Deterrence Thru Transparent Offensive Cyber Persistence

Lieutenant Colonel Ryan Tate
Colonel Chad Bates

ABSTRACT

State-enabled cyber campaigns are achieving cumulative, strategic effects on the United States. A lack of transparency limits offensive cyber capabilities from affecting the cost-benefit decisions of malicious cyber actors. However, recent operations suggest the United States can positively attribute malicious cyber activities, impose significant consequences with offensive cyber force, and translate those actions into deterrence of specific malicious activities using public communication. Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and achievable based on recent cyberspace operations. Transparent Offensive Cyber Persistence combines persistence with post factum, public disclosure of the justification, targets, and impacts of offensive cyber force, exchanging information for deterrence credibility. This work evaluates its suitability, acceptability, feasibility, and risks. Transparent Offensive Cyber Persistence exploits the relative advantages of offense in cyberspace to impose costs directly on malicious cyber actors, compel targets to defend everywhere, dissuade other actors, set a legitimate narrative of consequences for unacceptable malicious cyber activities, and shape international norms.

The United States (US) is under constant attack from increasingly capable state-enabled malicious cyber actors. The Cybersecurity and Infrastructure Security Agency (CISA) reported cyber incidents cost the US economy $242 billion in 2018.[1] McAfee and the Center for Strategic and International

LTC Ryan Tate is assigned to Joint Force Headquarters – Cyber (Army) (JFHQ-C) with duty at US Central Command. He holds a Master's degree in Computer Science from Duke University and in Strategic Studies from the US Army War College. He commissioned at the United States Military Academy in 2003 and transferred to Cyber Operations in 2016. His tactical assignments include the 3rd Battalion, 7th Infantry Regiment and 4th Brigade Combat Team, 3rd Infantry Division, where he deployed in support of Operation Iraqi Freedom (OIF), and the 326th Combat Engineer Battalion and 101st Sustainment Brigade, 101st Airborne Division, where he deployed for OIF. He served as assistant professor of Computer Science at West Point, NY and training chief for the US Army Cyber School. Finally, he served as a cyber combat mission team lead and JFHQ-C J35/planning lead at US Army Cyber Command.

Studies (CSIS) assess most attacks originate from Russia, China, North Korea, and Iran who have symbiotic relationships with malicious cyber actors.[2] Cybersecurity alone is unable to deter these actors: the US must significantly raise their perceived costs. US National Cyber Strategy deters via "the imposition of costs through cyber and non-cyber means."[3] U.S. Cyber Command (USCYBERCOM) has substantial offensive cyberspace capabilities, but the nature of cyberspace has limited their deterrent value.

The US must re-evaluate how offensive cyber force complements deterrence strategy. Cyber deterrence studies from Congress, the Department of State (DOS), and Department of Defense (DoD) produced foundational recommendations grounded in theory and practice.[4] Yet, challenges such as attribution and the risk of compromise impede implementation. USCYBERCOM adopted the strategic concept of *cyber persistence* to continuously contest adversaries in cyberspace. General Paul Nakasone, Commander of USCYBERCOM and Director of the National Security Agency (NSA), said that strategic effects "come from the use – not the mere possession – of cyber capabilities."[5] USCYBERCOM's persistence concept and recent offensive cyberspace operations illuminate new options for offensive cyber capabilities in deterrence. Scholars debate whether cyber deterrence is feasible and argue USCYBERCOM persistence is inherently defensive, but deterrence is central to US strategy and malicious cyber actors persist in their own offensive campaigns against the US. How can offensive cyber persistent engagement complement US cyber deterrence strategy?

Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and achievable based on recent cyberspace operations. The concept of *transparent offensive cyber persistence* combines cyber persistent engagement with calculated, post factum disclosure of operations information to

COL Chad Bates currently serves as faculty at the US Army War College in the Center for Strategic Leadership. COL Bates previously served as the Special Assistant to the Commanding General, US Army Cyber Command (ARCYBER), focusing on the readiness and training of ARCYBER's work force and served as the Deputy G-35/7 within the headquarters. He is currently a Cyber officer, but in 1995 he began his military career as a field artillery officer and in 2005 transferred to become a simulation operations officer (FA57) focusing on the field of modeling & simulation (M&S) and data science. He earned his PhD from George Mason University specializing in Earth systems and Geospatial Information Science, with a focus on spatial analysis and work process improvements. He earned a BS from the United States Military Academy, double Master's degrees from Webster University, and an additional Master's degree from the Naval War College.

influence the cost-benefit decisions of malicious cyber actors. This will shape international behavior by deterring the scope and aggressiveness of malicious cyber activities and encouraging like-minded allies to act in kind. Transparent offensive cyber persistence is based on deterrence theory, intragovernmental recommendations for cyber deterrence, scholarship, and observations from US and European law enforcement responses to malicious cyber activities, including US elections security interference, DarkSide, Trickbot, and Emotet. This work describes the strategic problem of malicious cyber activities, a framework for cyber deterrence with offensive cyberspace capabilities, US strategic guidance, and the concept of transparent offensive cyber persistence and then analyzes this concept and its implications.

