FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Building Partner Capabilities for Cyber Operations

By RADM (Ret.) Mark Montgomery and Annie Fixler

July 27, 2023

Executive Summary[1]

In December 2015, Russia turned the lights out in Kyiv. In the spring of 2022, they could not. But this was not for lack of trying.[2] Since the war began, Ukraine has sustained thousands of Russian cyberattacks,[3] but the nation has endured because it has spent the better part of the last decade building its cyber defenses, often with the help of the United States and other international partners. The country has demonstrated that one country's ability to prevent, mitigate, and recover from cyberattacks enhances global economic stability and security. Because of strong Ukrainian defenses, Russian cyberattacks have not cascaded across Europe and America, as was the case in 2017 with the Russian NotPetya malware.[4]

The Biden administration's National Cybersecurity Strategy argues that a prosperous future requires resilient global digital infrastructure built on the values of democracy, free speech, and innovation.[5] This means building and strengthening international partnerships to reinforce norms of responsible behavior, disrupt malicious actors, and enhance the ability of allies and partners to secure themselves against cyber threats. The 2023 U.S. Defense Cyber Strategy calls these allies and partners America's "foundational advantage in the cyber domain."[6]

The U.S. government conducts partner cyber capacity-building programs across multiple federal departments — to include the Departments of State, Justice, Energy, Homeland Security, Treasury, and Defense and the intelligence community. These programs help allies and partners build cyber resilience, develop national cyber strategies,

1. This research memo was submitted for workshop review at CyCon 2023, the 15th International Conference on Cyber Conflict in Tallinn, Estonia, on May 30, 2023.

2. "Russian hackers thwarted in attempt to take out electrical grid, Ukrainians say," *CyberScoop*, April 12, 2022. (https://cyberscoop.com/ukrainian-electrical-grid-industroyer2-russia-sandworm)

3. Mykhailo Fedorov, "Lessons from Ukraine in the Heat of an Ongoing Hybrid War," *Digital Front Lines*, May 31, 2023. (https://digitalfrontlines.io/2023/05/31/lessons-from-ukraine-in-the-heat-of-an-ongoing-hybrid-war)

4. Ellen Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," *The Washington Post*, January 12, 2018. (https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html)

5. The White House, "National Cybersecurity Strategy," March 2023. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

6. U.S. Department of Defense, "Fact Sheet: 2023 DoD Cyber Strategy," May 26, 2023. (https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF)

prosecute cyber criminals, and evict malicious cyber actors from critical networks. They have become so popular around the world that demand "exceeds our capacity to deliver," Nathaniel Fick, U.S. ambassador at large for Cyberspace and Digital Policy, said in June.[7]

Capacity-building programs help other countries learn to defend themselves in cyberspace. More resilient partners are less likely to succumb to an attack or need recovery assistance. But the U.S. government also helps partners recover, remediate, and conduct forensic analysis to determine the cause and culprit when cyberattacks succeed. These efforts can yield valuable insights about attacker techniques that can then be shared with other governments and the public.

In addition, the Department of Defense (DoD) has developed comprehensive partner capacity-building efforts with its North American Treaty Organization (NATO) allies and others. As part of this effort, U.S. Cyber Command conducts numerous cyber military exercises to practice planning, improve joint actions, and assess interoperability. These exercises reinforce what the U.S. military has long known — military communications and the ability to mobilize, deploy, and sustain forces require resilient U.S. and partner telecommunications systems, electrical power grids, water utilities, rail lines, airfields, ports, and other logistics infrastructure. If an adversary can cripple the backbone of these critical infrastructures, America and its partners could be slow to mobilize or even paralyzed, and their tools of economic statecraft will be weakened. The U.S. military has thus conducted dozens of overseas missions in the past few years to shore up allied infrastructure and gather insights to inform U.S. homeland defense.

While the U.S. government should prioritize, organize, and expand existing cyber defense programs, it should also address the next step in ally and partner capacity building: offensive cyber capabilities. While not all partners have the means or desire to conduct these operations, by refusing to begin to conceptualize how to help select allies and partners responsibly develop these capabilities, Washington is putting its partners and itself at risk. In the middle of a conflict, partners who want to use offensive cyber operations may turn to makeshift, volunteer offensive operators, as has occurred with the "Ukraine IT Army," if they do not have a professionally trained, accountable force, which takes years to develop.

This report concludes with recommendations for an organized, prioritized, and resourced effort to help embattled democratic U.S. allies and partners operate effectively in cyberspace.

1. **Make allied and partner cybersecurity capacity building a key element of the forthcoming international cybersecurity strategy.** The strategy should assess current activities and develop a plan of action to advance the administration's cyber strategy internationally and prioritize resources from both military and civilian U.S. agencies, remove redundancies, and close any seams.
2. **Prioritize building allied and partner cyber resilience in critical infrastructure**. Building cyber resilience of partner critical infrastructure — particularly ports, rail systems, and air transport systems — protects military mobility for both the host nation and U.S. forces. Other critical infrastructures — power, water, financial services, and pipelines — also undergird economic productivity.
3. **Provide additional funding for capacity building.** The Biden administration should request — and Congress should appropriate — additional funding to expand existing, successful cyber capacity-building efforts and create new ones. State and Defense capacity building should receive the lion's share of the increases.

7. Nathaniel Fick, "U.S. Leadership in Tech Diplomacy: A Conversation with Ambassador Nathaniel C. Fick," *Hudson Institute*, June 21, 2023. (https://www.hudson.org/events/us-leadership-tech-diplomacy-conversation-ambassador-nathaniel-c-fick)

Simultaneously, Congress should conduct increased oversight to ensure that authorized programs are getting the resources they require.

4. **Consolidate State Department cyber capacity-building funding under its Bureau of Cyberspace and Digital Policy**. Having been tasked with the international cyber strategy and given its existing work in traditional and non-traditional cyber capacity building, this bureau is best positioned to prioritize programs and funding.
5. **Conduct more bilateral and multilateral cyber exercises.** More military and civilian exercises are needed outside of the transatlantic theater. Washington should also explore replicating the annual U.S.-Israel cyber military exercise with other partners, including Taiwan, Japan, and South Korea.
6. **Selectively use bilateral memoranda of understanding (MOUs) to improve military cyber defense capabilities of American allies.** They should emphasize bilateral cybersecurity training, exercises, and joint operations to defend military networks, infrastructure, and systems.
7. **Develop offensive cyber force employment training capability**. The United States should develop and offer training events where U.S. operational, intelligence, and legal practitioners provide cyber-specific guidance on basic operational issues, including due diligence, sovereignty, collateral damage assessments, deconfliction with espionage operations, attribution techniques, and targeting processes.
8. **Assess future elements of offensive cyber force generation.** In preparation for a future in which today's operational, legal, and resource concerns are mitigated, the Department of Defense should study how best to build or support a partner's ability to conduct force generation for an offensive cyber capability and determine the resources required to execute such tasking.

Civilian Cyber Capacity-Building Programs

The Biden administration's National Cybersecurity Strategy envisions a world in which allies can secure critical systems, detect and respond effectively to incidents, share information, and pursue cyber diplomacy. While highlighting the State Department's unique role to coordinate whole-of-government efforts, the strategy commits the United States to "marshal[ling] expertise across agencies, the public and private sectors, and among advanced regional partners to pursue coordinated and effective international cyber capacity-building and operational collaboration efforts."[8]

Programs at civilian federal agencies currently focus on strengthening the ability of partners and allies to prevent attacks. With the rise of cryptocurrencies as an enabler of criminal activity, the U.S. government has launched complementary efforts on illicit finance and counter-ransomware.

Separately, the U.S. government also helps partners expand digital connectivity and modernize information technology as part of economic development initiatives.[9] This is not traditional capacity building as Washington

8. The White House, "National Cybersecurity Strategy," March 2023, page 31. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

9. See, for example: U.S. Department of State, Foreign Operations, and Related Programs, "Fiscal Year 2023 Congressional Budget Justification," April 2022, page 83. (https://www.usaid.gov/sites/default/files/2022-05/FY2023-Congressional-Budget-Justification.pdf); The White House, "FACT SHEET: New Initiative on Digital Transformation with Africa (DTA)," December 14, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta)

defines it,[10] but it is relevant because such activities advance norms around free and open internet and bolster cyber resilience. Washington also assists allies with incident response.

Building Cyber Resilience Through Preventive Capabilities

Cyber capacity-building programs at the departments of State, Justice, Energy, and Homeland Security strengthen partner nations' information-sharing capabilities, national policies, and adherence to international norms and standards. These departments, along with the FBI and Secret Service, also provide training and technical assistance to thwart cybercrime or investigate and prosecute it.[11]

Information-sharing efforts focus on improving the global sharing of technical information. The State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) encourages multilateral and bilateral relationships to share cybercrime information. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) hosts the U.S. government's Cybersecurity Incident Response Teams and works with global counterparts to share technical information about malware and emerging threats.[12] CISA and the FBI often also jointly distribute advisories with other U.S. agencies and partner nations.[13]

In developing national cyber strategies, State's new Bureau of Cyberspace and Digital Policy (CDP) takes the lead.[14] INL and the Department of Justice also help partners update national policies and strategies. While that work can be duplicative, INL and Justice also provide legal and legislative guidance on how to prosecute cybercrimes and protect intellectual property.[15]

State's CDP further promotes international norms and represents U.S. interests in multilateral and bilateral cyber summits. CDP is also playing an increasingly important role in an often-overlooked area of international collaboration: establishing transparent, rules-based policies at standards setting organizations. Together, Washington and its partners can ensure technical standards bodies advance a free and open internet rather than authoritarian goals that prioritize state control over human rights.[16] Robust diplomatic efforts secured the election of qualified leaders at the World Intellectual Property Organization in 2020 and the International Telecommunications Union in September 2022.[17] The latter effort became more organized after the creation of the CDP in April 2022.

10. Capacity building is an overarching term for programs that help strengthen a partner's abilities. Foreign assistance programs, meanwhile, help another country perform a task but may or may not strengthen the partner's ability to perform the task without assistance. The term security assistance is reserved for military and law enforcement programs. Capacity-building programs may or may not include foreign assistance and security assistance programs.

11. U.S. Government Accountability Office, "Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime," March 2023. (https://www.gao.gov/assets/gao-23-104768.pdf)

12. U.S. Department of Homeland Security, "Fact Sheet: DHS International Cybersecurity Efforts," April 21, 2022. (https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts)

13. See, for example: U.S. Federal Bureau of Investigation, Press Release, "U.S., U.K., and Australia Issue Joint Cybersecurity Advisory," July 28, 2021. (https://www.fbi.gov/news/press-releases/us-uk-and-australia-issue-joint-cybersecurity-advisory)

14. "Cyber Capacity Building," *U.S. Department of State*, accessed May 24, 2023. (https://www.state.gov/cyber-capacity-building)

15. U.S. Government Accountability Office, "Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime," March 2023, page 22. (https://www.gao.gov/assets/gao-23-104768.pdf)

16. Natalie Thompson and RADM (Ret.) Mark Montgomery, "Strengthening U.S. Engagement in International Standards Bodies," *Federation of American Scientists*, June 15, 2021. (https://fas.org/publication/strengthening-u-s-engagement-in-international-standards-bodies)

17. RADM (Ret.) Mark Montgomery and Ivana Stradner, "A Different Kind of Russian Threat — Seeking to Install Its Candidate Atop Telecommunications Standards Body," *Just Security*, September 28, 2022. (https://www.justsecurity.org/83286/a-different-kind-of-russian-threat-seeking-to-install-its-candidate-atop-telecommunications-standards-body)

After these successes, the importance of this collaboration has been getting fresh attention. The Biden administration included cooperation with private industry, academia, and foreign partners as a key objective in its May 2023 National Standards Strategy for Critical and Emerging Technology.[18] The strategy commits to enhancing U.S. and "like-minded nations' representation and influence in international standards governance and leadership."[19]

Outside of international standards bodies, CISA is also working with partners to develop technology standards so that products are engineered to be secure (by design) and include security features as standard rather than as add-on, premium features.[20] The goal is to increase critical infrastructure and societal cyber resilience by shifting the cybersecurity burden from the end user to large technology companies.

