Air Force Staff Sergeant Joseph Peralta, 52nd Communications Squadron mission defense team supervisor, identifies indicator of network compromise during exercise Tacet Venari, at Ramstein Air Base, Germany, May 19, 2022 (U.S. Air Force/Jared Lovett)

Transparent Cyber Deterrence

By Ryan Tate

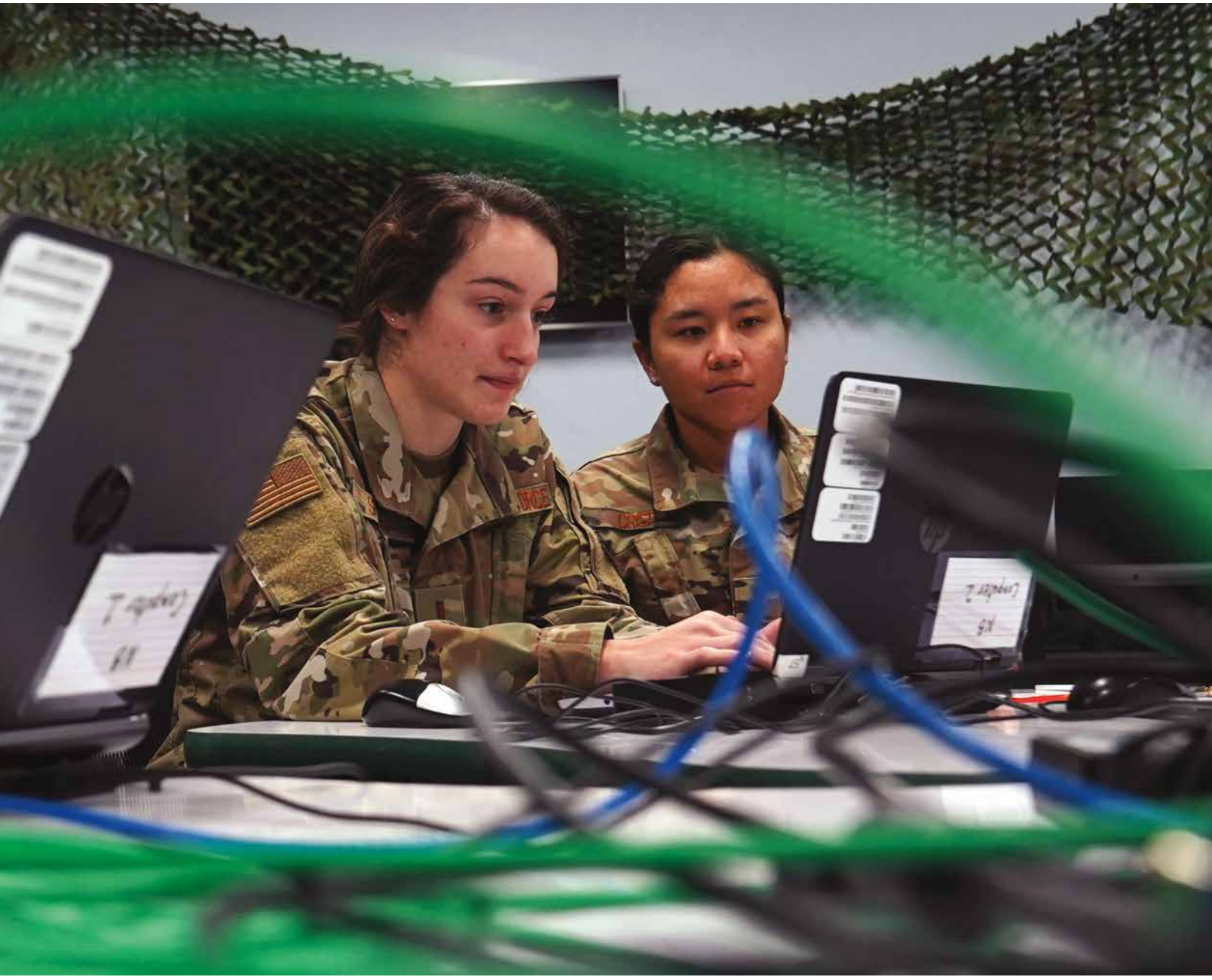
The United States is under constant attack from state-enabled malicious cyber actors. These malicious activities are estimated to cost the U.S. economy as much as $242 billion annually, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA).[1] Cyber security company McAfee, in conjunction with the Center for Strategic and International Studies, reported that the majority of cyber attacks on the United States and its allies originate from Russia, China, North Korea, and Iran, whose governments have adopted symbiotic relationships with state and nonstate malicious cyber actors.[2] The U.S. national cyber strategy calls for deterrence via "the imposition of costs through cyber and non-cyber means."[3] U.S. Cyber Command (USCYBERCOM) has substantial offensive cyber capabilities, but the nature of cyberspace has blurred its contribution to cyber deterrence. Cyber deterrence against determined, resilient, and often profitable actors has remained elusive. The U.S. Government must consider additional options that directly raise the costs of malicious cyber activities to deter them.

The 2020 Cyberspace Solarium Commission, the Department of State recommendations to the President, and a Department of Defense (DOD) task force all proposed critical actions to attain cyber deterrence. However, fundamental cyberspace challenges, such as attribution and the risk of compromise, impede implementation. General Paul Nakasone, commander of USCYBERCOM and director of the National Security Agency (NSA), stated strategic effects "come

Lieutenant Colonel Ryan Tate, USA, wrote this essay while a student at the U.S. Army War College. It won the Strategic Research Paper category of the 2022 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

from the use—not the mere possession—of cyber capabilities."[4] Recent uses of offensive cyber capabilities illuminate new options for deterrence. Deterrence is central to U.S. defense strategy, yet malicious cyber actors persist with impunity against the United States. How can offensive cyber capabilities complement cyber deterrence?