THE STRATEGIC PROBLEM OF MALICIOUS CYBER ACTIVITIES

State and non-state actors employ cyber activities to subvert US power and asymmetrically erode US competitive advantages. Emily Goldman argues that the US is facing a crisis, losing ground in cyberspace as the volume, diversity, and sophistication of threats increases and shifts from exploitation to disruptive and destructive attacks.[6] State-enabled malicious cyber activities include espionage of intellectual property, sanctioned cybercrime to fund illicit activities and degrade strategic competitors, covert influence campaigns, and disruptive attacks on critical infrastructure. General Nakasone describes the stakes:

> 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.[7]

Operating costs and risks for malicious cyber activity are low while pay-offs are substantial. British consulting firm Deloitte estimated monthly cyber-criminal enterprise operating costs for a campaign with multiple tools falls between $544 and $3,796.[8] Conversely, the Federal Bureau of Investigation (FBI) calculated $4.1 billion in thefts from the American public in 2020, averaging over $5,000 each incident.[9] Commercialization trends make more tools more available at lower costs. But malicious cyberspace activity benefits from more than cost-efficiency. Chris Demchak explains the design of cyberspace provides malicious cyber actors five advantages: choice of *scale*, ability to act from any *proximity,* access to tools with desired *precision,* surprise and reuse inherent in the *deception of tools*, and the ability to avoid retaliation from *opaqueness in origins*.[10] FBI Director Christopher Wray said "we've got to change the cost-benefit calculus of criminals and nation-states who believe they can compromise US networks, steal US financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves."[11] The US can raise costs using offensive cyberspace operations.

CYBER DETERRENCE FRAMEWORK

Deterrence theory implies the threat of consequences will discourage actors from conducting malicious cyber activities against the US. Joint doctrine explains deterrence will "prevent adversary action through the presentation of a credible threat of counteraction."[12] Offensive cyber forces – USCYBERCOM – may deter malicious cyber actors by creating the expectation that retaliatory costs will exceed the benefits of malicious cyber activities. Intragovernmental recommendations for such a strategy have emerged over the past several years.

Congressional, DOS, and DoD advisory groups published recommendations for offensive cyber deterrence. The 2020 US Cyberspace 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 ... for the purposes of signaling capability and intent to various audiences."[13] DOS stressed malicious cyber actors must be certain they will face consequences and the need for a range of swift, transparent consequences for significant cyber incidents combined with tailored public and private communications, improved attribution, direct targeting of cyber actors, interagency planning to manage escalation, and coordinated reprisal with international partners.[14] DoD's 2017 Task Force on cyber deterrence proposed tailored, scalable deterrence campaigns of countervailing costs targeting what malicious cyber actors value using multiple instruments of power, explicit or implicit (by precedent) communication of the capability and will to respond, investments in attribution, and risk management of unintended effects, escalation, tool compromise, and other policy objectives.[15] This Task Force predicted deterrence posture will lead to cyber norms and declaratory policies important for international legitimacy,

a better alternative to cyber arms races. Government recommendations encapsulate many of the underlying theories and challenges debated among scholars.

Scholars debate the feasibility of deterrence in cyberspace below the use-of-force threshold and articulate consistent themes on what cyber deterrence must address. Nye says cyber deterrence depends on perception, must address attribution, uncertainty, and escalation risks, and should consider costs in terms of entanglement and norms.[16] Goodman contends real-world examples demonstrate cyber deterrence is viable but concedes challenges include attribution, contestability (resulting from anonymity), scalability, a lack of reassurance, escalation, and clear signaling.[17] Conversely, Fischerkeller and Harknett argue the uniqueness of cyberspace makes deterrence infeasible below the use-of-force threshold, observing that continuous interactions encourage stable, agreed competition.[18] Taddeo reasons deterrence is limited by the dynamic, ambiguous nature of cyberspace conflict regarding attribution, credible signaling, escalation, uncertainty of effects, and proportionality.[19] Goldman says deterrence theory no longer explains continuous cyber engagement because there is a paradigm shift underway demanding development of persistence concepts.[20] Attribution, credibility, clear communication, scalability, environmental uncertainty, misperceptions, escalation risk, risks of compromise, unintended effects, and the question of norms are themes pervading scholarship debate on cyber deterrence. This intersection of government and scholars' recommendations provides a useful framework.

Effective deterrence requires capability, credibility, and communication. Capability is the power to project targeted, proportionate, and scalable cyberspace effects that impose significant costs. Credibility means malicious cyber actors believe there is capability and the resolve to use it. Communication is the mechanism to clearly signal intent to impose consequences for specific malicious cyber activities (below the use-of-force threshold) to target audiences.

Critical enabling capabilities are attribution, intelligence, and operations capacity.[21] Attribution is the ability to trace malicious cyber activities to a malicious cyber actor in sufficient degree to enable targeted reprisal, despite obfuscation and anonymity in cyberspace. Intelligence support enables cyberspace attribution, assessments of effects and reactions, and identification of malicious cyber actor interests and perceptions. Operations capacity implies the ability to plan, employ capabilities, and communicate to influence malicious cyber actor decisions, while mitigating risk and building international support and legitimacy.

The primary challenges, or risks, of cyber deterrence are compromise, unintended effects, and escalation. Compromise is the unintended disclosure of sensitive cyberspace capabilities and vulnerabilities or intelligence sources and methods. The inherent uncertainty and volatility of cyberspace makes operations susceptible to unpredictable effects and both ambiguity and manipulation of perception. Escalation includes unintended adversary responses that intensify conflict. Transparent offensive cyber persistence addresses each component of this model to raise expected costs for malicious cyber actors while nesting within US strategy.