To further enhance cyber diplomacy and norm development, the State Department (led by CDP) is training its diplomats with the goal of having a cyber and digital officer in every embassy by the end of next year.[21] This could be transformational. Even though some foreign service officers have some cyber knowledge, and the Department of Homeland Security (DHS) has attachés in more than 60 countries,[22] embassies have generally been able to pay only limited attention to cyber missions. Amplifying foreign service and DHS efforts are the FBI's cyber assistant legal attachés who train local law enforcement and play an important role in intelligence sharing and joint law enforcement operations in more than a dozen European countries, Israel, South Korea, and Taiwan.[23]

The FBI's cyber attaché program is just one piece of Washington's robust international training and technical assistance programs. CISA offers industrial control systems trainings as well as tabletop and incident response exercises to U.S. industry, state and local governments, and international partners.[24] The Department of Energy offers cybersecurity technical training programs to the U.S. private sector and international partners through its national laboratories.[25] The Department of Energy is also developing exchanges and training through the Partnership for Transatlantic Energy and Climate Cooperation.[26] The Department of Justice's Criminal Division,

18. The White House, "FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology," May 4, 2023. (https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology)

19. The White House, "United States Government National Standards Strategy for Critical and Emerging Technology," May 2023, page 10. (https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf)

20. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches," April 13, 2023. (https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches)

21. Jory Heckman, "State Dept cyber bureau plans to add tech experts to every embassy by next year," *Federal News Network*, April 12, 2023. (https://federalnewsnetwork.com/cybersecurity/2023/04/state-dept-cyber-bureau-plans-to-add-tech-experts-to-every-embassy-by-next-year)

22. U.S. Department of Homeland Security, "Fact Sheet: DHS International Cybersecurity Efforts," April 21, 2022. (https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts)

23. U.S. Federal Bureau of Investigation, Press Release, "National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners," October 26, 2016. (https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners)

24. U.S. Department of Homeland Security, "Fact Sheet: DHS International Cybersecurity Efforts," April 21, 2022. (https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts); "CISA International," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed May 24, 2023. (https://www.cisa.gov/resources-tools/programs/cisa-international); "CISA Tabletop Exercise Packages," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed May 24, 2023. (https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages)

25. "Cybersecurity Investigation training from Department of Energy National Laboratories," *Cyber Fire*, accessed May 24, 2023. (https://cyberfire.training)

26. Billy Mitchell, "With a new National Cyber Strategy, Department of Energy looks to boost cyber support for US allies," *FedScoop*, March 3, 2023. (https://fedscoop.com/energy-department-national-cyber-strategy)

meanwhile, works with partners to prosecute criminal cases and trains counterparts on cyber investigations.[27] The U.S. Secret Service trains foreign partners on digital forensics, cyber-enabled financial crime investigations, and cryptocurrency tracing.[28] These and other law enforcement programs are distinct from incident response assistance in the wake of a specific crime. The training enhances the ability of partners to conduct investigations with or without U.S. personnel on the ground.

State and Justice also co-manage the Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) of attorneys, computer forensic analysts, and law enforcement agents who conduct training on cyber investigations and evidence collection. GLEN currently has attorneys in 12 countries around the world.[29]

Shortcomings in Civilian Federal Agency Programs

A Government Accountability Office (GAO) assessment of U.S. cyber capacity-building programs at State, Justice, and Homeland Security urged a comprehensive evaluation of the programs to determine overall impact and effectiveness.[30] Despite the creation of CDP and its responsibility for many (non-law enforcement related) cyber capacity-building programs, much of the funding still comes from regional programs, like assistance to Eastern Europe, the Economic Support Fund programs in East Asia and the Pacific, and United States Agency for International Development (USAID) programs.[31] As a result, decisions about where to conduct cyber capacity building are driven by regional considerations that may not account for global, cyber-specific insights. Offices make programmatic decisions independently without coordinating with other departments, countries, or the private sector. This contrasts with the National Security Council's more effective efforts to achieve interagency alignment on the deployment of trusted infrastructure (discussed below) with about 20 priority countries.

To address GAO's recommendation, the State Department must assess how to identify and expand successful programs and strategically deploy limited capacity-building resources. Ambassador Nathaniel Fick noted that "demand for capacity building around the world is just overwhelming," exceeding the government's ability to deliver.[32] Fick highlighted the need for a dedicated cyber assistance fund overseen by the CDP and additional authorities and "autonomy" to move faster to respond to the changing threat landscape.

27. Justice Department training is conducted in partnership with the State Department. U.S. Government Accountability Office, "Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime," March 2023, page 14. (https://www.gao.gov/assets/gao-23-104768.pdf)
28. U.S. Department of Homeland Security, "Fact Sheet: DHS International Cybersecurity Efforts," April 21, 2022. (https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts)
29. U.S. Government Accountability Office, "Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime," March 2023, page 14. (https://www.gao.gov/assets/gao-23-104768.pdf)
30. Ibid.
31. The president's budget request for fiscal year 2024 contains nearly $400 million for cyber and digital development initiatives, including those within USAID and the State Department. The White House, "FACT SHEET: President Biden's Budget Keeps America Safe and Confronts Global Challenges," March 9, 2023. (https://www.whitehouse.gov/omb/briefing-room/2023/03/09/fact-sheet-president-bidens-budget-keeps-america-safe-and-confronts-global-challenges); Department of State, Foreign Operations, and Related Programs, "Fiscal Year 2024 Congressional Budget Justification," April 26, 2023. (https://www.state.gov/fy-2024-international-affairs-budget)
32. Nathaniel Fick, "U.S. Leadership in Tech Diplomacy: A Conversation with Ambassador Nathaniel C. Fick," *Hudson Institute*, June 21, 2023. (https://www.hudson.org/events/us-leadership-tech-diplomacy-conversation-ambassador-nathaniel-c-fick)

Illicit Finance and Counter-Ransomware Efforts

In addition to these long-standing programs, the Biden administration launched global efforts to combat cyber-enabled illicit finance and ransomware, most notably the multilateral Counter Ransomware Initiative.[33] Among other capacity-building efforts, member nations have committed to develop tools to aid public-private collaboration and to sharing lessons about proactively combating ransomware threats.[34] Members have also used the initiative to kickstart regional cyber resilience efforts.[35]

Alongside the first Counter Ransomware summit in October 2021, the Treasury Department also announced a bilateral partnership with Israel to "disrupt the ransomware business model" as well as improve information sharing, technical exchanges, and cybersecurity and anti-money laundering exercises.[36] About a month later, Israel hosted a multilateral, virtual tabletop simulating a major cyberattack on the global financial system. With treasury officials from 10 countries and participants from intergovernmental financial institutions, the exercise focused primarily on monetary policy responses,[37] but this type of exercise improves the coordination critical to cyber incident response writ large. At the end of April 2023, the U.S. Treasury and the Monetary Authority of Singapore similarly conducted an exercise simulating cyberattacks on their banks.[38]

More recently, the Internal Revenue Service launched a pilot program sending cyber attachés to Australia, Columbia, Germany, and Singapore to help improve partners' ability to combat financial crimes utilizing cryptocurrencies.[39] The new initiative aims to improve counter-ransomware capabilities, given cybercriminals' heavy reliance on cryptocurrencies for ransom payments.

Incident Response and Recovery Assistance

While U.S. cyber capacity-building programs aim to help partners become resilient against cyberattacks, Washington also deploys resources when foreign countries fall victim. The Biden administration's National

33. The White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," October 14, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021)
34. The White House, "FACT SHEET: The Second International Counter Ransomware Initiative Summit," November 1, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit)
35. Jonathan Greig, "Neuberger: Counter Ransomware Initiative focused on 'expanding the tent,' with Jordan, Costa Rica, Colombia joining," *The Record*, May 7, 2023. (https://therecord.media/counter-ransomware-initiative-expands-neuberger)
36. Annie Fixler and Enia Krivine, "Washington and Jerusalem Enhance Cooperation to Counter Ransomware," *Foundation for Defense of Democracies*, November 17, 2021. (https://www.fdd.org/analysis/2021/11/17/washington-jerusalem-enhance-cooperation-ransomware)
37. Steven Scheer, "IMF, 10 countries simulate cyberattack on global financial system," *Reuters*, December 9, 2021. (https://www.reuters.com/markets/europe/exclusive-imf-10-countries-simulate-cyber-attack-global-financial-system-2021-12-09)
38. U.S. Department of the Treasury, Press Release, "US Treasury and Monetary Authority of Singapore Conduct Joint Exercise to Strengthen Cross-Border Cyber Incident Coordination and Crisis Management," May 1, 2023. (https://home.treasury.gov/news/press-releases/jy1455). Two years earlier, the countries signed a memorandum of understanding on cybersecurity cooperation, pledging to expand training and "competency-building activities." U.S. Department of the Treasury, Press Release, "The United States Department of the Treasury and the Monetary Authority of Singapore Finalize a Memorandum of Understanding on Cybersecurity Cooperation," August 23, 2021. (https://home.treasury.gov/news/press-releases/jy0331)
39. U.S. Internal Revenue Service, Press Release, "IRS-CI deploys 4 cyber attachés to locations abroad to combat cybercrime," May 18, 2023. (https://www.irs.gov/compliance/criminal-investigation/irs-ci-deploys-4-cyber-attaches-to-locations-abroad-to-combat-cybercrime); Lorenzo Franceschi-Bicchierai, "The IRS is sending four investigators across the world to fight cybercrime," *TechCrunch*, April 21, 2023. (https://techcrunch.com/2023/04/21/the-irs-is-sending-four-investigators-across-the-world-to-fight-cybercrime)

Cybersecurity Strategy notes that this is one way Washington can "expose counter-normative state behavior and impose consequences" on adversaries.[40]

Domestically and internationally, the FBI leads investigations into cyber incidents. The bureau deploys cyber action teams internationally to help investigate crimes and then shares technical details, as appropriate, with interagency partners and the public to help defenders identify similar deficiencies in their own systems.

The FBI deployed a cyber team to Montenegro last summer after a ransomware attack disrupted government services and electricity distribution.[41] When the Albanian government suffered a devastating cyberattack in July 2022, the FBI, along with Microsoft, helped conduct forensic investigations to determine the culprit.[42] After the United States, Albania, and NATO partners publicly attributed the attack to Iran, the FBI and CISA issued a public advisory on how to avoid similar attacks.[43] Cyber Command subsequently helped Albania further harden its systems.[44]

Between July 2022 and February 2023, U.S. cybersecurity experts were continuously deployed to investigate the attack and bolster Albanian cybersecurity, Yuri Kim, U.S. ambassador to Albania, revealed in February.[45] She also confirmed a $50 million security assistance package, including $25 million "in direct response to Iran's attacks."