Public disclosure is necessary for offensive cyber capabilities to deter malicious cyber actors, nested with U.S. strategic guidance and achievable based on recent cyberspace operations. Disclosure of the targeted use of offensive cyber capabilities influences the cost-benefit decisions of malicious cyber actors. Use combined with disclosure—transparent cyber deterrence—raises the expectation that malicious actors will face consequences directly affecting them. This concept of transparency shapes international behavior by deterring the scope and aggressiveness of malicious cyber activities and encouraging like-minded allies to act in kind. Transparent cyber deterrence is based on deterrence theory, intragovernmental and scholarly recommendations for cyber deterrence, and recent U.S. and European cyberspace-enabled reprisals against Russian interference in U.S. elections and global cyber criminals DarkSide, Trickbot, and



Air Force 2nd Lieutenant Alexis Shirley and 2nd Lieutenant Trisha Crisp, 333rd Training Squadron cyber warfare officers, complete cyber tasks in cyber escape room inside Stennis Hall, at Keesler Air Force Base, Mississippi, November 10, 2021 (U.S. Air Force/Seth Haddix)

Emotet. This article examines the strategic problem of malicious cyber activities, a framework for cyber deterrence using offensive cyber capabilities, and U.S. strategic guidance. It then recommends the concept of transparent cyber deterrence and offers a brief analysis of its suitability, acceptability, feasibility, risks, and implications.

The Strategic Problem of Malicious Cyber Activities

State and nonstate actors employ cyber activities for a variety of reasons that ultimately subvert U.S. power and asymmetrically erode U.S. competitive advantages. Emily Goldman argues the United States is facing a crisis, losing ground in cyberspace as the volume, diversity, and sophistication of threats increase and shift from exploitation to disruptive and destructive attacks.[5] State-enabled malicious cyber activities include espionage of intellectual property, cyber crime to fund illicit activities and degrade competitors, covert influence campaigns, and disruptive attacks on critical infrastructure. General Nakasone summarizes the strategic challenge the United States faces now in cyberspace:

Today peer and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns. Cyberspace provides our adversaries with new ways to mount continuous, nonviolent operations that produce cumulative, strategic impacts by eroding U.S. military, economic, and political power without reaching a threshold that triggers an armed response.[6]

The proliferation of malicious cyber activity, whether financially or strategically motivated, threatens national interests. According to McAfee, malicious cyber activities cause losses in productivity that undermine national security and damage economies.[7] Despite advantages across the instruments of power, malicious cyber campaigns constantly undermine and erode U.S. economic and technological competitive advantages. State-enabled malicious cyber activities range from cyberspace espionage to empowering cyber crime (for example, allowing ransomware operations based in sovereign territory) to disruptive attacks on critical infrastructure and actions that undermine the integrity of democratic institutions and processes. For example, Reuters reported that North Korea used malicious cyber activities to generate funds for its nuclear and missile programs.[8] The cost-benefit advantages of malicious cyber activities contribute to their prevalence.

Operating costs and risks for cyber actors are low, while payoffs are substantial. British consulting firm Deloitte estimated monthly cyber-criminal operating costs between $544 and $3,796.[9] Conversely, the Federal Bureau of Investigation (FBI) calculated that thefts average $5,000 per incident.[10] Malicious cyber activity benefits from more than cost efficiency. The design of cyberspace provides five advantages: choice of scale, ability to act from any location, access to tools with desired precision, surprise and reuse inherent in the deception of tools, and the ability to avoid retaliation because of opaqueness in origins.[11] FBI director Christopher Wray stated the United States must "change the cost-benefit calculus of criminals and nation-states who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves."[12] The United States can raise costs for malicious cyber actors directly using offensive cyber capabilities, but influencing actors' decisions requires a focus on raising their cost expectations.

Cyber Deterrence Framework

Deterrence theory implies that it is possible to deter malicious cyber actors by creating the expectation that retaliatory costs will exceed the benefits of malicious activities. Congressional, State Department, and DOD advisory groups recently published recommendations for cyber deterrence. The 2020 Solarium Commission concluded cyber deterrence requires clear communication of consequences, costs that outweigh perceived benefits, credibility of capability and resolve, escalation management, the ability to attribute, and a policy for when to "voluntarily self-attribute cyber operations."[13] The State Department stressed the need for cyber actors to be certain they will face consequences and the need for public and private communications, improved attribution, direct targeting of cyber actors, and coordinated reprisal with international partners.[14] DOD's Task Force on Cyber Deterrence proposed deterrence campaigns targeting what malicious cyber actors value. This can be accomplished using multiple instruments of power, communication of the capability and will to respond, and risk management of unintended effects, such as escalation or tool compromise. The task force predicted that this posture would lead to cyberspace norms important for U.S. legitimacy.[15] Government recommendations encapsulate the primary issues debated among scholars.

Scholars debate the feasibility of deterrence in cyberspace and articulate recurrent themes on what cyber deterrence must address. Joseph Nye states cyber deterrence depends on perception, attribution, uncertainty, and escalation risks and should consider entanglement and norms.[16] Will Goodman contends that real-world examples demonstrate cyber deterrence is viable, but challenges include attribution, anonymity, scalability, reassurance, escalation, and clear signaling.[17] Conversely, Michael Fischerkeller and Richard Harknett argue that the uniqueness of cyberspace makes deterrence unfeasible below the use-of-force threshold, theorizing that continuous interactions encourage stable competition.[18] Mariarosaria Taddeo reasons deterrence is limited by the nature of cyberspace regarding attribution, credible signaling, escalation, uncertainty of effects, and proportionality.[19] Attribution, credibility, clear communication, scalability, environmental uncertainty, misperceptions, escalation, risks of compromise, unintended effects, and the question of norms are themes pervading scholarly debate. The intersection of government and scholarly recommendations informs a useful framework.

Effective deterrence requires capability, credibility, and communication. Capability is the power to project targeted, proportionate, and scalable cyberspace effects of significant cost. Credibility means malicious cyber actors believe the capability and the resolve to use it exist. Communication is the mechanism to clearly signal intent to impose consequences for specific malicious cyber activities for target audiences including cyber actors as well as allies and partners.