A STRATEGIC APPROACH

President Biden's Interim National Security Strategic Guidance identified a national priority to "deter and prevent adversaries from directly threatening the United States and our allies."[22] His guidance describes malicious cyber actors held accountable through proportionate costs and, with allies and partners, shaped global norms in cyberspace.[23] The 2018 National Cyber Strategy explains that 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."[24] In summary, a strategic objective for offensive cyber deterrence is: a transparent system of US allies and partners that imposes proportionate consequences on malicious cyber actors to reinforce and shape global norms in cyberspace.

In practice, the US has imposed swift, costly, and transparent consequences outside of cyberspace for certain malicious cyber activities. The Department of Justice (DOJ) recently announced an indictment of four Chinese nationals for malicious cyber activities targeting the US and its allies.[25] In April 2021, the Department of Treasury (USDT) retaliated for the SolarWinds attack with broad financial prohibitions on specific companies and individuals in the Russian defense and technology sector.[26] Similarly, reprisals against Russian cyber-enabled interference in the 2018 and 2020 US elections included criminal indictments disclosing significant intelligence on Project Lakhta and economic designations against the Internet Research Agency that revealed 15 names and specific activities.[27] US economic and legal reprisals divulged surprising details on the individuals, companies, and specific activities of malicious cyber actors.[28] This suggests that without compromising sensitive intelligence, the US can declassify and release sufficient information to attribute malicious cyber actors and describe their activities publicly. Yet, there are few public details of USCYBERCOM's offensive actions to impose costs on malicious cyber actors.[29]

USCYBERCOM does not discuss offensive cyberspace operations details. According to General Nakasone, cyber persistence empowers USCYBERCOM "to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way."[30] General Nakasone's 2019 statement to the Senate Armed Services Committee explained USCYBERCOM imposed costs and "changed [Russia's] risk calculus for future operations."[31] In 2020, the Director of National Intelligence declassified intelligence assessing Russia "did not make persistent efforts to access election infrastructure, such as those made by Russian intelligence during the last US presidential election."[32] A defense article reported USCYBERCOM conducted over 2,000 operations defending the 2020 elections.[33] This indicates US cyberspace operations deterred specific malicious cyber activities targeting the elections, but the contribution of offensive cyber capabilities remains classified.

In contrast to announcements from DOJ and USDT, there was insufficient detail to understand the impacts and targets of offensive cyberspace operations defending US elections. One reason to limit transparency in cyberspace operations is to minimize the chance of revealing intelligence or capability. But limited transparency also restricts information malicious cyber actors need to recognize the threat that US cyberspace capabilities pose to their interests. Despite the secrecy, the scale, and stated successes of USCYBERCOM operations provide two important observations. The first is that USCYBERCOM can design and deliver effects with offensive cyber capabilities without risking, or with acceptable risk of, the exposure of sensitive tools or methods. The second is that USCYBERCOM's concept of persistent engagement has the power to generate multiple options to impose costs on malicious cyber actors in cyberspace. Given such a capability, how important is transparency?

Transparency enables the communication required for deterrence credibility. Transparency via public disclosure attributes specific malicious cyber activities and describes their consequences, communicating a clear threat for unacceptable behavior. This message demonstrates the US ability to impose significant costs on malicious cyber actors and the resolve to respond to certain types of malicious cyber activities. This basic concept is built on the framework of deterrence theory, government recommendations, and scholarship precepts. Not only is offensive cyberspace operations transparency achievable but, when executed persistently, it builds legitimacy and shapes global norms consistent with US strategic guidance.

TRANSPARENT OFFENSIVE CYBER PERSISTENCE

Transparent offensive cyber persistence is a method to complement US cyber deterrence strategy with offensive cyberspace operations. Its two driving mechanisms are: (1) disclosure (i.e., transparency): post factum, public announcements stating which activities elicited reprisal, the specific targets with their justification, and the effects of the operation; and (2) persistence: an offensive cyberspace operation targeting malicious cyber actors' interests (e.g., cyberspace assets) to impose costs appropriate for proportionate reprisal.

Disclosure exchanges information for the credibility of capability and will. Publicly providing declassified information creates transparency that demonstrates the imposition of steep consequences for certain malicious activities. Transparency supports legitimacy by connecting the evidence of proportionate, targeted strikes to the culpability of specific actors or assets and their activities which elicited the response. Disclosure is essential to build deterrence credibility in a domain of impunity, to demonstrate legitimate reprisal for unacceptable activities, and to shape international norms.

Cyber persistence is USCYBERCOM's concept of continuous engagement to shape malicious cyber actor behavior. Persistence creates credibility in the US resolve to respond to cyber actors directly in cyberspace through consistent action. However, persistence alone has marginal influence on malicious cyber actor decision-making because of the limited observability

inherent in cyberspace. Disclosing cyberspace effects unambiguously communicates capability with intent and generates deterrence from persistent engagement.

Persistence with transparency will clearly communicate the high costs the US will impose in response to specific malicious cyber activities and shape international behavior. Consistently focusing on specific malicious cyber activities that threaten national interests, such as attacks on critical infrastructure or the integrity of elections, communicates which activities are most unacceptable.[34] This approach affords the ability to minimize compromise, escalation, and misperception and for consideration of information trade-offs in advance of an operation.