In addition to the FBI, the U.S. Secret Service works with allies and partners to investigate and prosecute cyber-enabled financial crimes. The Secret Service has an attaché detailed to the Joint Cybercrime Action Taskforce at Europol's European Cyber Crime Center at The Hague.[46]

Such law enforcement partnerships are indispensable for arresting cyber criminals,[47] dismantling ransomware network infrastructure,[48] and deactivating Russian malware.[49] And yet, the adage "an ounce of prevention is worth a pound of cure" continues to resonate in cyberspace. While the Department of Defense requested $62 million for

40. The White House, "National Cybersecurity Strategy," March 2023, page 31. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)
41. France also dispatched a team to assist. AJ Vicens, "Another European nation hit by hackers, Montenegro grapples with ongoing ransomware attack," *CyberScoop*, September 2, 2022. (https://cyberscoop.com/montenegro-ransomware-attack)
42. Llazar Semini, "Albania cuts diplomatic ties with Iran over July cyberattack," *Associated Press*, September 7, 2022. (https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a)
43. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," September 23, 2022. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a)
44. Martin Matishak, "Iran-linked incidents spurred Cyber Command to send 'hunt forward' team to Albania," *The Record*, March 23, 2023. (https://therecord.media/iran-albania-cyber-command-hunt-forward)
45. Ambassador Yuri Kim, "Cyber Security Challenges in Albania," *Conference Remarks*, February 7, 2023. (https://al.usembassy.gov/remarks-by-u-s-ambassador-yuri-kim-at-the-cyber-security-challenges-in-albania-conference)
46. U.S. Department of Homeland Security, "Fact Sheet: DHS International Cybersecurity Efforts," April 21, 2022. (https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts)
47. Europol, Press Release, "Bitzlato: senior management arrested," January 23, 2023. (https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested)
48. Tonya Riley, "FBI seizes Hive ransomware group infrastructure after lurking in servers for months," *CyberScoop*, January 26, 2023. (https://cyberscoop.com/fbi-europol-hive-ransomware-group)
49. U.S. Attorney's Office for the Eastern District of New York, Press Release, "Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service," May 9, 2023. (https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network)

the 2024 fiscal year for all its hunt forward operations,[50] the State Department committed $25 million to Costa Rica alone after ransomware attacks severely disrupted daily life and the government declared a state of emergency.[51]

Other incident response capabilities, however, lack speed and agility. Pending bipartisan legislation would rectify the problems that prevented CISA from quickly providing cybersecurity support to Ukraine in the wake of the Russian invasion.[52] CDP's proposed cyber assistance fund also aims to help allies and partners faster.

Unfortunately, Washington has not yet prioritized helping other countries develop attribution capabilities as part of incident response assistance. While the United States often attributes attacks through joint statements with partners and allies,[53] there are no attribution standards or mechanisms for sharing the intelligence and technical analysis.[54] Capacity building in this area would likely necessitate enhanced cyber forensic investigative training and sharing U.S. intelligence on adversarial tactics. To the extent that public attribution is a political question and not a technical challenge, Washington will need to convince partners that technically grounded, prompt, and multilateral attribution is a prerequisite for joint diplomatic and economic efforts to hold aggressors accountable.[55]

Non-Traditional Areas: Secure ICT, Digital Connectivity, and Research and Development

Alongside efforts to build partner resilience by building preventative, defensive capabilities, Washington helps allies and partners build secure and reliable digital infrastructure. Partners thus avoid insecure telecommunications equipment through which adversarial nations can compromise critical infrastructure.[56] Digital infrastructure policy is also intertwined with cybersecurity (and cyber capacity-building priorities) because some countries fear cyberattacks if they choose non-Chinese telecommunications suppliers.

50. U.S. Department of Defense, "Defense Budget Overview, Fiscal Year 2024 Budget Request," March 2023, page 31. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf)

51. U.S. Embassy in Costa Rica, Press Release, "United States Announces $25 Million to Strengthen Costa Rica's Cybersecurity," March 29, 2023. (https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity); "Costa Rica, 'under assault' is a troubling test case on ransomware attacks," *Associated Press*, June 17, 2022. (https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083)

52. Senate Homeland Security and Government Affairs Committee, Press Release, "Peters & Lankford Introduce Bipartisan Bill to Strengthen American Cybersecurity Partnerships With International Partners and Allies to Prevent Attacks," June 7, 2023. (https://www.hsgac.senate.gov/media/dems/peters-lankford-introduce-bipartisan-bill-to-strengthen-american-cybersecurity-partnerships-with-international-partners-and-allies-to-prevent-attacks)

53. See, for example: The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china); Joe Uchill, "UK, US and EU attribute Viasat hack against Ukraine to Russia," *SC Magazine*, May 10, 2022. (https://www.scmagazine.com/analysis/threat-intelligence/uk-us-and-eu-attribute-viasat-hack-against-ukraine-to-russia); Sergiu Gatlan, "US sanctions Iran's Ministry of Intelligence over Albania cyberattack," *Bleeping Computer*, September 9, 2022. (https://www.bleepingcomputer.com/news/security/us-sanctions-iran-s-ministry-of-intelligence-over-albania-cyberattack)

54. Georgianna Shea, "U.S. Leads International Efforts to Attribute China's Microsoft Hack," *Foundation for Defense of Democracies*, July 29, 2021. (https://www.fdd.org/analysis/2021/07/29/us-leads-efforts-chinas-microsoft-hack)

55. James Andrew Lewis, "Creating Accountability for Global Cyber Norms," *Center for Strategic and International Studies*, February 23, 2022. (https://www.csis.org/analysis/creating-accountability-global-cyber-norms)

56. Suzanne Smalley, "State Department needs more cyber policy muscle, says cyberspace ambassador nominee," *CyberScoop*, August 3, 2022. (https://cyberscoop.com/cyber-ambassador-state-dept-more-power-cybersecurity)

The Trump administration launched "The Clean Network" initiative,[57] highlighting the danger of embedding Chinese telecommunications equipment in critical partner networks because of the Chinese Communist Party's malign activities. The Biden administration replaced this effort with a "Declaration for the Future of the Internet," signed by 60 allies and partners.[58] While the declaration does not mention China, it commits to "promot[ing] and us[ing] trustworthy network infrastructure and services suppliers."[59] CDP is also working to convince partners and allies to shun Chinese telecommunications equipment. In early June, for example, Ambassador Fick offered U.S. and European Union (EU) commitments to finance secure 5G infrastructure in Costa Rica.[60]

The Trump administration also launched — and the Biden administration has expanded — the Digital Connectivity and Cybersecurity Partnership (DCCP) initiative.[61] Chaired by USAID and the State Department, the interagency initiative encourages foreign countries to purchase secure information and communication technology (ICT) infrastructure, including U.S. goods and services.[62] Its programs help create regulatory frameworks, provide technical assistance (including by embedding experts in host country ministries), and raise cybersecurity awareness among foreign government, industry, and civil society stakeholders. DCCP works primarily in Southeast and South Asia but will also "promote an open, interoperable, reliable, and secure digital ecosystem" as part of the White House's new Digital Transformation with Africa initiative.[63]

Last year, as part of the CHIPS and Science Act, Congress appropriated $100 million per year for five years for a new State Department fund to support the development of secure ICT.[64] The budget requests funding to expand international partners' critical minerals production and ICT manufacturing. This collaboration, while not traditional capacity building, helps secure U.S. and partner digital infrastructure against supply chain disruptions and adversarial attacks.

The U.S. government also promotes secure digital infrastructure through bilateral and multilateral research and development initiatives. More than 15 years ago, Congress established DHS's International Cooperative Programs Office to foster research and development partnerships on a wide range of homeland security issues.[65] Among these partnerships is the Israel-U.S. Binational Industrial Research and Development (BIRD) Cyber program. Announced in June 2022 as an outgrowth of nearly 50 years of bilateral, cooperative research and development,

57. "The Clean Network," *U.S. Department of State*, accessed May 24, 2023. (https://2017-2021.state.gov/the-clean-network/index.html)
58. The White House, "FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet," April 28, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet)
59. The White House, "A Declaration for the Future of the Internet," April 2022, page 2. (https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf)
60. John Sakellariadis, "Ahead of LatAm swing, Nate Fick looks to Beijing," *Politico Morning Cybersecurity*, June 5, 2023. (https://subscriber.politicopro.com/newsletter/2023/06/ahead-of-latam-swing-nate-fick-looks-to-beijing-00100166)
61. "Digital Connectivity and Cybersecurity Partnership (DCCP)," *United States Agency for International Development*, accessed May 24, 2023. (https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership)
62. Komal Bazaz Smith, "USAID Activities under the Digital Connectivity and Cybersecurity Partnership," *Presentation for the Community Showcase Hour at GFCE*, September 2022. (https://thegfce.org/wp-content/uploads/2022/10/DCCP-Presentation-For-GFCE-September-2022.pdf)
63. The White House, "FACT SHEET: New Initiative on Digital Transformation with Africa (DTA)," December 14, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta)
64. The new fund is called the International Technology Security and Innovation Fund. Department of State, Foreign Operations, and Related Programs, "Fiscal Year 2024 Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement," April 26, 2023, page 79. (https://www.state.gov/wp-content/uploads/2023/04/FY-2024-CBJ-Appendix-1-Full-Document-25-April-2023.pdf)
65. "International Partnerships," *U.S. Department of Homeland Security, Science and Technology Directorate*, accessed May 24, 2023. (https://www.dhs.gov/science-and-technology/st-icpo)

this effort will "promote the collaborative development of technologies" to "enhance the cyber resilience of critical infrastructure in the United States and Israel."[66]

Cyber Abraham Accords: An Opportunity for Regional Capacity Building

In September 2020, the Trump administration brokered a series of normalization agreements between Israel and its Arab neighbors known as the Abraham Accords. The administration has recently sought ways to increase their impact. To that end, in February 2023, DHS Under Secretary for Policy Robert Silvers announced the expansion of the accords to include cybersecurity cooperation.[67]

Middle Eastern states face similar cyber threats from Iran and its terrorist proxies. They are thus well positioned to work together and alongside the United States to combat these threats and improve cyber resilience, particularly as it relates to military mobility (especially given U.S. military basing in the region), critical infrastructure protection, and cyber-enabled disinformation. For example, as part of the Counter Ransomware Initiative, Israel and the United Arab Emirates (UAE) developed a new information-sharing platform. UAE cyber chief Muhammad al-Kuwaiti also revealed in June that Israel helped his country repel a cyberattack.[68]

Washington sees potential for tabletop exercises and other cyber capacity building beyond information sharing.[69] Pending bipartisan legislation would codify existing information sharing and authorize technical support, joint training, and exercises.[70]

Military Cyber Defense Capacity-Building Programs

Separate but complementary to the federal civilian agency programs, the DoD conducts extensive, well-resourced cyber capacity-building efforts. Most well-known among these are Cyber Command's hunt forward operations, where U.S. servicemembers engage in defensive cyber operations alongside host nation personnel. Combatant command-assigned forces and National Guard forces conduct military-to-military engagements. And DoD

66. U.S. Department of Homeland Security, Science and Technology Directorate, Press Release, "DHS and Israeli Partners Announce Collaboration on Cybersecurity," June 30, 2022. (https://www.dhs.gov/science-and-technology/news/2022/06/30/dhs-and-israeli-partners-announce-collaboration-cybersecurity); "About BIRD," *Israel-U.S. Binational Industrial Research and Development Foundation*, accessed May 24, 2023. (https://www.birdf.com/what-is-bird)