Critical enabling capabilities include attribution, intelligence, and operations capacity. Attribution is the ability to trace malicious cyber activities to an actor sufficiently to enable targeted reprisal, despite obfuscation or anonymity in cyberspace. Intelligence enables cyberspace attribution, assessment of effects and reactions, and identification of cyber actor interests and perceptions. Avoiding attribution and, therefore, retribution is key for malicious cyber actors to preserve favorable cost-benefit tradeoffs for cyber activities. Operations capacity is the ability to appropriately employ capabilities with communication, influencing malicious cyber actors' decisions while mitigating risk and building legitimacy.

The primary risks of cyber deterrence are compromise, unintended effects, and escalation. Compromise is the unintended disclosure of sensitive cyber capabilities and vulnerabilities or intelligence sources and methods. The inherent uncertainty and volatility of cyberspace make operations susceptible to unpredictable effects and to ambiguity and manipulation of perception. Escalation includes unintended responses that intensify conflict. Transparent cyber deterrence must address all these factors to raise expected costs for malicious cyber actors while supporting U.S. strategy.

A Strategic Approach

U.S. national security prioritizes deterrence.[20] President Joseph Biden's guidance is to hold malicious cyber actors accountable with proportionate costs and, along with allies and partners, to shape global cyberspace norms.[21] The 2018 National Cyber Strategy, issued under President Donald Trump, pursues deterrence "in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes" and includes criteria for "consensus on what constitutes responsible state behavior in cyberspace" and "consequences for irresponsible behavior." It states:

All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.[22]

Transparent cyber deterrence must enable an evident system of U.S. allies and partners that imposes proportionate consequences on malicious cyber actors to shape global norms in cyberspace.

The United States has imposed swift, costly, and transparent consequences outside of cyberspace for malicious cyber activities. The Department of Justice recently announced an indictment of four Chinese nationals for malicious cyber activities targeting the United States and its allies.[23] The Department of the Treasury retaliated for the SolarWinds attack in 2020 with broad financial prohibitions on specific Russian companies and individuals.[24] Reprisals against cyber-enabled interference in the U.S. elections include criminal indictments and economic designations against Russia's Internet Research Agency, revealing 15 names and specific activities.[25] U.S. economic and legal reprisals divulged surprising details on the identities, companies, and activities of malicious cyber actors.[26] This suggests that, without compromising sensitive intelligence, the United States can declassify and release sufficient information to attribute malicious cyber actors and describe their activities publicly. Yet there remain few public details of USCYBERCOM's offensive actions to impose costs on malicious cyber actors.[27]

USCYBERCOM is able "to compete with and contest adversaries globally, continuously, and at scale."[28] In 2018, National Security Advisor John Bolton confirmed the United States was conducting offensive cyber operations to defend the integrity of U.S. elections.[29] General Nakasone's 2019 statement to the Senate Armed Services Committee explained that USCYBERCOM imposed costs and "changed [Russia's] risk calculus for future operations."[30] The Director of National Intelligence declassified intelligence describing Russia's malicious activities in 2018 to influence U.S. public perceptions, assessing Russia "did not make persistent efforts to access election infrastructure, such as those made by Russian intelligence during the last U.S. presidential election."[31] A DOD news story reported that USCYBERCOM conducted more than 2,000 operations defending the 2020 elections.[32] The public record indicates U.S. cyber capabilities deterred malicious cyber activities in defense of recent U.S. elections, but details remain classified—along with their deterrence impact.

In contrast to announcements from Justice and Treasury, there is insufficient detail to understand the impacts and targets of USCYBERCOM offensive cyberspace operations. One reason to limit transparency is to minimize the chances of revealing intelligence or capability. But limited transparency also restricts the information malicious cyber actors need to recognize the threat that U.S. cyber capabilities pose to their interests. Despite their secrecy, USCYBERCOM operations offer two important observations. The first is that USCYBERCOM can deliver cyber effects using offensive cyber capabilities with acceptable risk to tools or methods. The second is that USCYBERCOM can generate numerous options to impose costs on malicious cyber actors—in other words, it can conduct offensive cyberspace operations at scale. Given such a capability, how important is transparency?

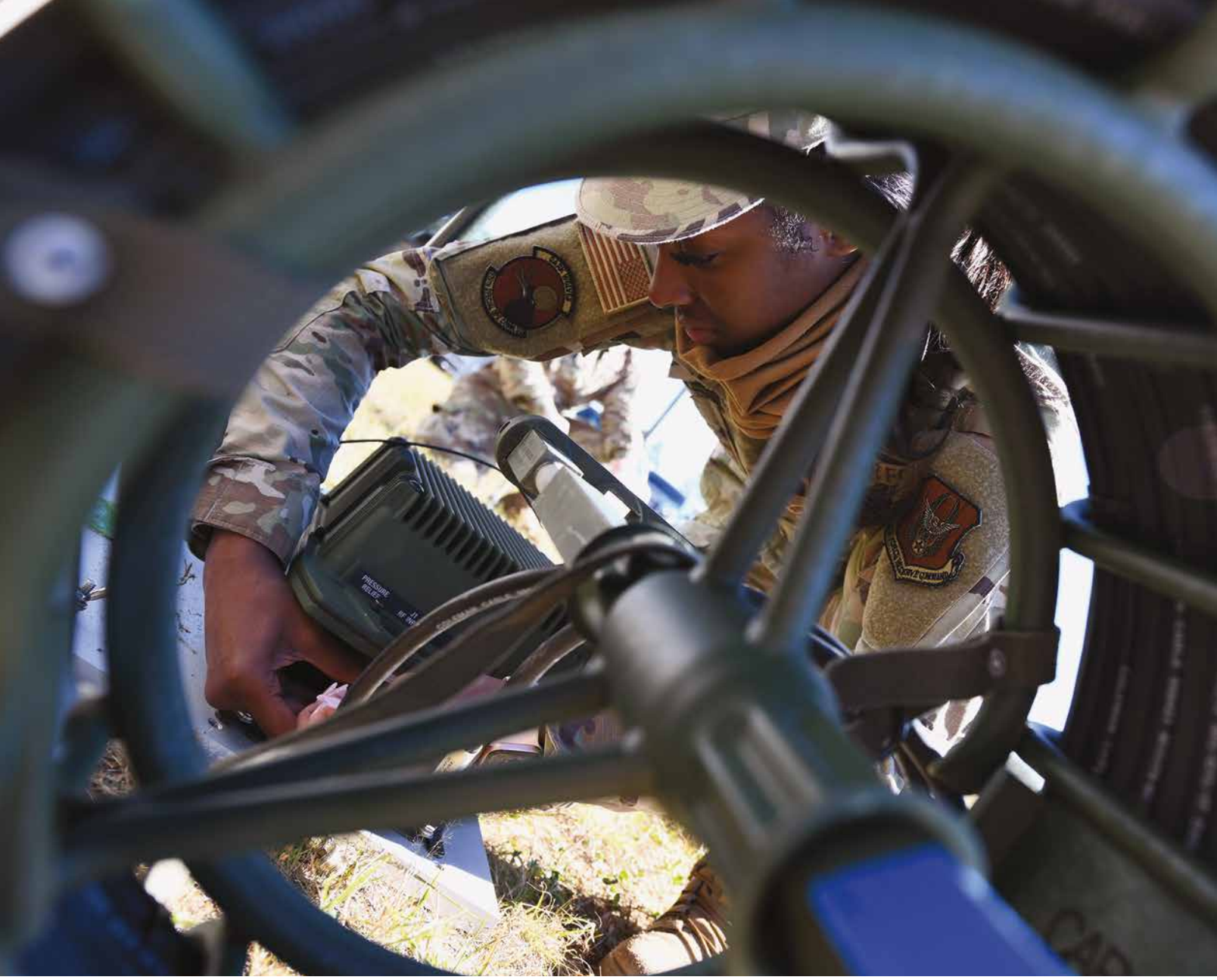
Senior Airman Robert Sleme, 62nd Cyber Squadron capabilities development manager, ensures hardware capabilities for classroom training usage on Buckley Space Force Base, Colorado, November 29, 2021 (U.S. Space Force/Andrew Garavito)