ANALYSIS: SUITABILITY, ACCEPTABILITY, FEASIBILITY, AND RISK

This section illustrates how the capability, credibility, and communication of transparent offensive cyber persistence shapes a transparent system of US allies and partners that imposes proportionate consequences on malicious cyber actors to reinforce and shape global norms in cyberspace. It examines the risks of compromise, unintended effects, and escalation, including a brief discussion of implementation risk. It also reviews repercussions for ethics, interagency and international partnerships, and USCYBERCOM's attribution, intelligence, and planning abilities.

Suitability

Cyberspace capabilities are capable of imposing costs that reverse the cost-benefit balance of malicious cyber activities. CISA reported median per-incident cyber damages range from $56,000 to $1.9 million including immediate expenses, lost revenues, and disruptions to business function.[35] The expectation of reprisal at this scale would provide a powerful disincentive for certain malicious cyber activities.[36] General Nakasone lauded USCYBERCOM's ability to effectively degrade malicious cyber actors and achieve decisive results.[37] Cyber-attacks disrupt operations, impose direct damages, compel expensive recovery and replacement measures, and damage reputations (e.g., forcing cover-ups). But what matters for deterrence is the expectation of facing those consequences.

Demonstrations of offensive cyber capability must overcome their inherent uncertainty, anonymity, and obfuscation to signal capability and resolve. Evan Montgomery's research on emerging military technologies with limited observability suggests capability employment is the most unambiguous way to signal a threat.[38] Recent law enforcement operations demonstrate transparency can extract deterrence credibility from offensive cyber capabilities. FBI and Europol cyberspace actions accompanied with public announcements generated a deterrent effect and enabled the voluntary coordination of cybersecurity partners to collectively raise costs for Trickbot, Emotet, and Darkside.[39]

A sophisticated operation in late 2020 reportedly disrupted Trickbot, a massive malware platform enabling "top-tier cybercriminals" to harvest financial data since 2016.[40] Malwarebytes

reported a 68% percent reduction in Trickbot activity since the operation.[41] Researchers assessed only short-term disruption and concluded meaningful deterrence would require "novel solutions" targeting the malicious cyber actors' own assets to include releasing information about the actors and aggressive targeting of Trickbot infrastructure.[42] This implies strong deterrence requires costs exceeding temporary deactivation – what USCYBERCOM can deliver. USCYBERCOM reprisal is necessary to deter resilient actors who have benefitted from years of state sponsorship and success. Europol approached this threshold in early 2021.

In January 2021, Europol announced actions across eight countries that severely disrupted the cyber infrastructure of Emotet, a notorious access vector for state-enabled actors.[43] As a disrupter, Emotet may have affected 19% of global networks since 2014 and recently enabled successful critical ransomware attacks against hospitals and the mid-2020 targeting of US state and local governments.[44] Security firm Checkpoint assessed that Europol's operation caused an 80% reduction in infections and 40% decrease in control communications.[45] Researchers reported that as a result Emotet became "pickier about who they target" after unprecedented adjustments.[46] Europol's operation demonstrates significant costs can have a deterrent effect on the scope and scale of malicious cyber activities.

In May 2021, Russian cybercriminal group DarkSide conducted a successful ransomware attack against Colonial Pipeline, operator of the largest US oil pipeline. One month later, DOJ announced an FBI cyber operation recaptured $2.3 million directly from DarkSide's cryptocurrency accounts, declaring, "We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks."[47] Reportedly, DarkSide suffered infrastructure disruption and announced it would stop its ransomware-as-a-service program and avoid public targets, as affiliates began to shun its services.[48] Trickbot, Emotet, and DarkSide reprisals illustrate how to transparently strike back in cyberspace, imposing costs and influencing actors' decisions.

Despite Trickbot, Emotet, and DarkSide resilience, law enforcement actions reduced the scope and scale of post-recovery activities. FBI and Europol announcements informed affiliated actors they can and will be subjected to cyberspace force. When the FBI announced it targeted DarkSide, there was rapid behavior change and distancing from DarkSide affiliates to avoid further costs.[49] In each case, public disclosure demonstrated resolve to impose consequences with offensive cyber capabilities, the costs those actions imposed, and the specific activities that precipitate them. Stronger deterrence requires costs that exceed temporary disablement. USCYBERCOM can impose those costs, and transparency is essential to clearly signal this intent.

Actions send a clear message of intention, and public disclosure is required to overcome perception challenges. Consistent disclosure of offensive cyberspace effects demonstrates the capability to attribute and impose costs combined with the resolve to respond to specific malicious cyber activities. Publishing the costs imposed in reprisal informs both actors responsible for targeted assets and parties likely to verify the incident.[50] Publicity creates reputational costs and reduces the chance for successful downplay, denial, and deception

by forcing the adversary to contend with a competing narrative.[51] Establishing the initial account of events with first-hand knowledge from an operation provides the opportunity to link consequences to specific malicious cyber activity and document their scope and scale as legitimate reprisal. Persistent, public disclosure of USCYBERCOM offensive cyberspace reprisal would significantly increase the credibility of threats to actors who conduct cyber activities threatening national interests. It also sets conditions for behavioral norms in the international community.

Transparent offensive cyber persistence shapes global norms on responses to malicious cyber activities. Norms are common expectations about acceptable behavior. The World Bank reports voluntary government alliances develop global norms by bringing issues into public discourse when there is strong leadership, accountability, and legitimacy.[52] The use of relevant and credible evidence is crucial in building public and political support.[53] Public disclosure provides a transparent accounting of consequences and specific malicious activities, enabling global discourse on unacceptable behaviors and legitimate reprisal. Transparency builds trust with the US population and with allies. In his remarks to the European Union in 2019, Under Secretary of State Christopher Ford 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 likeminded states, one that is called for in our National Cyber Strategy.[54]

Disclosure leads by example and demonstrates the acceptable use of offensive capabilities for deterrence, encouraging like-minded partners to contribute in-kind. A voluntary alliance of like-minded states imposing cyberspace consequences on malicious cyber actors will greatly improve deterrence.

