclusion, particularly in poorer countries where banks may decide that compliance costs outweigh potential profits from serving certain clients or regions.[261] This could further marginalize developing countries from the global financial system, exacerbating economic inequality and limiting their ability to engage in legitimate international trade.[262]

Additionally, developing countries may perceive U.S.-imposed AML measures targeting cyber activities as a form of development suppression. These countries may view these AML measures as an attempt by the U.S. to control access to cyberspace under the guise of combating illicit finance.[263] Without clear articulation from the U.S. regarding what constitutes acceptable offensive cyber

---

credit exposure to affected suppliers, driven by a reduction in the quantity of term loans but no change in credit line commitments and utilization. Banks also charge higher interest rate spreads and shorten the maturity of their credit exposures to affected suppliers following the imposition of export controls").

259. *See* Nicholas Roide, Comment, *Fintech and Anti-Money Laundering Regulation: Implementing an International Regulatory Hierarchy Premised on Financial Innovation*, 9 TEX. A&M L. REV. 465, 484-88 (2022).

260. *See, e.g.*, LOWERY & RAMACHANDRAN, *supra* note 253, at 9 (arguing that entities bypassing AML restrictions undermine global anti-money laundering efforts).

261. *See* LOWERY & RAMACHANDRAN, *supra* note 253, at vii.

262. *See* Clay Lowery & Vijaya Ramachandran, *Are Anti-Money Laundering Policies Hurting Poor Countries?-New CGD Working Group Report*, CTR. FOR GLOBAL DEV. (Nov. 9, 2015), https://www.cgdev.org/blog/are-anti-money-laundering-policies-hurting-poor-countries-new-cgd-working-group-report [https://perma.cc/4SAC-AXKD].

263. *Id.* at vii ("But the policies that have been put in place to counter financial crimes may also have unintentional and costly consequences, in particular for people in poor countries. … And sometimes, current policies may be self-defeating to the extent that they reduce the transparency of financial flows."); *see also* Louise Marie Hurel, *Accountability in Cyberspace: Lessons from and for Latin America*, THE HENRY L. STIMSON CTR. (Oct. 16, 2024), https://www.stimson.org/2024/accountability-in-cyberspace-lessons-from-and-for-latin-america/ [https://perma.cc/N9TB-G3D4] ("[C]competing security and economic incentives have created disjointed narratives with a securitized and militarized vision of cyberspace, on the one hand, and the commitment to market innovation, digital economy, and digital security, on the other.").

operations, U.S. AML enforcement against various cyber organizations could be interpreted by these countries as the U.S. forcing them to "purchase second-tier—i.e., less powerful or effective—spyware" in an effort to restrict their ability to develop digital economies or participate in global cyberspace activities.[264] Other countries may view such restrictions as a harsh double-standard.

The use of AML laws in this context also raises important questions for U.S. domestic policy regarding offensive cyber operations. The lack of clear standards or norms governing what types of offensive cyber operations are permissible creates ambiguity that could undermine both domestic and international support for these measures.[265] The application of AML laws to target PRC cyber activities could serve as a forcing function within U.S. policy circles, prompting a more explicit articulation of what types of offensive cyber operations are permissible under international law.[266] This clarity is crucial not only for ensuring consistent enforcement but also for maintaining credibility with international partners who may be skeptical of unilateral actions perceived as overreach.

---

264. *See* Silberman, *supra* note 156, at 264.

265. *See generally* THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023) https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/FE7P-A4QA] (calling for development of clear international cyber norms to reduce ambiguity in state conduct); U.S. DEP'T OF STATE, UNITED STATES INTERNATIONAL & DIGITAL POLICY STRATEGY (2024), https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf [https://perma.cc/7L4U-VGHM] (emphasizing the U.S. commitment to advancing and clarifying international norms for responsible state behavior in cyberspace).