Transparency provides the communication required for successful deterrence. Public disclosure attributes specific malicious cyber activities and their consequences. This communicates a credible threat of direct reprisal in cyberspace for unacceptable behavior. It demonstrates the U.S. ability to impose significant costs on malicious cyber actors and the resolve to respond to *certain* malicious activities. This concept leverages deterrence theory and both government and scholarly recommendations. With consistency, transparent cyber deterrence will build legitimacy and shape global norms consistent with U.S. strategic guidance.

Transparent Cyber Deterrence

Transparent cyber deterrence combines the use of cyber capabilities with disclosure (that is, transparency) in the form of post factum public announcements stating the activities that elicited reprisal, specific targets with their justification, and the effects of the operation. Offensive cyberspace operations targeting malicious actors' cyberspace assets (for example, digital infrastructure and accounts) impose costs that directly influence the cost-benefit balance of malicious cyber activity. Disclosure exchanges some information to buy credibility in capability and will. This approach affords the ability to minimize compromise, escalation, and misperception and to consider information trade-offs prior to operations. Cyberspace effects alone marginally influence cyber actor decisionmaking because of the limited observability inherent in cyberspace.

Disclosing cyberspace effects unambiguously communicates capability with intent and generates the expectation of costs for multiple actors. Transparency also builds legitimacy, documenting proportionate targeting of specific actors for their activities. Consistent reprisal for specific activities threatening national interests, such as critical infrastructure, communicates which activities are



Senior Airman Icy Walley, 919th Special Operations Communications Squadron radio frequency technician, connects antenna cable to high-frequency whip antenna at Duke Field, Florida, November 7, 2021 (U.S. Air Force/Michelle Gigante)

unacceptable. Cyberspace reprisals are unlikely to deter all malicious activities, such as cyberspace espionage. Disclosure is essential to demonstrate legitimate reprisal for unacceptable activities, shape international norms, and ensure deterrence credibility.

Analysis

The capability, credibility, and communication of transparent cyber deterrence enable a transparent system of U.S. allies and partners that imposes proportionate consequences on malicious cyber actors to shape global cyberspace norms. An analysis of the suitability, acceptability, feasibility, and risk shows that transparent cyber deterrence can be effective. Suitability analysis explores how capability, credibility, and communication achieve a transparent system of U.S. allies and partners imposing proportionate consequences on malicious cyber actors to reinforce and shape global norms in cyberspace. Acceptability analysis focuses on the risks of compromise, unintended effects, and escalation and conformance to ethical principles and partnership practices. Feasibility analysis evaluates the ability of USCYBERCOM to meet the requirements of attribution, intelligence, planning, and execution of transparent, persistent operations. It mitigates risks of compromise, unintended effects, and escalation and is well suited ethically to interagency and international partners and to USCYBERCOM's attribution, intelligence, and planning abilities.

Suitability. Offensive cyber capabilities can impose costs that reverse the cost-benefit balance of malicious cyber activities. CISA estimated that median per-incident cyber damages range from $56,000 to $1.9 million when including immediate expenses, lost revenue, and business disruptions.[33] Costs at this scale

convert most malicious cyber activities into financial losses.[34] General Nakasone lauded USCYBERCOM's ability to degrade malicious cyber actors and achieve decisive results.[35] Cyber attacks disrupt operations, impose direct damages, compel expensive recovery and replacement, and damage reputations (for example, forcing cover-ups). But what matters for deterrence is setting the expectation of facing those consequences.