The transparency of Trickbot and Emotet operations led to formulations of voluntary alliances to impose consequences. Microsoft coordinated global telecommunications providers and others to further disrupt Trickbot, securing court orders for direct disruption.[55] The FBI also continued reprisal, announcing additional indictments and releasing additional Trickbot information in June 2021.[56] Europol's Emotet reprisal also exemplified a security community coordinating to impose costs through cyberspace operations, law enforcement, and public announcements in eight countries. In his study on deterrence and norms in cyberspace, Tim Stevens argues norms-based "deterrence communities" increase the chance of deterrence and encourage the exercise of power, emphasizing that global normative frameworks not backed with credible force fail to deter non-state actors.[57] 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 tools, methods, and vulnerabilities or intelligence sources and methods. Conventional thinking is that disclosure compromises sensitive capabilities. However, FBI, Europol, and USDT announcements demonstrate disclosure can release details on costs imposed and specific targets while protecting methods and sources. Further, the volume of operations that USCYBERCOM conducted in its defense of the US elections indicate the command's ability to deliver noticeable effects without compromising capabilities. The plausibility of such information is extant in the accesses exposed during the observable effects of cyber-attack.[58] Therefore, post factum disclosure may reveal little more than the intelligence and access compromised already with reprisal. The aforesaid operations indicate it is possible to declassify enough intelligence for public attribution that legitimizes reprisal. The transparency of consistent public disclosure enables additional risk mitigation.

Transparency and persistence mitigate the risks of unintended effects. Cyberspace uncertainty causes unintended effects from misperceptions to unreliable timelines in executing operations. Even conventional military power is difficult to assess in advance of a conflict.[59] Persistence reduces this uncertainty through repetitive execution which builds experience in the execution and assessment of technical risks. Public disclosure communicates directly to target and international audiences the intended effects, targets of an operation, outcomes, and which activities provoked reprisal. Consistent disclosure demonstrates the intent to deliver targeted responses for certain malicious activities. Persistent demonstration reduces uncertainties regarding intentions externally and capabilities internally. Transparency limits misperception.

Consistent public disclosure provides a clear strategic message that reduces the risk of escalation. Timely disclosure connects cyberspace effects to malicious activity reprisal as (or before) adversary decision-makers learn of the strike. While disclosure attributes actions to the US, which aids attribution for malicious cyber actors, it also informs the international community. There is risk public exposure will incur accusations of misattribution or retaliation for reputational costs, in which case limited or private messaging may be more appropriate. Fischerkeller and Harknett note fears of escalation are unwarranted because malicious cyber activities already challenge national security and cyberspace competitive interaction stabilizes rather than escalates.[60] US actions during the Cold War suggest that creative uses of the military send strong signals not inherently escalatory.[61] Disclosing information provides the opportunity to ensure observers have sufficient data to assess US actions, including evidence of the justification, targets, and actions that reduce opportunities for misrepresentation.

Nothing in transparent offensive cyber persistence compromises the law of armed conflict or partnership practices at USCYBERCOM, which will continue to adhere to the principles

of necessity, proportionality, and distinction. While there is debate about the military intervening in cybercriminal activity, there is precedence for intervention against non-state actors when national interests are threatened, such as counter piracy. Further, it is possible to conduct a cyberspace attack on malicious cyber actors' logical assets while minimizing collateral damage to legitimate but unwitting host services. For example, FBI and Europol operations remediated bot access, freeing unsuspecting users' devices from malicious control without harming their hosts. Close coordination with law enforcement will continue to be fundamental in ensuring compliance with international law regarding third parties. Finally, USCYBERCOM operates closely with interagency partners to vet targets and facilitate the review of intelligence equities before releasing any information, minimizing unintended effects. Transparency also encourages international partners to assess the actions of USCYBERCOM and shape their adoption as international norms.

Feasibility

USCYBERCOM operations provide sufficient capability to project targeted, proportionate, and scalable cyberspace effects of significant cost. Its offensive teams degrade, disrupt, destroy, or manipulate adversary information, information systems, and networks.[62] Michael Warner provides a describes the progression of USCYBERCOM's offensive capabilities, which disrupted Islamic State social media in 2016, as reaching a "new level" in scale and scope during the defense of US elections in 2018.[63] Actions defending the US elections in 2018 and 2020 demonstrate the ability to attribute malicious cyber activities and execute at scale.[64] General Nakasone affirmed USCYBERCOM's ability to impose tailored costs on malicious cyber actors.[65] USCYBERCOM operates a Cyber Mission Force of 6,200 servicemembers including offensive forces organized in Cyber National Mission Teams and Cyber Combat Mission Teams.[66] It has multiple operational headquarters providing planning and coordination capabilities.[67] General Nakasone reported the combined strength of USCYBERCOM and subordinate commands reached 238,000 personnel with other supporting elements across DoD.[68] Disclosure to extract deterrence from existing USCYBERCOM activities may require a modest increase in personnel to support this additional function. However, USCYBERCOM also draws from the resources of the US intelligence community to support messaging, effects, and attribution.[69] 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