67. U.S. Department of Homeland Security, Press Release, "DHS Expands Abraham Accords to Cybersecurity," February 2, 2023. (https://www.dhs.gov/news/2023/02/02/dhs-expands-abraham-accords-cybersecurity)

68. Annie Fixler and Cole Knie, "Cooperation Between Israel and Its Neighbors Can Defeat Shared Cyber Threats," *Foundation for Defense of Democracies*, July 5, 2023. (https://www.fdd.org/analysis/2023/07/05/cooperation-between-israel-and-its-neighbors-can-defeat-shared-cyber-threats)

69. Tim Starks and Ellen Nakashima, "The Abraham Accords expand with cybersecurity collaboration," *The Washington Post*, January 31, 2023. (https://www.washingtonpost.com/politics/2023/01/31/abraham-accords-expand-with-cybersecurity-collaboration). Washington and Jerusalem have a strong foundation upon which to build this multilateral cooperation. In addition to BIRD Cyber and the Abraham Accords efforts, the two countries signed an MOU in March 2022 to increase information and intelligence sharing, exercises, and research and development on aviation and surface transportation cybersecurity. U.S. Department of Homeland Security, "Joint Statement of Intent Between the U.S. Department of Homeland Security and the Israel National Cyber Directorate," March 2, 2022. (https://www.dhs.gov/news/2022/03/02/joint-statement-intent-between-us-department-homeland-security-and-israel-national)

70. Barak Ravid, "New bill aims to boost cybersecurity cooperation between U.S., Abraham Accords nations," *Axios*, May 31, 2023. (https://www.axios.com/2023/05/31/bill-cybersecurity-cooperation-abraham-accords-nations)

provides resources through the Foreign Military Financing (FMF) program, conducts bilateral and multilateral military exercises, and, in limited cases, executes free-standing bilateral cybersecurity partnerships through MOUs.

Cyber Command and Hunt Forward Operations

Cyber Command's hunt forward operations are overseas deployments in which U.S. Cyber National Mission Force personnel engage in defensive operations alongside host nation personnel to detect and evict malicious actors from the host's networks. At the invitation of a foreign partner, the deployments can involve up to 30 servicemembers and last a couple of months.[71] When properly planned and executed, hunt forward operations can not only help a partner secure its networks but transition to helping the partner become more self-sufficient.

Hunt forward operations bring U.S. operators "closer to adversary activity," noted Major General William J. Hartman, commander of the Cyber Command's Cyber National Mission Force, helping America "better understand and then defend" itself.[72] The missions result in "the mass inoculation of millions of systems" against adversarial attacks, Cyber Commander Gen. Paul Nakasone explained.[73] And they help build relationships between U.S. and foreign personnel.[74]

Over the past five years, Cyber Command has conducted more than 47 missions in more than 20 countries, with the pace picking up significantly over the past two years.[75] Many deployments have been to Eastern and Central Europe. Earlier this year, Cyber Command completed its first hunt forward mission in Latin America.[76]

In addition to securing foreign partners, these missions bolster U.S. security by "exposing adversary tactics, techniques, and procedures before they can be used against the United States," according to Cyber Command.[77] Hunt forward operations in Montenegro in October 2019, for example, yielded information relevant to foreign

71. For more information, see also: Dina Temple-Raston, "Q&A with Gen. Hartman: 'There are always hunt forward teams deployed,'" *The Record*, June 20, 2023. (https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here)

72. U.S. Cyber Command, Press Release, "'Committed Partners in Cyberspace': Following cyberattack, US conducts first defensive Hunt Operation in Albania," March 23, 2023. (https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens)

73. Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020. (https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity)

74. U.S. Cyber Command, Press Release, "'Partnership in Action': Croatian, U.S. cyber defenders hunting for malicious actors," August 18, 2022. (https://www.cybercom.mil/Media/News/Article/3131961/partnership-in-action-croatian-us-cyber-defenders-hunting-for-malicious-actors)

75. Cyber Command conducted nine overseas operations in 2021, seven between May and August of 2022, and another 12 over the past six months. Martin Matishak, "US, Canada sent cyber experts to Latvia to bolster digital defenses," *The Record*, May 10, 2023. (https://therecord.media/latvia-hunt-forward-cyber-command-canada); Suzanne Smalley, "Nakasone says Cyber Command did nine 'hunt forward' ops last year, including in Ukraine," *CyberScoop*, May 4, 2022. (https://cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine); "U.S. Cyber National Mission Force Conducts First Hunt Forward Operation in Lithuania," *Homeland Security Today*, May 8, 2022. (https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-cyber-national-mission-force-conducts-first-hunt-forward-operation-in-lithuania)

76. Colin Demarest, "US cyber experts sent to Latin America on 'hunt-forward' mission," *C4ISRNet*, June 9, 2023. (https://www.c4isrnet.com/cyber/2023/06/09/us-cyber-experts-sent-to-latin-america-on-hunt-forward-mission)

77. U.S. Cyber Command Public Affairs, "CYBER 101: Hunt Forward Operations," November 15, 2022. (https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations)

interference in U.S. elections.[78] Multiple hunt forward operations the following year also contributed to efforts to protect the presidential election from foreign interference. Major General Hartman specifically highlighted the discovery of Iranian election interference while on a hunt forward operation.[79]

In 2021, after the discovery of a multi-year Russian cyber espionage operation, Cyber Command and CISA conducted a joint hunt forward operation at a victim's request.[80] The U.S. team helped the partner find Russian malicious activity, evict the hackers from the network, and prevent them from re-infecting the system, all "without the adversary having any idea" of Cyber Command's involvement, according to Hartman.[81] The mission uncovered virus samples that Washington then shared publicly so that other network defenders could bolster their own systems.[82]

In early May 2023, Cyber Command completed its first hunt forward mission conducted in conjunction with Canadian Forces. Together in Riga, personnel from the three countries worked to harden Latvian infrastructure.[83]

Military-to-Military Support Programs

The geographic combatant commanders organize and execute bilateral military-to-military capacity-building programs, utilizing resources from across the defense enterprise. In the cyber realm, these programs include cyber subject matter expert trainings,[84] contractor supported on-site training, and leadership courses, training, and mentoring programs on policy and strategy execution. The George C. Marshall European Center for Security Studies in Germany hosts a three-week-long cybersecurity studies course with students from more than 50 countries, and the DoD Cyber Crime Center hosts a five-week cyber forensics course.[85]

The State Partner Program (SPP) also contributes to military-to-military efforts. The U.S. National Guard runs the SPP, pairing individual state guard programs with a specific partner country based on specific skills the receiving

78. Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020. (https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity). See also a discussion of Cyber Command's deployments to Ukraine and North Macedonia prior to the 2018 midterm elections: Shannon Vavra, "Pentagon again deploying cyber personnel abroad to gather intel for 2020 elections," *CyberScoop*, November 1, 2019. (https://cyberscoop.com/pentagon-deploying-cyber-personnel-abroad-gather-intel-2020-elections)

79. Joseph Menn, "Iran gained access to election results website in 2020, military reveals," *The Washington Post*, April 24, 2023. (https://www.washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking)

80. U.S. Cyber Command, Press Release, "US Cyber Command, DHS-CISA release Russian malware samples tied to SolarWinds compromise," April 15, 2021. (https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co)

81. Dina Temple-Raston, "Q&A with Gen. Hartman: 'There are always hunt forward teams deployed,'" *The Record*, June 20, 2023. (https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here)

82. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Malware Analysis Report, "MAR-10327841-1.v1 — SUNSHUTTLE," April 15, 2021. (https://www.cisa.gov/news-events/analysis-reports/ar21-105a)

83. U.S. Cyber Command, Press Release, "'Shared threats, shared understanding': U.S., Canada and Latvia conclude defensive Hunt Operations," May 10, 2023. (https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun)

84. These training events and courses take place locally and at regional or U.S. training sites.

85. David Vergun, DOD News, "DoD CTA Aims to Arm Students with Essential Cybersecurity Skills," October 14, 2022. (https://dodcio.defense.gov/In-the-News/News-Display/Article/3267523/dod-cyber-training-academy-aims-to-arm-students-with-essential-cybersecurity-to)

country requires.[86] For example, Maryland has one of the most comprehensive state guard cyber programs — not surprising given that the National Security Agency is located in Maryland. Maryland is paired with Estonia, one of the most cyber-savvy NATO allies.[87] Only 20 states, however, have an organic cyber capacity embedded in their guard and can routinely provide cyber-specific security assistance.

In a more direct form of assistance, the Defense Security Cooperation Agency sometimes embeds cyber advisors in foreign defense ministries as part of its Ministry of Defense Advisors Program.

Because training and other capacity-building resources are scarce, geographic combatant commands prioritize and align resources based on partner capacity, regional needs, and the risk to U.S. force mobilization and maneuver.[88] Based on the assessment, the combatant commands determine where to deploy service component forces, Cyber Command forces, National Guard forces, bilateral or multilateral cyber exercises, cyber classroom activities, and FMF programs.

Not all efforts are applicable or appropriate for every ally or partner. Some countries may be too wealthy for U.S.-funded training. Others may not have a cyber-capable state guard paired with them through the SPP.

NATO partners, meanwhile, may receive a great deal of partner capacity-building assistance from the alliance as part of the accession process. Once they have formally joined NATO, however, this alliance-provisioned funding ceases. It can be a significant problem for newly joined NATO members facing Russian cyberattacks if bilateral military-to-military programs do not immediately fill this gap.

Foreign Military Financing

The State Department's FMF program provides grants for U.S. allies and partners to acquire U.S. defense services, training, and equipment. Most FMF funds are used to buy armored vehicles, munitions, vessels, aircraft, and other equipment. In the cyber realm, FMF funds pay for training, mentoring programs, contractor support, and exercise participation. It is often the funding source for the DoD programs mentioned in this report.

Annually, a portion of FMF funds is used for the Countering Russian Influence Fund and the Countering the People's Republic of China Influence Funds.[89] This year's budget request includes $350 million in FMF for equipment and training in Europe and Eurasia, a small percentage of which will go towards "cyber and information domain projects."[90] For example, Montenegro used FMF funds to add two cyber consultants to its Ministry of Defense.[91]

86. This SPP was developed 30 years ago to help coordinate and execute security assistance programs with former Warsaw Pact and Soviet states. "State Partnership Program," *U.S. National Guard Bureau*, accessed June 25, 2023, (https://www.nationalguard.mil/leadership/joint-staff/j-5/international-affairs-division/state-partnership-program)

87. Christopher Schepers, "Maryland Airman, Estonia Build Cyber Sharing Platform," *Air National Guard*, June 21, 2023. (https://www.ang.af.mil/Media/Article-Display/Article/3434815/maryland-airmen-estonia-build-cyber-sharing-platform)

88. Jim Hansis, "ECJ6/JCC Security Cooperation Engagement Strategy," U.S. European Command Headquarters, October 2020, (https://community.apan.org/cfs-file/__key/docpreview-s/00-00-14-88-27/ECJ6-Cyber-Security-Cooperation-Overview.pdf)

89. U.S. Congress, "Joint Explanatory Statement, Division K-Department Of State, Foreign Operations, And Related Programs Appropriations Act, 2023," December 2022, pages 75 and 90. (https://www.appropriations.senate.gov/imo/media/doc/Division%20K%20-%20SFOPS%20Statement%20FY23.pdf)

90. Department of State, Foreign Operations, and Related Programs, "Fiscal Year 2024 Congressional Budget Justification," April 26, 2023, page 161. (https://www.state.gov/wp-content/uploads/2023/06/508-compliant-FY-2024-CBJ_FINAL_4.26.2023.pdf) This request mirrored the prior year's. See: U.S. Department of State, Foreign Operations, and Related Programs, "Fiscal Year 2023 Congressional Budget Justification," May 2022, page 138. (https://www.usaid.gov/sites/default/files/2022-05/FY2023-Congressional-Budget-Justification.pdf)

91. "US and Montenegro Armies Strengthen Security Cooperation Relationship," *Military Leak*, August 5, 2021. (https://militaryleak.com/2021/08/05/us-and-montenegro-armies-strengthen-security-cooperation-relationship)

The Czech Republic is using $6 million in FMF funds to create a Deployable Cyber Response Center.[92] In both cases, Russian cyber threats were the driving force.