FBI and Europol announcements accompanied their recent cyberspace operations neutralizing malicious cyber activities. A 2020 cyberspace operation disrupted Trickbot, a "top-tier" cyber criminal active since 2016.[36] Researchers reported a 68 percent reduction in Trickbot activity but assessed that the effects would be temporary and that lasting deterrence would require targeting digital infrastructure combined with releasing information about the actors.[37] In January 2021, Europol announced actions in eight countries, severely disrupting the cyber infrastructure of Emotet, an actor behind the 2020 targeting of U.S. state and local governments.[38] Researchers assessed an 80 percent reduction in infections and unprecedented adjustments as Emotet became "pickier about who they target."[39] In April 2021, the FBI announced that a cyber operation recaptured $2.3 million in cryptocurrency directly from DarkSide shortly after the Russian cyber criminal's ransomware attack against Colonial Pipeline.[40] Reportedly, DarkSide suffered infrastructure disruption and announced it would avoid public targets as affiliates distanced themselves.[41] Trickbot, Emotet, and DarkSide later demonstrated resilience in various degrees, but law enforcement actions reduced the scope and scale of post-recovery activities. These cases illustrate how transparently striking back in cyberspace directly imposes costs on cyber actors' assets and influences multiple actors' decisions. Stronger deterrence requires costs that exceed temporary disablement. USCYBERCOM can impose such costs and, when combining them with transparency, raise the expected costs of targeted malicious activities for actors who have benefited from years of success and state protections.

Transparency must overcome the uncertainty, anonymity, and obfuscation inherent in cyberspace. Research on emerging military technologies with limited observability suggests capability employment is the most unambiguous way to signal a threat.[42] The use of offensive cyber capabilities demonstrates skill while public disclosure overcomes perception challenges. Publicity establishes a credible threat to other actors, creates reputational costs, and reduces the chance for successful downplay, denial, or manipulation of events.[43] Publicizing a firsthand accounting of cyber reprisal links consequences to specific malicious activity and promotes desired norms.

Transparent cyber deterrence shapes global cyberspace norms, which are common expectations about acceptable behavior. The World Bank reports that voluntary government alliances develop global norms by bringing issues into public discourse when there is strong leadership, accountability, and legitimacy.[44] Relevant and credible evidence is key to building acceptability and support.[45] Public disclosure provides a transparent accounting of consequences and malicious activities, enabling global discourse on unacceptable behaviors and what constitutes legitimate reprisal. In his remarks to the European Union in 2019, Christopher Ford, Assistant Secretary of State for International Security and Nonproliferation, explained:

Normative understandings can help anchor the policy choices of responsible states in responding to bad behavior in cyberspace—which is what normative regimes do by way of compliance enforcement. This issue of consequences is an emerging area of cooperation between like-minded states, one that is called for in our National Cyber Strategy.[46]

Disclosure demonstrates the acceptable use of offensive capabilities for deterrence, encouraging like-minded partners to contribute in kind.

The transparency of the Trickbot and Emotet operations led to formulations of voluntary alliances imposing consequences. Microsoft coordinated with global telecommunications providers, securing court orders for additional Trickbot disruption.[47] Europol's Emotet reprisal exemplified a security community raising costs through cyberspace operations, law enforcement, and public announcements across eight countries. In his study on deterrence and cyberspace norms, Tim Stevens argues that norms-based "deterrence communities" increase the chance of deterrence and encourage the exercise of power when it serves material interests.[48] Stevens adds that global normative frameworks not backed with coordinated and credible force fail to deter nonstate actors who are the most likely to conduct malicious cyber activities.[49] The United Nations Group of Governmental Experts in Information and Telecommunications Security concluded:

Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. . . . Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States.[50]

Publicly holding malicious cyber actors accountable facilitates cooperation from like-minded partners and an international system that curbs unacceptable behavior, cumulatively raising costs for malicious cyber actors. The United States can impose significant consequences with offensive cyber capabilities and translate those actions into deterrence with public disclosure to shape global norms.

Acceptability. It is possible to disclose the impact of an offensive cyber operation and release intelligence regarding targets without compromising methods or information. Conventional thinking is that disclosure compromises sensitive capabilities. However, FBI, Europol, and Treasury Department announcements demonstrate disclosing costs imposed with specific targets can satisfy public attribution and legitimacy requirements while protecting methods

and sources. Also, the volume of operations USCYBERCOM conducted defending the U.S. elections indicates the ability to deliver substantial effects without compromising capabilities. Last, post factum disclosure may reveal little more than the intelligence and access that are inherently compromised with a cyber strike. Transparency enables additional risk mitigation.

Transparency mitigates the risks of unintended effects from the uncertainty and limited observability in cyberspace. Disclosure communicates directly to target audiences the intended effects, targets, and actual outcomes and which activities provoked reprisal. Consistent justifications, as the FBI demonstrated, reduce uncertainties regarding intentions and thereby reduce risks of escalation. One concern with disclosure is that it risks accusations of misattribution or retaliation for reputational costs, in which case limited or private messaging may be more appropriate. However, Fischerkeller and Harknett contend that fears of escalation are unwarranted because malicious cyber activities already challenge national security and cyberspace competitive interaction stabilizes rather than escalates risk.[51] U.S. actions during the Cold War suggest that creative uses of the military send strong signals that are not inherently escalatory.[52] Disclosing information helps ensure that observers have sufficient data to assess U.S. actions, including evidence of the justification, targets, and actions that reduce opportunities for misrepresentation.

Transparent cyber deterrence upholds the Law of Armed Conflict principles of necessity, proportionality, and distinction, while ensuring that proper coordination and planning will protect partner interests. It is possible to conduct a cyberspace attack on cyber actors' logical assets while eliminating collateral damage to legitimate but unwitting host services. For example, FBI and Europol operations remediated bot access, freeing users' devices from malicious control without harming their hosts. Close coordination with law enforcement will remain fundamental in ensuring compliance with international law regarding third parties. Finally, USCYBERCOM operates closely with interagency partners to vet targets and review intelligence equities before releasing any information, minimizing unintended effects. Transparency also encourages international partners to assess reprisals and fosters their adoption of international norms.