266. *See* Anusha Pakkam, *The Evolving Interpretation of the Use of Force in Cyber Operations: Insights from State Practices*, LIEBER INST.: ARTICLES OF WAR (Nov. 25, 2024), https://lieber.westpoint.edu/evolving-interpretation-use-of-force-cyber-operations-insights-state-practices/ [https://perma.cc/T5F9-REHL] ("[R]eflect[ing] a significant trend toward recognizing that the impacts of cyber operations, particularly those causing substantial economic damage or loss of functionality, can cross the threshold for a use of force, thereby shaping the emerging legal framework governing State behavior in cyberspace and influencing determinations in this evolving area of international law."); *see also* PUBLIC-PRIVATE ANALYTIC EXCH. PROGRAM, COMBATTING ILLICIT ACTIVITY UTILIZING FINANCIAL TECHNOLOGIES AND CRYPTOCURRENCIES PHASE III at 26 (2024), https://www.dhs.gov/sites/default/files/2024-09/2024aepphaselllcombattingillicitactivityutilizing financial.pdf [https://perma.cc/UD5U-ZHGL] ("There is also a push for greater international cooperation to combat cross-border cryptocurrency-related crimes.").

While using AML laws to target PRC MCA may seem like an effective tool for disrupting illicit financial flows associated with these operations, it carries significant risks. These include exacerbating global financial fragmentation, imposing heavy compliance costs on U.S. financial institutions, sending negative signals to developing countries about access to cyberspace, and calling into question the United States' own policies towards offensive cyber operations.[267] A multilateral approach that balances enforcement with clear norms and standards may mitigate some of these risks while still achieving the same strategic objectives.[268]

IV. COURSE CORRECTION: INTERNATIONAL AML COOPERATION AND LEGISLATIVE PROPOSALS

International AML cooperation provides a strategic response to PRC MCA by targeting financial networks that support theire operations.[269] Separately, the proposed Combating Money Laundering in Cyber Crime Act would enhance investigative authority over

267. *See* BANK POL'Y INST. GLOBAL FINANCIAL MARKETS ASSOCIATION & INST. INT'L FIN., THE COSTS OF FRAGMENTATION AND POSSIBLE SOLUTIONS 3-8 (2025), https://www.gfma.org/wp-content/uploads/2025/07/the-costs-of-fragmentation-and-possible-solutions-2025.07.08.pdf [https://perma.cc/62N3-U8WU] (noting that fragmentation in global financial regulation exacerbates systemic risk and imposes heavy compliance burdens on financial institutions); Press Release, Int'l Telecomm. Union, World's Least Developed Countries Threatened by Deepening Digital Divide (Mar. 5, 2023), https://www.itu.int/en/mediacentre/Pages/PR-2023-03-05-facts-and-figures-focus-on-least-developed-countries.aspx [https://perma.cc/Q9XC-TH2V] (highlighting digital connectivity challenges in developing countries that underscore difficult access to cyberspace); Brandon Valeriano & Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint*, THE CATO INST. (Jan. 15, 2019), https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint [https://perma.cc/EM3Y-CFVZ] (arguing that expansive U.S. offensive cyber operations risk negative international signaling and exacerbate strategic tensions).

268. *See generally* NORBERT J. MICHEL & JENNIFER J. SCHULP, CATO INST., REVISING THE BANK SECRECY ACT TO PROTECT PRIVACY AND DETER CRIMINALS 2 (2022), https://www.cato.org/sites/cato.org/files/2023-04/policy-analysis-932-update-4-12-23.pdf [https://perma.cc/8PWR-WTJ6] (critiquing the high compliance costs and unintended consequences of AML regulations on financial institutions).

269. *See* Fin. Action Task Force, Countering Ransomware Financing 9-10, 47 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf [https://perma.cc/A5DF-VY59] ("For example, illicit payments had to be made to various criminal partners and used for infrastructure (software engineers and developers, bullet proof hosts for servers, bullet proof VPN services to hide communication or connection to the command-and-control servers, ML services to organize peel chain movements, etc.), and to find mules and cash-out facilities.").

digital asset transactions and unlicensed money transmitters.[270] This approach may assist in disrupting the operational capabilities of both state-sponsored units and their private-sector proxies while avoiding direct military confrontation.[271]

A. International AML Cooperation

International cooperation is essential for combating the financial tethers of PRC MCA, as these crimes often exploit vulnerabilities in cross-border transactions. Existing frameworks need to not only be more consistently applied, but should also be strengthened through enhanced information sharing, coordinated law enforcement actions, and the reinforcement of global norms to protect the integrity of the international financial system.[272] U.S. and allied governments, financial institutions, and technology companies must work together across borders to reduce fragmentation, build collective resilience, and ensure a rapid, unified response to PRC MCA.[273]