FMF funds have played a critical part in U.S. efforts to support Ukraine after Russia's invasion. The January 2023 announcement of another $3.75 billion in military assistance for Ukraine, for example, included nearly $700 million in FMF funds for European partners to backfill materiel stocks they had donated to Ukraine and strengthen cyber defense.[93] A prior package in September 2022 included $1.2 billion in FMF funds for Central and Eastern Europe and Baltic states to strengthen capabilities including cyber defense capabilities to counter Russia.[94] While they are a small percentage of the funds, cyber capacity-building expenditures are proving effective.

Military Cyber Exercises

Bilateral and multilateral cyber exercises are a core component of cyber defense capacity building. Annually, Cyber Command hosts a multinational exercise called CYBER FLAG "to enhance readiness and interoperability by exercising collaboration through realistic defensive cyberspace training."[95] Cyber defense teams detect and mitigate simulated attacks, while Cyber Command hosts briefings on information sharing and regional threats. The most recent exercise, conducted in November 2022, included 250 participants from eight countries. For the first time, the exercises included partners from the Pacific theater.

Cyber Command also conducts bilateral cyber defense exercises, like the annual Cyber Dome with the Israel Defense Forces (IDF).[96] In the exercise, teams of intelligence and cyber personnel react to complex, realistic scenarios simulating nation-state-level threats.[97]

The United States also participates in NATO's annual Cyber Coalition exercise in Tallinn, Estonia (which also houses NATO's Cyber Range).[98] It is one of the largest cyber defense exercises in the world, with about a hundred experts and operators participating in person and another 900 participants joining remotely.[99] In December, 26 NATO allies plus Finland, Sweden, Georgia, Ireland, Japan, Switzerland, and the European Union, as well as industry and academic experts, participated. The exercise simulated a sophisticated adversary attempting to compromise

92. U.S. Embassy in the Czech Republic, Press Release, "United States Announces $106 Million in Military Financing for Czech Republic," September 29, 2022. (https://cz.usembassy.gov/united-states-announces-106-million-in-military-financing-for-czech-republic)
93. Secretary of State Antony J. Blinken, Press Statement, "More Than $3.75 Billion in U.S. Military Assistance to Ukraine and Countries Impacted by Russia's Brutal War," January 6, 2023. (https://www.state.gov/more-than-3-75-billion-in-u-s-military-assistance-to-ukraine-and-countries-impacted-by-russias-brutal-war)
94. Joe Gould and Sebastian Sprenger, "US unveils $2B in military aid for Europe, arms for Ukraine," *Defense News*, September 8, 2022. (https://www.defensenews.com/pentagon/2022/09/08/us-unveils-2b-in-military-aid-for-europe-arms-for-ukraine)
95. U.S. Cyber Command, Press Release, "CYBERCOM concludes CYBER FLAG 23 exercise," November 4, 2022. (https://www.cybercom.mil/Media/News/Article/3209896/cybercom-concludes-cyber-flag-23-exercise)
96. Israel Defense Forces, Press Release, "IDF and U.S. Cyber Command Complete Cyber Dome Exercise," December 9, 2022. (https://www.idf.il/en/articles/2022/idf-and-u-s-cyber-command-complete-cyber-dome-exercise)
97. U.S. Army, Press Release, "U.S., Israeli cyber forces build partnership, interoperability during exercise Cyber Dome VII," December 8, 2022. (https://www.army.mil/article/262622/u_s_israeli_cyber_forces_build_partnership_interoperability_during_exercise_cyber_dome_vii); Emanuel Fabian, "IDF Cyber Defense unit holds drill with US Cyber Command," *The Times of Israel* (Israel), December 9, 2022. (https://www.timesofisrael.com/idf-cyber-defense-unit-holds-drill-with-us-cyber-command-2)
98. "Cyber Coalition," *North Atlantic Treaty Organization, Allied Command Transformation*, accessed May 24, 2023. (https://www.act.nato.int/cyber-coalition)
99. Maggie Miller, "NATO prepares for cyber war," *Politico*, December 3, 2022. (https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060)

a NATO mission using cyber operations to help "prepare cyber defenders for real-life cyber challenges, including attacks on critical infrastructure as well as disruption of NATO and allied assets while in operations," NATO said.[100]

In addition, NATO hosts an annual Coalition Warrior Interoperability Exercise.[101] While not explicitly a cyber exercise, participants address interoperability for cyber operations and practice jointly detecting and responding to cyber incidents.[102]

NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE) in Tallinn, Estonia, also conducts its own annual cyber defense exercise, Locked Shields.[103] The exercise is larger than Cyber Coalition, boasting 3,000 participants from 38 countries during its last iteration in April.[104] Whereas Cyber Coalition is a collaborative exercise, Locked Shields is a competitive red-blue exercise in which the game creators serve as the attackers in a simulation.[105] Participants compete against each other to see who can best repel a large-scale attack — combining technical skills, strategic decision-making, and crisis communications.[106] CCDCOE also hosts an annual red team exercise, Crossed Swords, which includes technical and leadership training relevant to "planning and executing a full-spectrum cyber operation."[107]

Bilateral Cybersecurity Cooperation Agreements

The United States develops bilateral cybersecurity cooperation with select allies — usually countries facing specific threats or that host U.S. forces. Cooperation includes bilateral cybersecurity training activities and exercises and other joint operations to defend military systems and eradicate malicious cyber activity. Some agreements deploy commercial and military cybersecurity technology and services to harden and defend networks and infrastructure. Pursuant to an agreement with the Kingdom of Jordan, the United States helped establish a regional cybersecurity center. Because these agreements require extensive effort by both Cyber Command and the relevant geographic combatant command, only a limited number of them can be undertaken simultaneously.

Cyber Capacity-Building Efforts by International Partners

Some U.S. allies and partners have their own mature, effective cyber capacity-building efforts. These efforts include those of larger organizations, such as NATO and the European Union, as well as those of individual countries.

Cyber capacity building is a priority for NATO members. As far back as the 2014 Wales summit, NATO affirmed that cyber defense is part of collective defense and that the alliance would incorporate cyber defense into its

100. North Atlantic Treaty Organization, Allied Command Transformation, Press Release, "Exercise Cyber Coalition 2022 Concludes in Estonia," December 2, 2022. (https://www.nato.int/cps/en/natohq/news_209972.htm)
101. North Atlantic Treaty Organization, Joint Force Training Center, Press Release, "CWIX 2022 poised to deliver a more interoperable, innovative Alliance. Major NATO Interoperability Testing Event in Poland," June 16, 2022. (https://www.jftc.nato.int/articles/cwix-2022)
102. "Exercises," *The NATO Cooperative Cyber Defence Center of Excellence*, accessed May 24, 2023. (https://ccdcoe.org/exercises)
103. "Locked Shields," *The NATO Cooperative Cyber Defence Center of Excellence*, accessed May 24, 2023. (https://ccdcoe.org/exercises/locked-shields)
104. NATO Cooperative Cyber Defence Center of Excellence, Press Release, "World's largest cyber defense exercise Locked Shields brings together over 3000 participants," accessed May 24, 2023. (https://ccdcoe.org/news/2023/6016)
105. North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe, Press Release, "Exercise Locked Shields 2022 Concludes," April 23, 2023. (https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes)
106. "Locked Shields," *The NATO Cooperative Cyber Defence Center of Excellence*, accessed May 24, 2023. (https://ccdcoe.org/exercises/locked-shields)
107. "Crossed Swords," *The NATO Cooperative Cyber Defence Center of Excellence*, accessed May 24, 2023. (https://ccdcoe.org/exercises/crossed-swords)

planning and operations.[108] In 2016, NATO members pledged to improve their cyber defenses through training, education, exercises, and information sharing.[109] The June 2022 Strategic Concept pledges to "boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security."[110] Most recently, the July Vilnius Summit Communiqué pledged that cyber defense will be a larger part of the alliance's deterrence posture and announced a new initiative to improve incident response assistance to members.[111] Alongside the summit, NATO announced new partnerships with South Korea and Japan on cybersecurity and other issues.[112]

NATO academies, meanwhile, provide cyber-defense training for operators and strategic decision makers.[113] The NATO CCDCOE offers strategic, legal, operational, and technical trainings. For the past five years, the center has been "responsible for identifying and coordinating education and training solutions in cyber defence" for NATO allies and partners, having been tasked as such by NATO strategic command.[114]

For its part, the European Union has recognized for at least the last decade the importance of the cybersecurity of its members and partner capacity building.[115] The EU's cybersecurity strategies have repeatedly highlighted this as a key pillar. The most recent strategy, released in December 2020, commits the EU to increasing partner capacity building and developing a cyber capacity-building agenda.[116] A year prior, Brussels founded the EU CyberNet to help EU members and other partners find the right experts for their training and advising needs. EU CyberNet is also building an information-sharing platform and a curriculum to "train the trainers" for cybersecurity awareness.[117] Over the decade, EU investment in capacity building has increased ten-fold (although the figure is a fraction of what the United States spends on civilian programs). With the increased investment, the EU has expanded its programs to include strategic partnerships on cyber norms and ICT standards.[118]

Meanwhile, the World Bank has incorporated cybersecurity into its development efforts. While all countries struggle with cybersecurity investments and workforce development, the bank determined that the way that low-

108. North Atlantic Treaty Organization, "Wales Summit Declaration," September 5, 2014. (https://www.nato.int/cps/en/natohq/official_texts_112964.htm)
109. North Atlantic Treaty Organization, "Cyber Defence Pledge," July 8, 2016. (https://www.nato.int/cps/en/natohq/official_texts_133177.htm)
110. North Atlantic Treaty Organization, "NATO 2022 Strategic Concept," June 29, 2022, page 8. (https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf)
111. North Atlantic Treaty Organization, "Vilnius Summit Communiqué," July 11, 2023. (https://www.nato.int/cps/en/natolive/official_texts_217320.htm); Alexander Martin, "NATO allies' new cyber pledges to remain classified — but here's what we know," *The Record*, July 12, 2023. (https://therecord.media/nato-new-cyber-pledges-remain-classified-here-is-what-we-know)
112. Sakura Murakami and Kentaro Sugiyama, "Japan and NATO agree on new partnership programme at NATO Vilnius summit, *Reuters*, July 12, 2023. (https://www.reuters.com/world/japan-nato-agree-new-partnership-programme-nato-vilnius-summit-2023-07-12); North Atlantic Treaty Organization, Press Release, "Secretary General welcomes NATO's deepening partnership with South Korea," July 11, 2023. (https://www.nato.int/cps/en/natohq/news_217034.htm)
113. "Cyber defence," *North Atlantic Treaty Organization*, last updated June 22, 2023. (https://www.nato.int/cps/en/natohq/topics_78170.htm)
114. "Training," *The NATO Cooperative Cyber Defence Center of Excellence*, accessed May 24, 2023. (https://ccdcoe.org/training)
115. "About project," *EU CyberNet*, accessed May 24, 2023. (https://www.eucybernet.eu/about-project)
116. European Commission, Press Release, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," December 16, 2020. (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391)
117. "Project deliverables," *EU CyberNet*, accessed May 24, 2023. (https://www.eucybernet.eu/project-deliverables)
118. Robert Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," *European Union Institute for Security Studies*, September 2021, pages 56- 57. (https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf)

and middle-income economies fund cybersecurity is "neither feasible nor sustainable."[119] In 2016, the World Bank launched its Global Cybersecurity Capacity Program, piloting cybersecurity awareness and technical training in Albania, Bosnia and Herzegovina, North Macedonia, Ghana, Kyrgyzstan, and Burma.[120] After initial successes, the program expanded,[121] and the World Bank launched a Cybersecurity Multi-Donor Trust Fund.[122]

Australia and Japan also have bilateral and multilateral cyber capacity-building programs in Asia. Australia's programs focus on government, industry, academia, and civil society partnerships in Southeast Asia and the Pacific. Over the past two years, Canberra expanded its efforts to include cooperation on critical technologies.[123] Japan, meanwhile, conducts tabletop exercises, workshops, and trainings with ASEAN members.[124] These countries provide an example of how more cyber-mature nations can help elevate the defenses of regional partners.