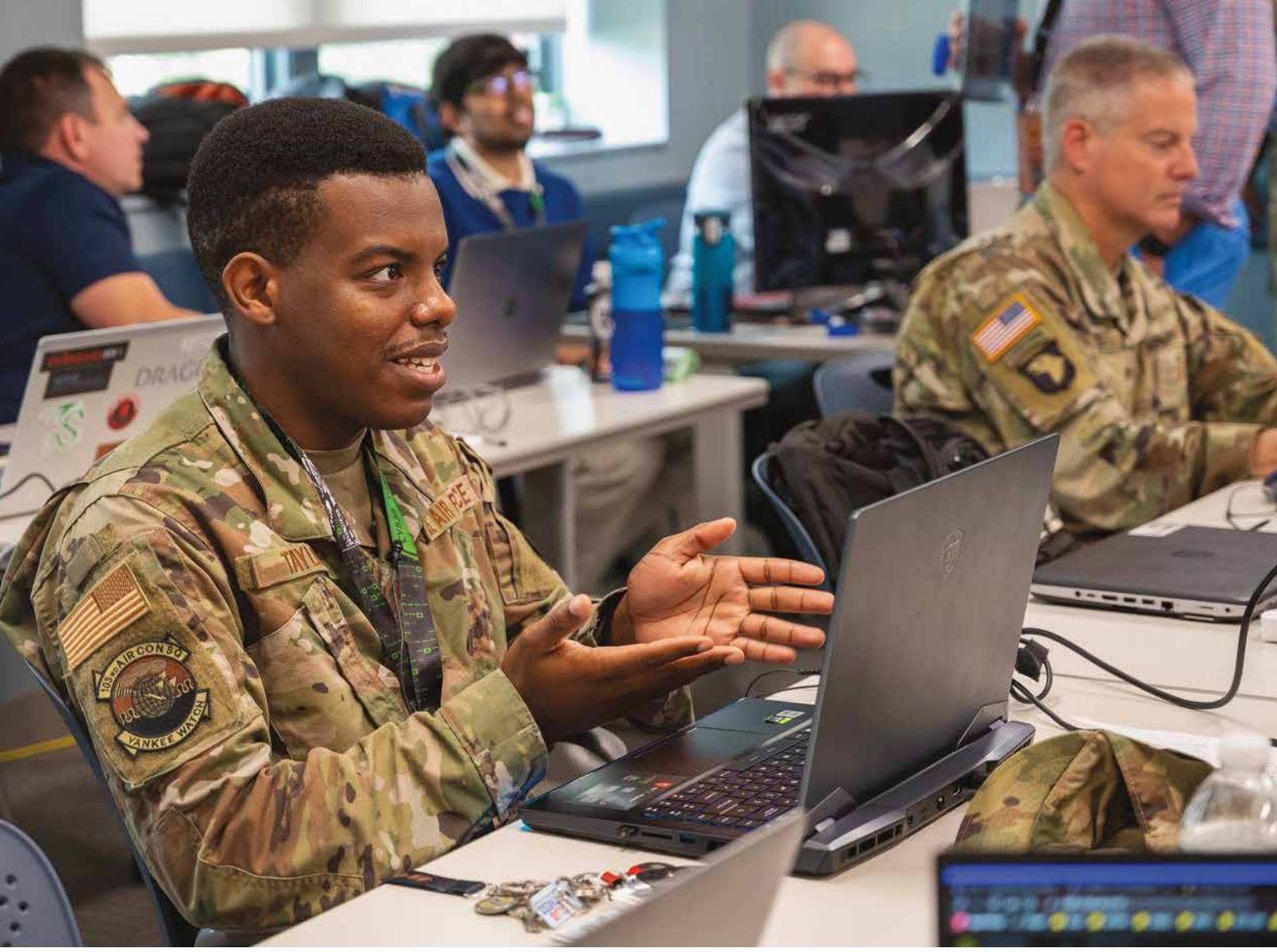
Feasibility. USCYBERCOM and its components provide sufficient capability to project targeted, proportionate, and scalable cyberspace effects of significant cost to malicious cyber actors. Its offensive teams degrade, disrupt, destroy, or manipulate adversary information, information systems, and networks.[53] The command operates a cyber mission force of 6,200 Servicemembers, including offensive forces organized in cyber national mission teams and cyber combat mission teams.[54] It also has multiple subordinate operational headquarters.[55] Additionally, USCYBERCOM is collocated with NSA and draws from the resources of the U.S. Intelligence Community to support messaging, effects, and attribution.[56] Public disclosure of USCYBERCOM operations may require a modest increase in personnel to plan and coordinate information release.

With these resources, USCYBERCOM is well positioned to deter malicious cyber actors. Michael Warner provides a brief overview of the command's offensive capabilities, from disruption of social media from the so-called Islamic State in 2016 to a "new level" in scale and scope targeting actors interfering in the 2018 elections.[57] Actions defending the U.S. elections in 2018 and 2020 demonstrate the ability to attribute malicious cyber activities and execute at scale.[58] General Nakasone affirmed USCYBERCOM's ability to impose tailored costs on malicious cyber actors.[59] In summary, USCYBERCOM has the planning, intelligence, and teams capable of generating a range of effects suitable for imposing proportionate consequences and the resources to attribute malicious cyber activities.

Risk. Public disclosure reduces the previously discussed risks of compromise, unintended effects, and escalation. There is also risk of underproducing the declassified intelligence or effects options for reprisal. Early planning for public disclosure in most offensive cyberspace operations will maximize future options. A campaign of targeted reprisal actions will afford the best opportunity to exceed the cost-benefit thresholds of resilient malicious cyber actors. While this will require significant resources, even periodic demonstrations can shape adversary decisionmaking. Finally, interagency coordination to mitigate intelligence equities and political-military risk will remain an important requirement. Ultimately, greater risk lies in allowing malicious cyber actors to continue their activities undermining the U.S. economy.

Implications. Law enforcement and economic actions are powerful but fail to impose high enough costs to deter malicious cyber actors, particularly for actors beyond jurisdictional reach. The FBI and Europol demonstrated consequences for major ransomware operations with public announcements detailing tangible costs and specific intelligence on malicious cyber actors. They leveraged successful multinational, public-private deterrence communities targeting cybercriminals without compromising sensitive intelligence or capabilities. Yet cybercriminals continue to make fortunes and benefit from state support, building resiliency and learning to hide from the law. Malicious cyber activities targeting critical infrastructure and other interests of national security demand higher consequences.