The Financial Action Task Force (FATF) plays a leading role in setting global standards for AML frameworks by requiring member countries to implement robust regulatory regimes under Recommendation 26.[274] FATF's risk-based approach ensures that countries

---

270. COMBATING MONEY LAUNDERING IN CYBER CRIME ACT OF 2024, H.R. 7156, pt. 1, 118th Cong. (2024).

271. *See* Matt Bracken, *Senators Re-Up Bill To Expand Secret Service's Financial Cybercrime Authorities*, CYBERSCOOP (Apr. 4, 2025), https://cyberscoop.com/secret-service-financial-cybercrimes-senate-bill/ [https://perma.cc/TL5U-RTCP] ("The Department of Justice and Treasury Department have warned in recent years about the increasing frequency with which digital assets are being used in ransomware attacks, fraud schemes, money laundering and other crimes.").

272. *See* Tim Maurer & Arthur Nelson, *The Global Cyber Threat*, INT'L MONETARY FUND (2021), https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm [https://perma.cc/R96Z-GGS7] (noting the urgency of international collaboration and the need for strengthened norms and coordinated responses to protect the global financial system).

273. *Cf.* Press Release, United Nations Off. on Drugs & Crime, UN General Assembly Adopts Landmark Convention on Cybercrime (Dec. 24, 2024), https://www.unodc.org/unodc/en/press/releases/2024/ December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html [https://perma.cc/XM8Q-KRE9] ("The adoption of this landmark convention is a major victory for multilateralism, marking the first international anti-crime treaty in 20 years. It is a crucial step forward in our efforts to address crimes like online child sexual abuse, sophisticated online scams and money laundering.").

274. *See* FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF

prioritize resources to address the most pressing threats, while its "High-Risk Jurisdictions [S]ubject to a Call for Action" and "Jurisdictions [U]nder Increased Monitoring" lists (colloquially referred to as the "black and grey lists")[275] incentivize compliance by imposing reputational and financial penalties on noncompliant nations.[276] Similarly, the Egmont Group facilitates secure information sharing among its 177 members, which includes FinCEN, and enables the exchange of SARs and other reports to trace illicit financial flows tied to cybercrime.[277] These frameworks reduce safe havens for cybercriminals and harmonize enforcement globally, making it harder for PRC-linked actors to launder proceeds from MCA or procure infrastructure, software, or talent.[278]

Despite these efforts, challenges remain in achieving widespread international cooperation. Uneven implementation of FATF standards across jurisdictions creates enforcement gaps that PRC actors can exploit, particularly in areas like cryptocurrency transactions and zero-day vulnerability markets.[279] Moreover, the extraterritoriality limitations of U.S. AML laws require multilateral coalitions to align enforcement priorities and close regulatory loopholes like the current lack of "international cooperation on trade in zero-days and related software."[280] To address these issues, the

---

RECOMMENDATIONS 23 (2025) https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf [https://perma.cc/78ZK-8NGS] (urging countries to "take the necessary legal or regulatory measures" to enforce AML standards against domestic financial institutions).

275. *Black and Grey Lists*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html [https://perma.cc/L9UQ-QXA8].

276. *See What Is the Financial Action Task Force (FATF)?*, NICE ACTIMIZE, https://www.niceactimize.com/glossary/financial-action-task-force/ [https://perma.cc/AG74-NX5W].

277. *About the Egmont Group*, EGMONT GROUP, [hereinafter *About Egmont Group*] https://egmontgroup.org/about [https://perma.cc/E8Y8-C4QF]; *see* EGMONT GROUP, EGMONT GROUP STRATEGIC PLAN 2022-2027 4-11 (2022), https://egmontgroup.org/wp-content/uploads/2022/08/33.-Egmont-Group-Strategic-Plan-2022-2027-1.pdf [https://perma.cc/J9S4-6XXE].