The Role of the Private Sector

Cybersecurity and technology companies provide a vast amount of the goods and services that serve a nation's cyber resilience. In addition to the products these companies offer, an increasing number of for-profit companies and nonprofit organizations, like the Cyber Readiness Institute, offer free or heavily discounted services to help small businesses, underserved populations, civil society organizations, and countries.[125] The Cyber Defense Assistance Collaborative has pulled together many of these resources to align capacity-building needs and private sector capabilities.[126] The Global Forum on Cyber Expertise has similar clearinghouses.[127]

To close the cyber workforce gap globally, private companies are also offering free cybersecurity training. Microsoft, for example, partners with global and local organizations to train cyber educators and to encourage more women

119. Francesca Spidalieri and Anat Lewin, "Enabling cyber resilient development," *The World Bank's Digital Development blog*, January 18, 2023. (https://blogs.worldbank.org/digital-development/enabling-cyber-resilient-development)
120. "Global Cybersecurity Capacity Program: Lessons Learned and Recommendations towards strengthening the Program," *The World Bank*, 2019. (https://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf)
121. "Global Cyber Security Capacity Program Phase I and II: Strengthening national Cyber Security Environment of Selected Developing Countries," *The World Bank*, June 1, 2020. (https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp)
122. The World Bank, Press Release, "World Bank and Partners Announce New Global Fund for Cybersecurity," August 16, 2021. (https://www.worldbank.org/en/news/press-release/2021/08/16/world-bank-and-partners-announce-new-global-fund-for-cybersecurity)
123. "Capacity Building," *Australian Department of Foreign Affairs and Trade*, accessed May 24, 2023. (https://www.internationalcybertech.gov.au/our-work/capacity-building)
124. "Japan's Major Capacity Building Projects for Developing Countries (As of Dec 2021)," *Japanese Ministry of Foreign Affairs*, accessed May 24, 2023. (https://www.mofa.go.jp/files/100347811.pdf)
125. "Cyber Readiness Institute," *Cyber Readiness Institute*, accessed May 24, 2023. (https://cyberreadinessinstitute.org); "Our Work," *CyberPeace Institute*, accessed May 24, 2023. (https://cyberpeaceinstitute.org/our-work); "Project Galileo," *Cloudflare*, accessed May 24, 2023. (https://www.cloudflare.com/galileo). On its website, CISA offers a list of more than 100 free commercial and open-source tools to reduce vulnerabilities, improve detection and response capabilities, and strengthen resilience. "Free Cybersecurity Services and Tools," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed May 24, 2023. (https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools)
126. Greg Rattray, Geoff Brown, and Robert Taj Moore, "The Cyber Defense Assistance Imperative: Lessons From Ukraine," *The Aspen Institute*, February 2023. (https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf)
127. "The GFCE," *Global Forum on Cyber Expertise*, accessed July 12, 2023. (https://thegfce.org)

to join the field.[128] The World Economic Forum also offers free training in partnership with Salesforce, Fortinet, and the Global Cyber Alliance.[129]

These private initiatives complement rather than replicate U.S. government efforts. They do not directly address the ability of governments to protect their citizens, implement national strategies, and prosecute cyber criminals, but private companies are often crucial to identifying cyber threats and remediating attacks, as demonstrated repeatedly during the war in Ukraine. Recognizing this, CDP is seeking to broker arrangements between private companies and international partners who have suffered attacks.[130]

Ukraine: A Case Study in Successful Capacity Building

After the Russian cyberattack on Ukraine's electric grid in December 2015, Washington dispatched an interagency team of industrial control system and incident response experts to assist with remediation and forensic analysis.[131] Based on what the response team learned, the Department of Energy developed (and continues to run) a specialized training for energy infrastructure operators to understand how to mitigate the kind of attacks Kyiv suffered.[132] While U.S.-Ukrainian energy security collaboration predated the 2015 attack,[133] it accelerated in September 2017 with the first U.S.-Ukraine Bilateral Cyber Dialogue. Washington announced new cyber assistance funds for Ukraine and efforts to improve "cybersecurity policy structures and cyber incident response procedures."[134]

Over the next five years, the U.S. government provided Ukraine with more than $40 million in cyber assistance. Through a USAID grant program, Washington embedded technical experts within the Ukrainian government to help strengthen laws and regulations and expand university cyber courses for workforce development. The program also deployed hardware and software to bolster Ukraine's incident response and recovery capabilities.[135]

The U.S. Treasury Department, meanwhile, worked with the National Bank of Ukraine to improve cyber information sharing with its financial sector. This initiative and the Department of Energy's long-standing collaboration increased in the lead-up to Russia's February 2022 invasion.[136] Cyber threat information sharing with the FBI and CISA also escalated in the run up to the invasion, helping Ukrainian defenders thwart Russian operations.[137]

128. Kate Behncken, "Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries," *Microsoft*, March 23, 2022. (https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries)
129. "Delivering free and globally accessible cybersecurity training," *World Economic Forum*, accessed May 24, 2023. (https://www.weforum.org/impact/cybersecurity-training)
130. John Sakellariadis, "State Department sets sights on international cyber strategy," *Politico Morning Cybersecurity*, April 7, 2023. (https://subscriber.politicopro.com/newsletter/2023/04/state-department-sets-sights-on-international-cyber-strategy-00090940)
131. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," July 20, 2021. (https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01)
132. Idaho National Laboratory, "INL CyberStrike," *YouTube*, May 28, 2019. (https://www.youtube.com/watch?v=ZvMf5eHg89s)
133. U.S. Department of State, Fact Sheet, "Energy Security Support to Ukraine," November 29, 2022. (https://www.state.gov/energy-security-support-to-ukraine); "U.S.-Ukraine Energy Cooperation," *U.S. Department of Energy, Office of International Affairs*, accessed May 24, 2023. (https://www.energy.gov/ia/us-ukraine-energy-cooperation)
134. U.S. Embassy in Ukraine, Press Release, "Embassy Statement on the First US-Ukraine Bilateral Cyber Dialogue," September 29, 2017. (https://ua.usembassy.gov/embassy-statement-first-us-ukraine-bilateral-cyber-dialogue)
135. U.S. Department of State, Fact Sheet, "U.S. Support for Connectivity and Cybersecurity in Ukraine," May 10, 2022. (https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine)
136. Ibid
137. In July 2022, CISA announced an expansion of its bilateral collaboration. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Press Release, "United States and Ukraine Expand Cooperation on Cybersecurity," July 27, 2022. (https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity)

On the military side, beginning in 2017, the U.S. Army funded a joint cybersecurity, command and control, and information system for the Ukrainian Ministry of Defense[138] to help transition Ukrainian infrastructure from old Russian systems. At the time, U.S. officials warned that the older, Russian equipment "may have back doors that the Russians are aware of."[139] Within three years, the U.S. Army transitioned operational responsibility of the system to Ukraine.[140]

A decisive piece in the capacity building was Cyber Command's December 2021 hunt forward mission in Ukraine. Alongside other European partners,[141] more than three dozen U.S. servicemembers (the largest team ever deployed) spent months in Ukraine — supported remotely with additional personnel conducting analytical and advisory activities.[142] Cyber Command revealed that U.S. personnel were in-country "when Russia began executing destructive cyber-attacks in mid-January."[143] Working with Ukrainian counterparts, U.S. operators identified Russian intrusions and prevented crippling cyberattacks.

Since the war began, U.S. government cyber assistance has only expanded. The FBI is sharing threat information and investigative methods, disrupting disinformation campaigns, and helping Ukraine procure network defense tools.[144] USAID is providing technical experts and emergency communications equipment. The Department of Energy is helping Ukraine implement cyber resilience standards so its electric grid can be integrated into Europe's. And CISA and Cyber Command are exchanging technical information. During the annual U.S.-Ukraine Cyber Dialogue in June, the State Department affirmed that the White House is "working with Congress to deliver an additional $37 million in cyber assistance to Ukraine, which would bring the total to $82 million since February 2022, and over $120 million since 2016."[145]

Meanwhile, U.S. allies have also provided indispensable cybersecurity support. In 2021, the EU launched efforts to help Ukraine strengthen cybersecurity laws. In the lead-up to the war, the United Kingdom provided intelligence briefings on Russian cyber operations. After February 2022, the EU deployed a team to help with threat detection and has provided about $31 million in cybersecurity assistance.[146]

138. Loren Blinde, "US Army selects Black Box for Ukraine Security Assistance Initiative-Information Technology (USAI-IT)," *Intelligence Community News*, February 7, 2017. (https://intelligencecommunitynews.com/us-army-selects-black-box-for-ukraine-security-assistance-initiative-information-technology-usai-it)

139. "Ukrainian cybersecurity slowed by need to replace Soviet-era tech," *Fifth Domain*, March 30, 2017. (https://www.c4isrnet.com/home/2017/03/30/ukrainian-cybersecurity-slowed-by-need-to-replace-soviet-era-tech)

140. "ASA(ALT) at work: Program Executive Office for Enterprise Information Systems (PEO EIS)," *U.S. Army AL&T Magazine*, July 26, 2019. (https://www.army.mil/article/225052/asaalt_at_work_program_executive_office_for_enterprise_information_systems_peo_eis)

141. Ines Kagubare, "US, EU cyber investments in Ukraine pay off amid war," *The Hill*, March 13, 2022. (https://thehill.com/policy/technology/597921-us-eu-cyber-investments-in-ukraine-pay-off-amid-war); David Vergun, "Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say," *DOD News*, December 3, 2022. (https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say)

142. Gordon Corera, "Inside a US military cyber team's defence of Ukraine," *BBC News* (UK), October 30, 2022. (https://www.bbc.com/news/uk-63328398)

143. U.S. Cyber Command, Press Release, "Before the Invasion: Hunt Forward Operations in Ukraine," November 28, 2022. (https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine)

144. U.S. Department of State, Fact Sheet, "U.S. Support for Connectivity and Cybersecurity in Ukraine," May 10, 2022. (https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine)

145. U.S. Department of State, Media Note, "Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue," June 5, 2023. (https://www.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue)

146. James Andrew Lewis and Georgia Wood, "Evolving Cyber Operations and Capabilities," *Center for Strategic and International Studies*, May 18, 2023, page 17. (https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities)

Private U.S. cybersecurity and technology companies have also contributed to Ukraine's defense in a "powerful way," noted former Google CEO Eric Schmidt.[147] Some of these companies had (and continue to have) contracts with Ukrainian government and private sector entities to provide network defense.[148] These companies blunted Russian attacks by updating systems "at scale in near real time, based on collaboration with the U.S. intelligence community," according to Ambassador Fick.[149] As the war began, Microsoft, Cisco Talos, and others thwarted Russian malware targeting Ukrainian government networks.[150] And in the weeks preceding and immediately following the invasion, Kyiv worked with Microsoft and Amazon to shepherd its critical data to cloud platforms hosted outside the country.[151]

Joanna LaHaie, CDP's acting director of international engagement and capacity building, noted that the private companies moved much more rapidly than government actors.[152] Some companies donated equipment and product licenses.[153] Others provided threat intelligence and monitoring services. In still other cases, the U.S. government subsidized the licenses and training by private companies.[154] Nearly a dozen private companies joined together to provide cybersecurity assistance services.[155]

Together with allies and industry, the United States helped Ukraine harden its defenses against cyber aggression. Ukraine remains in peril, but cyber capacity building has worked.