U.S. military cyberspace operations should respond to unacceptable malicious cyber activities by imposing dramatic countervailing costs directly on actors' cyberspace assets. Such actions would send a strong message that conducting malicious cyber activities threatening national and allied interests is not cost-effective. USCYBERCOM efforts should complement legal and other countermeasures, target the most significant malicious cyber actors, and significantly deepen costs (that is, exceed disablement) for activities threatening critical infrastructure, elections, or other national interests. Transparent cyber deterrence is essential to take back the offensive advantage in cyberspace.



Senior Airman with 103rd Air Control Squadron works as his Blue Team's communication liaison during Cyber Yankee 2022, in Niantic, Connecticut, June 16, 2022 (Air National Guard/David Pytlik)

Transparent cyber deterrence creates opportunities to secure advantages in the information environment. Using offensive cyber capabilities to impose consequences in an appropriate, transparent manner exploits the relative advantages of offense in cyberspace, compelling targets to defend everywhere and discouraging other malicious cyber actors. Disclosure seizes the initiative, setting the narrative of legitimate reprisal. It provides a public account of U.S. actions with evidence that malicious cyber actors must refute. Publicity reduces actors' abilities to construct alternate stories and downplay consequences. The costs of reprisal can be significant, as discussed, and portend substantial second-order effects from ensuing investigation and remediation. Offensive cyber capabilities are the means to impose costs on actors less susceptible to diplomatic, law enforcement, or economic actions. Additionally, consistency in public disclosure provides the ability to privately message some adversaries when it is crucial to demonstrate restraint or retain the option to escalate reputational costs. Furthermore, transparency encourages like-minded allies to reinforce acceptable behavior in cyberspace. This will create a deterrence community with the resolve and capability to raise costs for malicious cyber actors.

Conclusion

Malicious cyber actors operate with impunity, enjoying the low-cost benefits of cyberspace and often state support. The cumulative effects of malicious cyber activities already threaten national security. Malicious cyber activities targeting national interests, such as critical infrastructure, demand higher consequences. Strategist B.H. Liddell Hart stated, "It is folly to imagine that the aggressive types, whether individuals or nations, can be bought off . . . but they can be curbed. Their very belief in force makes them more susceptible to the deterrent effect of a formidable, opposing force."[60] Offensive cyber capabilities are the means to impose costs on actors that are increasingly resistant to diplomatic, legal, or economic instruments. Using offensive cyber capabilities, the United States can alter the cost-benefit

decisions of such actors while shaping international norms.

Recent cyberspace operations suggest the United States can positively attribute malicious cyber activities, impose significant consequences with offensive cyber capabilities, and translate those actions into deterrence with calculated public communication. Transparent cyber deterrence combines transparency with the use of offensive cyber capabilities to impose dramatic costs on actors undertaking unacceptable activities. It exploits the relative advantages of offense in cyberspace to compel reprisal targets to defend everywhere while publishing evidence of the consequences, actors, and their activities. Such evidence would be difficult to ignore and would influence the cost-benefit decisions of other actors. The expectation of costly reprisal is what is required to deter the scope and aggressiveness of malicious cyber activities.

Transparent cyber deterrence implements U.S. strategic guidance, leverages disclosure to maximize deterrence credibility while minimizing the risks inherent in cyberspace operations, and shapes cyberspace norms. The United States must demonstrate offensive cyber capabilities to influence the cost-benefit decisions of malicious cyber actors. A transparent approach would also advance discourse among allies, promote international norms, and force strategic dilemmas on malicious cyber actors and their enablers who seek cost-effective strategies to attack the United States, its allies, and its partners. **JFQ**

Notes

[1] *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, VA: Cybersecurity and Infrastructure Security Agency [CISA], 2020), 11, available at <https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf>.

[2] Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime* (Washington, DC: Center for Strategic and International Studies, 2020) 3, 27–32, available at <https://www.csis.org/analysis/hidden-costs-cybercrime>.

[3] *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), 3, available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

[4] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019), 12.

[5] Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Newport Paper 45 (Newport, RI: U.S. Naval War College, 2020), 35–36.

[6] Nakasone, "A Cyber Force for Persistent Operations," 10–11.

[7] Smith and Lostri, *The Hidden Costs of Cybercrime*, 4.

[8] Michelle Nichols, "North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: UN Report," Reuters, August 5, 2019, available at <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX>.

[9] *Black-Market Ecosystem: Estimating the Cost of "Pwnership"* (London: Deloitte, December 2018), 21, available at <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf>.

[10] *Internet Crime Report 2020* (Washington, DC: Federal Bureau of Investigation, Internet Crime Complaint Center, 2020), 3, available at <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>.

[11] Schneider et al., *Ten Years In*, 49.

[12] "FBI Strategy Addresses Evolving Cyber Threat: Director Wray Emphasizes Closer Partnerships to Combat Cyber Threats and Impose Greater Costs to Cyber Actors," video, 16:47, Federal Bureau of Investigation, September 16, 2020, available at <https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620>.

[13] Angus King and Mike Gallagher, *United States of America Cyberspace Solarium Commission Report* (Washington, DC: Cyberspace Solarium Commission, 2020), 26–34, available at <https://www.solarium.gov/>.

[14] "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," Department of State, Office of the Coordinator for Cyber Issues, May 31, 2018, available at <https://2017-2021.state.gov/recommendations-to-the-president-on-deterring-adversaries-and-better-protecting-the-american-people-from-cyber-threats/index.html>.

[15] *Final Report of the Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: Department of Defense Science Board, 2017), 1–7, available at <https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf>.

[16] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017), 44–71.

[17] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010), 102–135. Will Goodman has advised Senator Patrick Leahy (D-VT) and the Assistant Secretary of Defense for Homeland Defense and Global Security.

[18] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (May 2017), 381–393.

[19] Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology* 31, no. 3 (October 2018), 339–355.

[20] *Interim National Security Strategic Guidance* (Washington, DC: The White House, 2021), 9, 18.

[21] Ibid., 18.

[22] *National Cyber Strategy*, 21.

[23] "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," press release, Department of Justice, July 19, 2021, available at <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>.

[24] "Treasury Sanctions Russia with Sweeping New Sanctions Authority," press release, Department of the Treasury, April 15, 2021, available at <https://home.treasury.gov/news/press-releases/jy0127>.