Previous subsections discussed the primary risks of compromise, unintended effects, and escalation but implementation risk requires elaboration. Implementation risk includes under-delivering attribution or disclosure intelligence and under-producing cyber effects options

required for reprisal. Early planning for public disclosure in most offensive cyberspace operations will maximize future options to enhance deterrence. A campaign of targeted reprisal actions will afford the best opportunity to exceed the cost-benefit thresholds of resilient malicious cyber actors. Some diversion of resources may be required to develop options for public disclosure. Not every opportunity will fit, but even periodic demonstration will provide important input to adversary decision-making. Interagency coordination to discover intelligence equities and political-military risk (e.g., conflict with other policy objectives) will remain an important factor in decisions to execute operations and declassify intelligence. Ultimately, greater risk lies in allowing malicious cyber actors to continue without imposing any significant costs their campaigns of malicious cyber activities that undermine US power.

IMPLICATIONS

Law enforcement and economic actions are powerful but fail to impose high enough costs to deter resolute cyber actors, particularly those outside jurisdictional reach. The FBI and Europol demonstrated consequences for major cybercriminals with public announcements detailing tangible costs and specific intelligence on the actors. They leveraged successful multi-national, public-private deterrence communities targeting cyber criminals without compromising sensitive intelligence or capabilities. Yet, cybercriminals have made fortunes and benefited from state support, building resiliency to legal and economic measures. Malicious cyber activities targeting critical infrastructure and other interests of national security demand higher consequences. When authorized, military power projection in and through cyberspace must severely degrade and destroy malicious cyber actors' assets. Such actions will send a strong message that malicious cyber activities threatening national and allied interests are not worthwhile. USCYBERCOM efforts may complement whole-of-government action, target the most significant malicious cyber actors, and significantly deepen costs for activities threatening critical infrastructure, elections, or other national interests.

Transparent offensive cyber persistence creates opportunities to achieve information advantage. Information advantage involves securing the initiative over other actors' behavior, situational understanding, and decision-making.[70] Using offensive cyber forces to impose consequences in a transparent manner exploits the relative advantages of offense in cyberspace, compelling targets to defend everywhere while discouraging other malicious cyber actors. Disclosure seizes the initiative, setting the narrative of legitimate reprisal coincidently with reprisal discovery. It provides a public account of US 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 above, and instigate substantial second order effects from the ensuing investigation and remediation.[71] 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 adversaries when it is crucial to demonstrate restraint or retain the option to escalate reputational costs. Furthermore, transparency encourages like-minded allies to also 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 activities erode the competitive advantages of the US. Malicious cyber actors operate with impunity despite economic, legal, and diplomatic reprisals, leveraging symbiotic relationships with Russia, China, North Korea, and Iran. Historian and theorist Sir B.H. Liddell Hart said, "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."[72] The US can influence the cost-benefit decisions of such actors. It can lead like-minded states to new international norms that make cyberspace a costly domain to conduct certain malicious activities, such as infrastructure or elections attacks. Transparent offensive cyber persistence provides this deterrent framework, combining transparency and persistence.

Persistent, public disclosure is necessary for offensive cyberspace operations to deter malicious cyber activities, nested with US strategic guidance, and attainable based on recent cyberspace operations. Recent 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. Whole-of-government cyberspace operations demonstrate consistent action with disclosure is likely to deter the scope and aggressiveness of malicious cyber activities. Those operations and USCYBERCOM's limited public record also suggest the significant, additional costs of military power projection in cyberspace would greatly influence malicious cyber actor decision-making. Transparent offensive cyber persistence exchanges disclosure for credible cyber deterrence, supports US strategic ends suited to offensive cyber capabilities, mitigates the risks of compromise and escalation, and demands few additional resources. The primary mechanisms of persistence and disclosure implement key intragovernmental and scholarship recommendations for cyber deterrence while addressing the unique challenges of cyberspace. Consistent and transparent consequences will send a clear threat to malicious cyber actors, return the advantages of offense in cyberspace to US strategy, and facilitate new norms in cyberspace.

The concept of deterrence will remain as valid as the utility of influencing adversary decisions. The cumulative effect of malicious cyber activities already threatens national security.

Some argue persistent strategic competition in cyberspace tends toward stability below the use-of-force threshold, but it is unknown if malicious cyber actors are actively attempting to cross that threshold. The US must demonstrate offensive cyber capabilities not only to influence the cost-benefit analysis of malicious cyber actors. It must also advance discourse among allies, promote international norms, upgrade perceptions of US power, and force strategic dilemmas on malicious cyber actor enablers who seek cost-effective strategies to attack the United States.