278. *See* INST. FOR FIN. INTEGRITY, CYBER-ENABLED FRAUD: FATF ISSUES REPORT ABOUT ILLICIT FINANCIAL FLOWS 12 (2023), https://finintegrity.org/wp-content/uploads/2024/01/IFI-Expert-Insight-Cyber-Enabled-Fraud.pdf [https://perma.cc/G9JR-4GUZ] ("International cooperation is critical to detecting and deterring the movement of funds obtained through CEF [cyber enabled fraud].").

279. *See* FIN. ACTION TASK FORCE, *supra* note 14, at 49-58.

280. Fidler, *supra* note 137, at 716. *See* Slawotsky, *supra* note 248, at 434 ("In the wider context of hegemonic power rivalry, nations may object to extraterritorial jurisdiction based upon a violation of the principle of 'non-intervention' in another sovereign's affairs.").

U.S. must work with "multilateral coalitions of the willing" to enhance information sharing and coordinate enforcement actions against PRC-linked entities.[281] Certain objectives, such as financial enrichment and intellectual property theft, may be more easily deterred or disrupted through AML frameworks, particularly if U.S. allies and neutral nations are willing to coordinate in enforcement.[282] By strengthening international AML cooperation, the global community can more effectively disrupt the financial networks underpinning PRC MCA.[283]

B. Proposed Legislative Changes

In August 2024, "U.S. Senators Catherine Cortez Masto (D-Nev.), Chuck Grassley (R-Iowa), and Amy Klobuchar (D-Minn.) introduced the *Combatting Money Laundering in Cyber Crime Act.*"[284] This bill would provide additional investigative authority to the Secret Service over unlicensed money transmitting businesses with the intent of creating heightened scrutiny over cybercrimes involving digital assets.[285] The bill also includes a five-year extension to the requirement that FinCEN "report to the Congress on a voluntary public-private partnership ... [between] financial institutions, law enforcement, and intelligence agencies."[286] This bill should go a step further and fund permanent personnel to oversee public-private intelligence sharing and enforcement action coordination against

281. *See* Fidler, *supra* note 137, at 758.

282. *See* THE WHITE HOUSE, *supra* note 265; *see also* Fin. Action Task Force, *supra* note 269, at 46.

283. *See* U.S. DEP'T OF THE TREASURY, *supra* note 18, at 1, 8.

284. Press Release, Catherine Cortez Masto, Cortez Masto, Grassley Introduce Bipartisan Bill to Strengthen Secret Service's Ability to Combat Cyber Money Laundering (Aug. 2, 2024), https://www.cortezmasto.senate.gov/news/press-releases/cortez-masto-grassley-introduce-bipartisan-bill-to-strengthen-secret-services-ability-to-combat-cyber-money-laundering/ [https://perma.cc/Z3NW-NSF4].

285. H.R. REP. NO. 118-590, pt. 1, at 5-6 (2024). The U.S. House Report on the bill noted that "a significant portion of this illicit activity involves unlicensed money transmitting businesses, illicit structuring of transactions, and other criminal or unlawful activity in or against organizations that are not federally insured financial institutions, but are financial institutions as defined under the Bank Secrecy Act (31 U.S.C. § 5312) [which] ... presents challenges for U.S. law enforcement in addressing criminal activity involving digital assets." *Id.* at 2-3.

286. *Id.* at 6.

PRC MCA just like the interagency Joint Ransomware Task Force.[287] It would also "extend the requirement that the U.S. executive director of the International Monetary Fund support an increase in the amount the agency allocates for programs to prevent money laundering and the financing of terrorism."[288] Most importantly, the bill "mandates a Government Accountability Report within a year to assess law enforcement's ability to detect and deter money laundering."[289] These legislative changes seek to support U.S. federal law enforcement's "ability to investigate various crimes related to digital asset transactions and to counter transnational cyber-criminal activity."[290] Companion legislation was introduced by U.S. House "Representatives Scott Fitzgerald (R-Wis.-05), Zach Nunn (R-Iowa-03), Gregory Meeks (D-N.Y.-05), and Madeleine Dean (D-Pa.-04)."[291]

The U.S. AML framework has evolved to address emerging threats, and further adaptations are necessary to effectively counter PRC MCA. Domestically, clearer guidance from FinCEN is needed on AML like KYC and SAR filing standards. FinCEN's June 2024 Notice of Proposed Rulemaking emphasized the importance of risk-based AML programs, but any adopted rules should specifically require financial institutions to identify and report transactions potentially linked to MCA, such as those involving shell companies or cryptocurrency brokers.[292] Similarly, legislation akin to the Digital Asset Anti-Money Laundering Act of 2023 should be leveraged

287. *See* FIN. CRIMES ENF'T NETWORK, *supra* note 209, at 8-11; *Joint Ransomware Task Force*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/joint-ransomware-task-force [https://perma.cc/MU7E-PPTG]. The bill could also require large financial institutions to send a representative to attend the public-private cyber threat intelligence sharing meetings.