Conceptualizing Offensive Cyber Capacity Building

Until now, U.S. cyber capacity-building programs have focused almost exclusively on cyber defense. As U.S. partners become more capable in cyberspace, they will begin to reach a threshold where they could successfully conduct offensive operations.[156] Washington will need to ask itself a simple question: would it not be better if we collaborated with our partners rather than letting them independently develop new capabilities where their mistakes or miscalculations could risk wider conflict and loss of human life?

147. Eric Schmidt, "Thinking Forward After the NSCAI and CSC: A Discussion on AI and Cyber Policy," *Foundation for Defense of Democracies*, June 7, 2023. (https://www.fdd.org/events/2023/06/07/thinking-forward-after-the-nscai-and-csc)
148. Tom Burt, "Malware attacks targeting Ukraine government," *Microsoft*, January 15, 2022. (https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government)
149. Chris Riotta, "U.S. cyberspace ambassador lays out technology's role in geopolitical contests," *Nextgov/FCW*, February 2, 2023. (https://fcw.com/security/2023/02/us-cyberspace-ambassador-lays-out-technologys-role-geopolitical-contests/382538)
150. James Andrew Lewis and Georgia Wood, "Evolving Cyber Operations and Capabilities," *Center for Strategic and International Studies*, May 18, 2023, pages 26-27. (https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities)
151. Ryan White, "How the cloud saved Ukraine's data from Russian attacks," *C4ISRNET*, June 22, 2022. (https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks); Russ Mitchell, "How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia," *The Los Angeles Times*, December 15, 2022. (https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data)
152. Joanna LaHaie, "The Private Sector's Evolving Role in Conflict—From Cyber Assistance to Intelligence," *R Street*, June 13, 2023. (https://www.rstreet.org/events/the-private-sectors-evolving-role-in-conflict)
153. Kent Walker, "New ways we're supporting Ukraine," *Google*, December 1, 2022. (https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine)
154. AJ Vicens, "IRS gives Ukraine tools to expose Russian oligarchs hiding riches in crypto exchanges," *CyberScoop*, May 11, 2023. (https://cyberscoop.com/irs-gives-ukraine-tools-to-expose-russian-oligarchs-hiding-riches-in-crypto-exchanges)
155. CRDF Global, Press Release, "CRDF Global becomes Platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine," November 14, 2022. (https://www.prnewswire.com/news-releases/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-301676373.html)
156. A country's decision to use offensive cyber operations will no doubt have to consider the target's possible responses and whether it has sufficient defenses to thwart a potential counterattack.

The risks of ignoring the issue have already materialized in Ukraine. Prior to the war, despite significant investments in national resilience against cyberattacks, the Ukrainian armed forces lacked a dedicated offensive cyber capability. When the war started, the Ministry of Defense quickly recruited a volunteer, mostly civilian "IT Army" to disrupt Russian government assets online. While this may have been a propaganda victory, its impact has been limited.[157] Moreover, the use of a volunteer force comes with risks. These operators lack a broader view of the operational and strategic battlefield and thus may inadvertently hinder a Ukrainian military effort or provoke Russian escalation.

Relying on NATO to provide persistent offensive capacity building is not feasible. Only a few countries — Denmark, France, the Netherlands, the United Kingdom, and the United States — acknowledge having offensive cyber capabilities. NATO policy for addressing national offensive cyber contributions, the Sovereign Cyber Effects Provided Voluntarily by Allies, ensures only the nation contributing the offensive cyber capabilities knows the details of those capabilities.[158] This mechanism is fundamentally different from how NATO operates in other domains where weapons systems are integrated into alliance planning and operations mechanisms.

Some partners and allies may decide to refrain from conducting offensive operations, the same way some partners choose not to field certain weapons systems, such as fighter aircraft or submarines. Many countries have eschewed the development of offensive cyber capabilities for legal, technical, financial, or other reasons. Some countries may be comfortable relying on an equipped ally or partner like the United States. Others, however, are likely to see offensive cyber operations as a necessary tool for deterring or punishing adversaries. Having determined offensive cyber capabilities are necessary for their national security, these countries will pursue the capabilities with or without U.S. assistance.

Effective offensive cyber operations take years of personnel training and infrastructure, tool, and organizational development. Offensive capacity building, therefore, is not about selling computer viruses and zero-day exploits to every country willing to buy. Rather, it involves judiciously enhancing the ability of select partners and allies to develop the people and tools to observe adversarial tactics, thwart attacks before they occur, and rapidly respond to emerging conflicts.

How Offensive Cyber Operations Are Used

The purpose of offensive cyber operations is to gain access, pursue adversaries where they operate, and deliver effects against the adversary when warranted. The cyber domain is dynamic; opportunities are often short-lived, and adversaries are agile and adaptive. Therefore, countries often use offensive cyber operations to gain situational awareness and provide early warning for defenders. Operators observe adversary tactics then deploy countermeasures to thwart or mitigate them.

Offensive operations can also counter an adversary's own cyber capabilities, dismantle the infrastructure that supports adversarial campaigns, and force adversaries to shift to alternate targets and divert resources. The United States calls this "defending forward," with U.S. operators persistently engaging the adversary and "defending

157. Joe Tidy, "Meet the hacker armies on Ukraine's cyber front line," *BBC News* (UK), April 15, 2023. (https://www.bbc.com/news/technology-65250356). For a more in-depth examination of the "IT Army" and its evolving role, see: James Andrew Lewis and Georgia Wood, "Evolving Cyber Operations and Capabilities," *Center for Strategic and International Studies*, May 18, 2023, pages 10-12. (https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities)

158. Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA): The Devil is in the Kilobyte," *Cyber Defense Magazine*, November 11, 2019. (https://www.cyberdefensemagazine.com/sovereign-cyber)

against malicious cyberspace activities as far forward as possible," General Nakasone testified to Congress.[159] Ahead of the 2018 midterm elections, Cyber Command reportedly blocked a Russian troll farm from interfering in the election.[160] Prior to the 2020 presidential elections, U.S. Cyber Command conducted more than two dozen operations to prevent foreign interference.[161] Without offensive cyber capabilities, countries have less situational awareness about adversarial capabilities and are less able to prevent and thwart attacks.

Offensive cyber capabilities provide another option for rapidly responding to emerging geopolitical situations. Offensive cyber operations can provide decision makers with "cyber options" to support crisis bargaining and responses that are independent of existing cyber campaign plans. Public information about this kind of highly classified operation is limited. Reportedly, Cyber Command disabled the internet access of North Korea's military spy agency in 2017.[162] In 2019, Cyber Command reportedly carried out cyberattacks twice in response to Iranian interference with international shipping and proxy attacks on Saudi oil fields.[163]

In conflict, offensive cyber operations can deliver a direct strike, or they can amplify, enable, or enhance kinetic strikes with non-kinetic cyber effects. Offensive cyber capabilities are important for placing adversary command and control networks at risk and enabling long-range strikes into heavily defended areas, two challenging missions for kinetic effects alone.

Potential Components of Offensive Capacity Building

Preparations for the use of cyber forces, as with any military forces, involves force generation (building the force in question) and force employment (how one utilizes that force in operations). While force generation is the process of creating a capability, force employment is the process of utilizing, sustaining, and deploying a capability in routine operations, crisis, and combat. It allows the force employer to develop a wide range of options and quickly deploy capabilities for emerging requirements while maintaining readiness to respond to contingencies.[164] In the United States, the force employer for offensive cyber operations is Cyber Command.

In many other domains, the United States assists partners with both force generation and force employment. Even in cyber defense capability development, Washington does the same. For offensive cyber operations, assistance with force generation may be possible, but as an initial matter, assistance with force employment is more feasible in the short and medium term.

159. Gen. Paul Nakasone, *Statement before the Senate Committee on Armed Services*, February 14, 2019. (https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf)
160. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, February 27, 2019. (https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html)
161. Mark Pomerleau, "US military conducted 2 dozen cyber operations to head off 2020 election meddling," *C4ISRNET*, March 25, 2021. (https://www.c4isrnet.com/cyber/2021/03/25/us-military-conducted-2-dozen-cyber-operations-to-head-off-2020-election-meddling)
162. Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump signed presidential directive ordering actions to pressure North Korea," *The Washington Post*, September 30, 2017. (https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html)
163. Ellen Nakashima and Paul Sonne, "U.S. military carried out secret cyberstrike on Iran to prevent it from interfering with shipping," *The Washington Post*, August 28, 2019. (https://www.washingtonpost.com/national-security/us-military-carried-out-secret-cyber-strike-on-iran-to-prevent-it-from-interfering-with-shipping/2019/08/28/36202a4e-c9db-11e9-a1fe-ca46e8d573c0_story.html); Idrees Ali and Phil Stewart, "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials," *Reuters*, October 16, 2019. (https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK)
164. Force employment largely utilizes the "organizational" element of both the DOTMLPF and PETIO models.

In force generation, required resources are produced to provide an operational commander with the necessary capabilities at the right scale and readiness to accomplish the task. The United States has historically viewed force generation through the DOTMLPF model: Doctrine (the way to fight); Organization (how to organize to fight); Training (both individual and unit level training up to large-scale exercises); Materiel (the equipment the forces need); Leadership and education (preparing soldiers to lead the fight from squad leader to general); Personnel (recruitment of qualified personnel); and Facilities (installations and infrastructure that support the forces). Cyber scholar Max Smeets has developed a cyber-specific model he calls PETIO: Personnel (both recruitment and training); Exploits (the vulnerabilities that will be taken advantage of); Tools (the computer programs used to support operations); Infrastructure (the processes and structures used to support operations); and Organization (structures used to conduct operations).[165]

If an ally or partner were to ask for assistance with force generation, the request is most likely to be in the personnel and training areas. Smeets identifies 15 specialties requiring offensive cyber-specific training. (This includes not just operators but other personnel like lawyers.) This number of specialties expands significantly, however, with the disaggregation of functional job descriptions (such as "vulnerability analyst") into specific technologies and skill sets. Currently, the U.S. service schools' offensive cyber curriculum is long and challenging, with a high dropout rate.