DISCLAIMER

The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

NOTES

1. Cybersecurity and Infrastructure Security Agency (CISA), *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, Virginia: CISA, October 26, 2020), 11, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf , CISA reported $242B was the median estimate in a range from $1B to over $7T.
2. Zhanna M. Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime* (San Jose, California: McAfee, December 2020) 3, 27-32, https://www.csis.org/analysis/hidden-costs-cybercrime .
3. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 3.
4. Specifically, the 2020 US Cyberspace Solarium Commission, 2017 Defense Science Board Task Force on Cyber Deterrence, and the 2018 US Department of State Recommendations to the President.
5. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly 92, no. 1,* (2019): 12.
6. Jacquelyn Scheider, Emily Goldman, Michael Warner, Paul Nakasone, et al., *Ten Years In: Implementing Strategic Approaches to Cyberspace* (Newport Papers, 2020), 35-36; Dr. Emily Goldman served as a strategist working for the Department of State and USCYBERCOM.
7. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly 92, no. 1,* (2019): 10-11.
8. Deloitte Development LLC, *Black-market Ecosystem: Estimating the Cost of Pwnership*, (Deloitte, December 2018), 21, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf.
9. Federal Bureau of Investigation (FBI), *Internet Crime Report 2020* (Washington, DC: FBI, 2020), 3, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf .
10. Scheider et al., *Ten Years ...*, 49; Dr. Chris Demchak is the RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies at the US Naval War College.
11. Federal Bureau of Investigation (FBI), "FBI Strategy Addresses Evolving Cyber Threat," last modified September 16, 2020, https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620.
12. Joint Chiefs of Staff, *Doctrine of the Armed Forces of the United States, JP 1* (Washington DC: Joint Chiefs of Staff, 2017), I-15.
13. Sen. Angus King and Rep. Mike Gallagher, The United States Cyberspace Solarium Commission (final report, Washington, DC: US Congress, March 2020), 26-34, https://www.solarium.gov/; The 2019 National Defense Authorization act chartered the CSC to address the challenge of increasing cyberspace attacks on the United States.
14. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats* (Washington, DC: Department of State, May 2018), https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf .
15. Department of Defense, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* (Washington, DC: Department of Defense Science Board, February 2017), 1-7, https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.
16. Joseph Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016): 44-71; Dr. Joseph Nye, Jr. is University Distinguished Service Professor at Harvard University.
17. Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-135; Will Goodman advised Senator Patrick Leahy and the Assistant Secretary of Defense for Homeland Defense and Global Security.
18. Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," Orbis 61, no. 3 (2017): 381-393; The authors' concept of continuous interaction shaped USCYBERCOM's concept of persistent engagement. Dr. Fischerkeller is a researcher in the Institute for Defense Analyses and Dr. Harknett is Professor and Dept. Head of Political Science at the University of Cincinnati.
19. Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology 31,* no. 3 (2018): 339-355; Mariarosaria Taddeo is Associate Professor and Senior Research Fellow, Oxford Internet Institute, University of Oxford.
20. Scheider et al., *Ten Years...*, 38-40.
21. Avoiding attribution and, in that, retribution is key for malicious cyber actors to preserve favorable cost-benefit tradeoffs for cyber activities.

NOTES

22. Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 9.
23. Biden, *Interim National Security Strategic Guidance*, 18.
24. Trump, *National Cyber Strategy*, I, 21.
25. Department of Justice, "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" (Washington DC: Department of Justice, July 19, 2021), https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.
26. Department of Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority" (press release, Washington, DC: Department of Treasury, April 15, 2021), https://home.treasury.gov/news/press-releases/jy0127.
27. Department of Justice Office of Public Affairs, "Russian National Charged with Interfering in U.S. Political System," last updated October 19, 2018, https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system; and "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," last updated December 19, 2018, https://home.treasury.gov/news/press-releases/sm577.
28. Department of Treasury, "Sanctions Related to Significant Malicious Cyber-Enabled Activities," accessed September 4, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities and Department of Justice, "search results for cyber indictment," accessed September 4, 2021, https://search.justice.gov/search?utf8=%E2%9C%93&affiliate=justice&sort_by=&query=cyber+indictment.
29. USCYBERCOM defensive actions provide substantial detail; See USCYBERCOM Public Affairs, "US Cyber Command, DHS-CISA release Russian malware samples tied to SolarWinds compromise," last updated April 15, 2021, https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/.
30. Nakasone, "A Cyber Force for Persistent Operations," 12.
31. Hearing before the Senate Committee on Armed Services, 116th Congress, February 14, 2019 (statement of General Paul Nakasone, Commander of US Cyber Command).
32. *Foreign Threats to the 2020 US Federal Elections*, National Intelligence Council (declassified report, Washington, DC: Director of National Intelligence, March 20, 2021), 3, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections .
33. David Verdun, "Cybercom's Partnership With NSA Helped Secure U.S. Elections, General Says," Department of Defense, last updated March 25, 2021, https://www.defense.gov/Explore/News/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/.
34. Cyberspace reprisals are unlikely to deter all malicious activities, such as cyberspace espionage. USCYBERCOM strikes may optimally supplement law enforcement responses to maximize costs when malicious cyber activities threaten national interests.
35. Cybersecurity and Infrastructure Security Agency (CISA), *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, Virginia: CISA, October 26, 2020), 9-16, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf; CISA also mentions that full costs are likely underrepresented in some datasets.
36. Deloitte, *Black-market Ecosystem*, 21, reported monthly cyber-criminal operating costs between $544 and $3,796.
37. Nakasone, "A Cyber Force for Persistent Operations," 11.
38. Evan Braden Montgomery, "Signals of Strength: Capability Demonstrations and Perceptions of Military Power," *Journal of Strategic Studies* 43, no. 2 (2020): 317-324; Montgomery also suggests demonstrating low observability, emerging capabilities is required to upgrade estimates of US power. Evan Montgomery is a Senior Fellow and Director of Research and Studies at the Center for Strategic and Budgetary Assessments in Washington, D.C.
39. Europol is the European Union Agency for Law Enforcement Cooperation; For additional information, see https://europa.eu/european-union/about-eu/agencies/europol_en.
40. Krebs on Security, "Attacks Aimed at Disrupting the Trickbot Botnet," last modified October 2, 2020, https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/; The unattributed operation neutralized bots and directly degraded control servers.