288. *Id.*

289. Matt Bracken, *Bipartisan Senate Bill Calls for Stronger Secret Service Financial Cybercrime Probes*, CYBERSCOOP (July 30, 2024), https://cyberscoop.com/secret-service-financial-cybercrime-investigations-senate-bill/ [https://perma.cc/LNX9-UE8B].

290. H.R. REP. NO. 118-590, at 2.

291. Cortez Masto, *supra* note 284. Although neither bill was included in the 2025 National Defense Authorization Act (NDAA), Senator Cortez Masto has reintroduced the bill in 2025. *See* Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, 138 Stat. 1773 (2024); Combating Money Laundering in Cyber Crime Act of 2025, S. 1273, 119th Cong. (2025); Bracken, *supra* note 271.

292. *See Fact Sheet: Proposed Rule to Strengthen and Modernize Financial Institution AML/CFT Programs*, FIN. CRIMES ENF'T NETWORK (June 28, 2024), https://www.fincen.gov/sites/default/files/shared/Program-NPRM-FactSheet-508.pdf [https://perma.cc/6XT9-7DH3].

to close gaps in cryptocurrency regulation by classifying overseas fiat-to-crypto brokers as financial institutions under the Bank Secrecy Act, ensuring they are subject to the same reporting and compliance requirements.[293]

Internationally, the U.S. should advocate for multilateral enhancements to global AML standards that expand on FATF's existing recommendations. The additions should address the global financial ecosystem that enables MCA in order to better equip member countries to combat those threats.[294] Additionally, strengthening cooperation among national financial intelligence units under the Egmont Group would improve the sharing of financial intelligence, to include SARs, across jurisdictions.[295] By fostering collaboration among willing partners, the U.S. can encourage global alignment on AML enforcement priorities, reduce the available maneuver space for PRC-linked cyber actors, and amplify the deterrent effect of these measures. These reforms would help AML laws address the unique challenges posed by PRC MCA.

CONCLUSION

The U.S. should utilize AML laws to disrupt, degrade, and deny the PRC access to financial networks that enable its MCA. By leveraging existing legal frameworks, the U.S. can nudge financial institutions to identify and report suspicious transactions tied to PRC-linked actors, thereby hampering the infrastructure and operational requirements of both private-sector and state-controlled cyber units. However, AML may face significant limitations without broader multilateral support. Funding for military cyber operations often bypasses traditional financial channels targeted by AML regulations, making it nearly impossible to fully disrupt state-sponsored MCA. Nonetheless, AML enforcement could slow down the private-sector actors conducting PRC MCA by complicating their access to

293. *See* Digital Asset Anti-Money Laundering Act of 2023, S. 2669, 118th Cong. (2023) (addressing the role of intermediaries that enable the exchange of cryptocurrency for sovereign currency, a step often essential to monetizing ransomware proceeds).

294. *See* FIN. ACTION TASK FORCE, *supra* note 274, at 27-30. Regulators could specifically address cyber-crimes in either the "[m]utual legal assistance" or "[m]utual legal assistance: freezing and confiscation" recommendations sections. *Id.*

295. *See About the Egmont Group*, *supra* note 277.

global financial systems. Despite these challenges, opportunities exist to refine AML laws and enforcement strategies by clarifying FinCEN rules and encouraging international bodies like FATF to adopt recommendations specifically addressing PRC MCA.

Owen T. Tremblay[*]

* J.D. Candidate, 2026, William & Mary Law School; B.S., Business, 2018, New York University. Thank you to my Notes Editor, Sally Harnish, along with the entire *William & Mary Law Review* staff, for all of the time and effort spent shepherding this Note through the publication process.