U.S. military services each conduct cyber force generation and are already operating at maximum capacity. In fact, Cyber Command recently had to readjust its planned force expansion because of the U.S. Navy's inability to meet readiness requirements.[166] Washington may not overtly offer force generation support in part because its services barely have the bandwidth to man, train, and equip the forces they are required to generate for Cyber Command.

That said, if the United States were to provide allies with force generation support, offensive cyber-specific personnel training would be a logical first step. The United States could help establish the intake, initial training, and specialty training. U.S. military services could establish "train the trainer" models where they provide a notional curriculum, work with a handful of high-proficiency partner servicemembers, help the partner build its own school, and then continuously assess progress. This tasking would be challenging, however, as it draws on a personnel training system already under duress. Nevertheless, U.S. special forces have successfully used this model.

Cooperation in the development of exploits, tools, and infrastructure is even more complicated. The U.S. military services and Cyber Command are responsible for this work, and there is little excess bandwidth for partner capacity building. Beyond that, sharing exploits and tools is complicated for operational, legal, and risk assessment reasons. Smeets and others have referred to this aspect of force development as "arms transfers." In addition to the usual risks in arms transfers in other domains, transferring "cyber weapons" carries the risk that adversaries will more easily compromise the tools or development techniques once the United States is not the sole holder of that information. There could also be unintended collateral damage when an ally or partner uses an exploit.

Given all these challenges, mentions of offensive cyber operations in a training or exercising environment with allies and partners likely refer only to America demonstrating its ability to impose cyber effects in the exercise or training rather than any effort to build the offensive cyber capabilities of its partners.

There are more opportunities, however, for offensive cyber capacity building in the force employment process. Through classroom training, tabletop exercises, and operational exercises, U.S. operational and legal practitioners

165. Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022), chapter 5.
166. Martin Matishak, "Cyber Command reshuffles force expansion due to Navy readiness woes," *The Record*, June 14, 2023. (https://therecord.media/cyber-command-reshuffles-cyber-mission-force-due-to-navy-readiness-woes)

could provide cyber-specific guidance on basic legal issues such as due diligence, sovereignty, and jurisdiction as well as more complex operational issues such as collateral damage assessments, clarification on when states can "hack back," and when states can engage in self-defense. Intelligence practitioners could assist in deconfliction with espionage operations, developing timely and accurate attribution techniques and implementing a comprehensive targeting process.

Bandwidth issues in the force employment area are also less challenging than those for force generation. And the activities can be done in the United States or with alliance support organizations like NATO's CCDCOE.

The United States has spent the better part of two decades grappling with the policy decisions surrounding offensive cyber operations. The Defense Department has established doctrine about acceptable collateral damage in cyberspace. Even as the commander of Cyber Command is dual hatted as the head of the National Security Agency, Washington delineates between military operations and espionage operations both in practice and in law. America's democratic partners and allies — while each operating under unique legal regimes — will need to establish their own similar rules and could benefit from training on doctrinal development.

Conclusion and Recommendations

American cyber capacity-building efforts should promote and reinforce cyber resiliency of allies and partners to help maintain their warfighting capabilities, ensure the mobility of U.S. forces within the host nation, and support global economic productivity. While the United States needs allies and partners with more skilled cyber defenders, Washington also must begin thinking about training select partners and allies in elements of offensive cyber operations. The following recommendations outline how to meet these challenges.

1. **Make allied and partner cybersecurity capacity building a key element of the forthcoming international cybersecurity strategy.** As part of the National Defense Authorization Act (NDAA) for Fiscal Year 2023, Congress required the president to develop an international cyberspace and digital policy strategy to advance cyber norms, improve collaboration with allies and partners, and deter foreign threats.[167] The strategy is due to Congress in December 2023. It should align with the National Cybersecurity Strategy, the National Security Strategy, National Defense Strategy, and the Defense Cyber Strategy.

   Ambassador Fick confirmed that the Bureau of Cyberspace and Digital Policy is drafting the strategy in accordance with the statute.[168] He must ensure it examines more than just State Department equities. According to the congressional directive, the strategy should assess current activities and develop a plan of action for all departments to advance the administration's cyber strategy internationally. It should recognize Cyber Command hunt forward operations' importance to capacity building and strategic partnership building. And the strategy should prioritize resources from both military and civilian U.S. agencies, remove redundancies, and close any seams. It should also account for the role that cyber-developed allies and partners and the private sector will play. The State Department and its interagency partners must then follow through on an implementation plan that promotes partner cyber resiliency to support their warfighting capabilities, America's ability to maneuver forces across host nation battle space, and global economic productivity.

167. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 STAT. 3902, U.S.C §10302. (https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf)

168. John Sakellariadis, "State Department sets sights on international cyber strategy," *Politico Morning Cybersecurity*, April 7, 2023. (https://subscriber.politicopro.com/newsletter/2023/04/state-department-sets-sights-on-international-cyber-strategy-00090940)

2. **Prioritize building allied and partner cyber resilience in critical infrastructure**. Building cyber resilience of partner critical infrastructure — particularly ports, rail systems, and air transport systems — protects military mobility for both the host nation and U.S. forces. Other critical infrastructures — power, water, financial services, and pipelines — also undergird economic productivity. Capacity building should focus on critical infrastructure resilience, and priority should be given to countries whose infrastructure is most critical to U.S. force maneuver. CISA and sector risk management agencies have also developed programs, collaboration frameworks, and industry-specific guidance that partners could adapt rather than create anew.

3. **Provide additional funding for capacity building.** The Biden administration should request — and Congress should appropriate — additional funding to expand existing, successful cyber capacity-building efforts and create new ones. With more dedicated funds, Energy and DHS can provide more training and expand information-sharing initiatives. The FBI, meanwhile, needs more cyber assistant legal attachés.

   State and DoD capacity building should receive the lion's share of the increases. Ambassador Fick has stated that his bureau wants to create a dedicated fund for cyber, digital, and emerging technology assistance.[169] U.S. responses in Albania, Costa Rica, and elsewhere were too slow. The federal government must respond faster and with more agility and autonomy. Washington could draw lessons from changes to counterterrorism assistance after 9/11 for how to tackle endemic challenges. Fick also noted the bureau wants to scale capacity building and broker more relationships between cybersecurity companies and foreign partners. This will likely require more appropriations if not also additional authorizations from Congress. Fick has requested $250 million. This is a reasonable starting point, but the number may need to grow over time.

   As allies and partners see the benefits of hunt forward operations, Cyber Command will likely need more funding to conduct more missions, and the military services will need more resources to generate the forces. To the extent that some partners view the term "hunt" as implying aggressive actions, this expansion could be paired with a rebranding that more explicitly markets these deployments as capacity-building operations where U.S. personnel teach counterparts their techniques and leave behind some technology.

   Simultaneously, Congress should conduct increased oversight to ensure that authorized programs are getting the resources they require. For example, despite language in appropriations bills indicating congressional intent that the U.S.-Israel Cybersecurity Cooperation Grant Program and the Binational Industrial Research and Development (BIRD) be funded through DHS's Science and Technology Directorate, members of Congress are concerned these programs have not been resourced. Congress should ensure that the executive branch is using increased resources to develop stronger bilateral relationships between civilian agencies as well as military-to-military and intelligence community-to-intelligence community.

4. **Consolidate State Department cyber capacity-building funding under CDP**. Simply throwing more money at cyber capacity building is not a responsible way to spend taxpayer dollars. Having been tasked with drafting the international cyber strategy and given its existing work in traditional and non-traditional cyber capacity building, CDP is best positioned to prioritize programs and funding rather than the disparate regional bureaus. The Bureau of International Narcotics and Law Enforcement Affairs, however, should retain all funding related to law enforcement and legal cybersecurity training.

169. Elias Groll, "US plans to boost tech diplomats deployed to embassies," *CyberScoop*, April 12, 2023. (https://cyberscoop.com/fick-cyber-diplomats-embassies)

5. **Conduct more bilateral and multilateral cyber exercises.** Between Cyber Command exercises and NATO exercises, the United States and its partners have a robust schedule. More military and civilian exercises, however, are needed outside of the transatlantic theater. As Washington helps Abraham Accord signatories deepen their information sharing, it should explore tabletop exercises on shared threats. Washington should also explore replicating the annual U.S.-Israel cyber military exercise with other partners, including Taiwan, Japan, and South Korea. This will help strengthen military-to-military relationships.
6. **Selectively use bilateral MOUs to improve military cyber defense capabilities of American allies.** Last year's NDAA established a program to expand cooperation with Jordan on military cybersecurity activities.[170] Congress is considering a similar provision for Taiwan this year.[171] The bipartisan legislation, the Taiwan Cybersecurity Resiliency Act, directs the Defense Department to conduct training and exercises and leverage U.S. commercial and military technology to harden Taiwan's networks.[172] Bilateral MOUs tax resources across national security agencies. Where prospective partners (like Taiwan) are both critical to America's ability to maneuver forces and under duress from capable cyber adversaries, the effort is warranted. These MOUs should emphasize bilateral cybersecurity training, exercises, and joint operations to defend military networks, infrastructure, and systems. They can also deploy commercial and military cybersecurity technology and services to harden and defend networks.
7. **Develop offensive cyber force employment training capability**. The United States should develop and offer bilateral and multilateral training events for select partners and allies where U.S. operational, intelligence, and legal practitioners provide cyber-specific guidance on basic operational issues including (but not limited to) due diligence, sovereignty, collateral damage assessments, deconfliction with espionage operations, attribution techniques, and targeting processes. These force employment development opportunities could be delivered through classroom training or exercises and should leverage willing partners with cyber offensive experience. The effort may also be able to leverage the existing trainings at the NATO CCDCOE.
8. **Assess future elements of offensive cyber force generation.** There appears to be limited appetite today to build partner capacity to generate forces for offensive cyber operations. In preparation for a future in which existing operational, legal, and resource concerns are mitigated, however, the Department of Defense should pick a military service to study how to best build or support a partner's ability to conduct force generation for an offensive cyber capability and determine the resources required to execute such tasking.

***

The United States has a robust, if somewhat ad-hoc, program for supporting the cyber capacity-building needs of its allies and partners. Unfortunately, adversaries are continuously improving and developing new avenues of attack. Even non-state criminal actors can have serious national security impacts. As such, the United States needs to maintain or even increase its support for the cyber defense capabilities of its partners and allies and begin thinking about training them in elements of offensive cyber operations.

170. U.S. Senate Armed Services Committee, "Summary of the Fiscal Year 2023 National Defense Authorization Act," December 2022. (https://www.armed-services.senate.gov/imo/media/doc/fy23_ndaa_agreement_summary.pdf)
171. Bryant Harris, "House defense bill adds special Ukraine IG, Taiwan cyber cooperation," *Defense News*, June 22, 2023. (https://www.defensenews.com/congress/budget/2023/06/22/house-defense-bill-adds-special-ukraine-ig-taiwan-cyber-cooperation)
172. Taiwan Cybersecurity Resiliency Act of 2023, S.1241, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/senate-bill/1241)

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

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

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

FDD's Center on Military and Political Power (CMPP)

FDD's Center on Military and Political Power promotes understanding of the defense strategies, policies, and capabilities necessary to deter and defeat threats to the freedom, security, and prosperity of Americans and our allies, by providing rigorous, timely, and relevant research and analysis.

RADM (Ret.) Mark Montgomery serves as senior director of CCTI and directs CSC 2.0, an initiative to continue the work of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. **Annie Fixler** is the director of CCTI, contributing to the cyber-enabled economic warfare project and the Transformative Cyber Innovation Lab, and a research fellow at FDD.