[25] "Russian National Charged with Interfering in U.S. Political System," Department of Justice, October 19, 2018, available at <https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system>; "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," press release, Department of the Treasury, December 19, 2018, available at <https://home.treasury.gov/news/press-releases/sm577>.

[26] "Sanctions Related to Significant Malicious Cyber-Enabled Activities," Department of the Treasury, available at <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities>.

[27] "U.S. Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise," press release, U.S. Cyber Command, April 15, 2021, available at <https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/>.

[28] Nakasone, "A Cyber Force for Persistent Operations," 12.

[29] "John Bolton on National Security Strategy," C-SPAN, video, 57:36, October 31, 2018, available at <https://www.c-span.org/video/?453856-1/john-bolton-discusses-national-security-strategy&start=1573>.

[30] General Paul Nakasone, Commander of U.S. Cyber Command, *Statement Before the Senate Armed Services Committee*, 116th Cong., 1st sess., February 14, 2019, available at <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf>.

[31] *Foreign Threats to the 2020 U.S. Federal Elections: Intelligence Community Assessment* (Washington, DC: National Intelligence Council, declassified March 10, 2021), 3, available at <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>.

[32] David Vergun, "Cybercom's Partnership with NSA Helped Secure U.S. Elections, General Says," March 25, 2021, *DOD News*, available at <https://www.defense.gov/Explore/News/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>.

[33] *Cost of a Cyber Incident*, 9–16.

[34] *Internet Crime Report 2020*, 3; *Black-Market Ecosystem*, 21.

[35] Nakasone, "A Cyber Force for Persistent Operations," 11.

[36] "Attacks Aimed at Disrupting the Trickbot Botnet," *Krebson Security*, October 2, 2020, available at <https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/>.

[37] Adam Kujawa et al., *State of Malware Report 2021* (Santa Clara, CA: Malwarebytes Inc., 2021), 18, available at <https://www.malwarebytes.com/resources/files/2021/02/mwb_stateofmalwarereport2021.pdf>; "Recent Trickbot Disruption Operation Likely to Have Only Short-Term Impact," *Intel471*, October 13, 2020, available at <https://intel471.com/blog/trickbot-disruption-microsoft-short-term-impact/>.

[38] "World's Most Dangerous Malware Emotet Disrupted Through Global Action," press release, Europol, January 27, 2021, available at <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>; National Cyber Awareness System, "Alert (AA20-280A): Emotet Malware," CISA, October 24, 2020, available at <https://us-cert.cisa.gov/ncas/alerts/aa20-280a>.

[39] "Collaborative Global Effort Disrupts Emotet, World's Most Dangerous Malware," *Check Point*, January 28, 2021, available at <https://blog.checkpoint.com/2021/01/28/collaborative-global-effort-disrupts-emotet-worlds-most-dangerous-malware/>; Kujawa et al., *State of Malware Report 2021*, 18.

[40] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," press release, Department of Justice, June 7, 2021, available at <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

[41] "The Moral Underground? Ransomware Operators Retreat After Colonial Pipeline Hack," *Intel471*, May 14, 2021, available at <https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>.

[42] Evan Braden Montgomery, "Signals of Strength: Capability Demonstrations and Perceptions of Military Power," *Journal of Strategic Studies* 43, no. 2 (2020), 317–324.

[43] Nye, "Deterrence and Dissuasion in Cyberspace," 48, 60.

[44] Johanna Martinsson, *Global Norms: Creation, Diffusion, and Limits* (Washington, DC: World Bank, Communication for Governance and Accountability Program, 2011), 4, 8, available at <https:// openknowledge.worldbank.org/bitstream/handle/10986/26891/649860WP00PUBLIC00Box361550B0GlobalNorms.pdf?sequence=1&isAllowed=y>.

[45] Ibid., 22.

[46] Christopher Ashley Ford, "Rules, Norms, and Community: Arms Control Discourses in a Changing World," remarks by Assistant Secretary of State for International Security and Nonproliferation to the European Union Conference on Nonproliferation, Brussels, December 13, 2019, available at <https://2017-2021.state.gov/rules-norms-and-community-arms-control-discourses-in-a-changing-world/index.html>.

[47] "Trickbot: U.S. Court Order Hits Botnet's Infrastructure," *Threat Intelligence*, Symantec Enterprise, October 12, 2020, available at <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption>.

[48] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (2012), 148–170.

[49] Ibid., 165.

[50] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: United Nations General Assembly, July 22, 2015), 7, available at <https://digitallibrary.un.org/record/799853?ln=en>.

[51] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review* (2019), 267–287.

[52] Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* 3, no. 2 (Spring 2020), 94–109, available at <https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/>.

[53] Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), II-7.

[54] "Cyber Mission Force Achieves Full Operational Capability," U.S. Cyber Command, May 17, 2018, available at <https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/>.

[55] "A Command First: CNMF Trains, Certifies Task Force in Full-Spectrum Operations," U.S. Cyber Command, June 7, 2021, available at <https://www.cybercom.mil/Media/News/Article/2647621/a-command-first-cnmf-trains-certifies-task-force-in-full-spectrum-operations/>.

[56] Michael Warner, *U.S. Cyber Command's First Decade*, Aegis Series Paper No. 2008 (Washington, DC: Hoover Institution, 2020), 9, available at <https://www.hoover.org/research/us-cyber-commands-first-decade>; "Joint Statement on Advancing State Behavior in Cyberspace," Department of State, September 23, 2019, available at <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace>.

[57] Warner, *U.S. Cyber Command's First Decade*, 14–18.

[58] General Paul Nakasone, *Posture Statement Before the Senate Armed Services Committee*, 117th Cong., 1st sess., March 25, 2021, available at <https://misi.tech/docs/Nakasone_03-25-21.pdf>.

[59] General Paul Nakasone, *Statement Before the Subcommittee on Intelligence and Emerging Threats and Capabilities, House Armed Service Committee*, 117th Cong., 2nd sess., March 4, 2020, available at <https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf>.

[60] Basil H. Liddell Hart, *Strategy*, 2nd ed. (New York: Penguin, 1991), 359.