NOTES

41. Adam Kujawa et al., *State of Malware 2021,* Report (Santa Clara, CA: Malwarebytes Inc., 2021), 18, https://www.malwarebytes.com/resources/files/2021/02/mwb_stateofmalwarereport2021.pdf.
42. Intel471, "Recent Trickbot Disruption Operation Likely to Have Only Short-Term Impact," last modified October 13, 2020, https://intel471.com/blog/trickbot-disruption-microsoft-short-term-impact/ .
43. Europol, "World's Most Dangerous Malware Emotet Disrupted Through Global Action," Press Release, last modified January 27, 2021, https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action .
44. Check Point, Ltd., "Collaborative Global Effort Disrupts Emotet, World's Most Dangerous Malware," last modified 28 January, 2021, https://blog.checkpoint.com/2021/01/28/collaborative-global-effort-disrupts-emotet-worlds-most-dangerous-malware/; state and local government targeting is from CISA, "Emotet Malware," National Cyber Awareness System Alert AA20-280A, last modified October 24, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-280a.
45. Check Point, Ltd., "Collaborative Global Effort."
46. Kujawa et al., *State of Malware* 2021, 18.
47. Department of Justice Office of Public Affairs, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," last updated June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside; Colonial Pipeline paid 75 bitcoins to Darkside as ransom to restore critical data.
48. Intel471, "The Moral Underground? Ransomware Operators Retreat After Colonial Pipeline Hack," last updated May 14, 2021, https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.
49. There are more examples publicly available; for example, FBI cyber and non-cyber actions targeting Game Over Zeus in 2014 caused it to "never return to its previous scale" as described in https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group; for more recent operations, see https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.
50. Parties likely to verify a reprisal include third party cybersecurity researchers and malicious cyber actors' affiliates and sponsors.
51. Nye, "Deterrence and Dissuasion in Cyberspace," 48, 60.
52. Johanna Martinsson, "Global Norms: Creation, Diffusion, and Limits" (World Bank: Washington, DC, 2011), 4, 8, https://openknowledge.worldbank.org/handle/10986/26891.
53. Martinsson, Global Norms, 22.
54. Christopher Ford, "Rules, Norms, and Community: Arms Control Discourses in a Changing World," (remarks of Dr. Ford, Under Secretary of State for Arms Control and International Security, to the European Union in Brussels, December 13, 2019) https://2017-2021.state.gov/rules-norms-and-community-arms-control-discourses-in-a-changing-world/index.html.
55. Symantec, "Trickbot: U.S. Court Order Hits Botnet's Infrastructure," last modified October 12, 2020, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption.
56. US Department of Justice, "Latvian National Charged for Alleged Role in Transnational Cybercrime Organization," last modified June 4, 2021, https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization.
57. Tim Stevens, "A cyberwar of ideas? Deterrence and norms in cyberspace." Contemporary Security Policy 33, no. 1 (2012): 148-170, 156-157; Dr. Tim Stevens is Senior Lecturer in Global Security at King's College London.
58. Reprisal target system administrators would likely identify exposed accesses as a plausible source of information but may also downplay or deny the extent of any network penetration.
59. Evan Braden Montgomery, "Signals of Strength," 316.
60. Michael Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review* (2019): 267-287.
61. Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," accessed June 14, 2021, https://tnsr.org/2020/02/coercion-theory-a-basic-introductionfor-practitioners/.
62. Joint Chiefs of Staff, *Cyberspace Operations, JP 3-12* (Washington, DC: Joint Chiefs of Staff, 2018), II-7.

NOTES

63. Michael Warner, "US Cyber Command's First Decade," *A Hoover Institution Essay, Aegis Series Paper,* no. 2008 (2020): 14-18.
64. Hearing before the Senate Committee on Armed Services, 117th Congress, March 25, 2021 (statement of General Paul Nakasone, Commander of US Cyber Command).
65. Hearing before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, 116th Congress, March 4, 2020 (statement of General Paul Nakasone, Commander of US Cyber Command).
66. "Cyber Mission Force Achieves Full Operational Capability," USCYBERCOM Public Affairs, last modified May 17, 2018, https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/.
67. USCYBERCOM Public Affairs, "A Command First: CNMF trains, certifies task force in full-spectrum operations," last updated June 7, 2021, https://www.cybercom.mil/Media/News/Article/2647621/a-command-first-cnmf-trains-certifies-task-force-in-full-spectrum-operations/.
68. Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the 117th Congress Senate Armed Services Committee, March 25, 2021 (testimony of General Paul Nakasone, Commander of US Cyber Command).
69. Warner, "US Cyber Command's First Decade," 9; and Department of State, "Joint Statement on Advancing State Behavior in Cyberspace" (joint statement, Washington, DC: Department of State, September 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.
70. Information advantage is an emerging doctrinal concept. This definition is based on an Army strategic leader's presentation to the US Army War College on November 9, 2021.
71. Based on consensus reached during the author's operational planning with senior leaders in USCYBERCOM and partner forces from January – April 2021.
72. Basil H. Liddell Hart, Part IV, "Fundamentals of Strategy and Grand Strategy," in Strategy, 2nd ed. (New York: Penguin, 1991), 359.