U.S. Cyber Deterrence:
Bringing Offensive Capabilities into the Light

This research article was awarded third place in the 2022 CJCS National Defense and Military Strategy Essay Competition within the Strategic Research Paper category. While many students at JFSC achieve a high level of research, papers submitted to the competition represent some of the best research, writing, and thinking completed each academic year at Professional Military Education institutions. Manuscripts receiving recognition achieve an extraordinarily high bar. Other contest winners will be found at Joint Forces Quarterly.

Written by[1]
LCDR Stephanie Pendino,
MAJ Robert K. Jahn, Sr., and
Mr. Kirk Pedersen

Ubiquitous internet connectivity supports many conveniences central to the modern American way of life but also makes the United States vulnerable to cyberattacks from strategic competitors like China, Russia, North Korea, and Iran. The U.S. strategy to deter this threat has been largely defensive in nature, a posture of deterrence by denial. When U.S. policymakers have waded into the realm of deterrence by punishment, few have included explicit threats of cyber response in their pledges to "impose cost" on aggressors. The United States should pursue a declaratory cyber deterrence policy that includes the use of offensive cyber operations (OCO) against nation-states that violate clearly articulated norms. In order to do this effectively, however, U.S. policymakers must tailor historical notions of deterrence to the cyber domain, define realistic red lines, and navigate myriad political challenges.

Concepts of Deterrence

The concept of absolute nuclear deterrence has been effective largely due to the fear of mutually assured destruction (MAD). One contributing factor to the effectiveness of nuclear deterrence is the demonstrated U.S. resolve to use a nuclear weapon if necessary, as evidenced by the bombings of Hiroshima and Nagasaki at the end of World War II. There have been two potential nuclear flashpoints since: the Taiwan Strait crisis from 1954-1958 and the Cuban missile crisis in 1962. Since no nuclear attacks occurred, one could argue that deterrence worked. The Cold War, however, revealed that nuclear deterrence alone did not prevent all Soviet military provocations. One of the lessons of the Cold War was that integrating nuclear deterrence with all instruments of national power – diplomatic, informational, military, and economic (DIME) – was more effective than MAD alone. In addition to the fear of uncontrollable escalation, ethical considerations and political realities, such as the loss of public and allied support, helped to prevent the use of nuclear weapons against the same nation-states the United States now faces in the cyber domain.

[1] The views expressed are those of the author(s) and do not reflect the official policy or position of Joint Forces Staff College, National Defense University, the Department of Defense, or the U.S. Government.

Cyber warfare, however, is different from nuclear warfare in two obvious ways. First, the stakes are lower. Despite the possibility that large-scale cyberattacks could result in catastrophic effects, cyberattacks are mostly non-lethal, resulting in the loss of economic capital or information. Second, while a nuclear exchange has thankfully never occurred, cyber conflict between nation-states is a daily occurrence. GEN Paul Nakasone, Commander, U.S. Cyber Command (USCYBERCOM), notes: "Today peer- and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns."[1] Over the past twenty years, China, Russia, Iran, and North Korea have learned to employ OCO against the United States in ways that do not trigger a decisive military response. Such OCO falls into the category hybrid warfare, or actions taken under a "nonviolent revisionist grand strategy that seeks gains while avoiding reprisal through exploiting the gray zone between peace and war."[2] Whether one calls it "hybrid warfare," "gray zone conflict," or "strategic competition," the modern environment is in many ways more complex than the Cold War environment that gave rise to nuclear deterrence policies. For that reason, historic lessons about deterrence must be supplemented with new thinking.

Secretary of Defense Lloyd J. Austin III has offered the concept of integrated deterrence as the cornerstone of the upcoming U.S. National Defense Strategy (NDS). Integrated deterrence includes all domains of warfare (air, sea, land, space, and cyber), all instruments of national power (DIME), and the coordinated capabilities of allies and partners. It is integrated "across the spectrum of conflict from high intensity warfare to the gray zone."[3] Some of these concepts may not seem particularly new, but what has changed is the character of modern warfare and the way strategic competitors use hybrid techniques to erode the U.S.-led international rules-based order over time. The concept of integrated deterrence acknowledges and addresses these challenges in a useful way.

Cybersecurity has also importantly received significant U.S. policy attention over the past decade. President Obama was the first U.S. president to declare an emergency in cyberspace, levying sanctions in response to a North Korean cyber hack of Sony Pictures.[4] President Trump also declared an emergency in cyberspace, banning certain telecommunications equipment classified as a "national security risk" from use by U.S. companies.[5] President Biden signed an Executive Order aimed at improving the nation's cybersecurity.[6] At the operational level, the U.S. Department of Homeland Security (DHS) has made significant strides toward protecting U.S. critical infrastructure by partnering with private industry, while USCYBERCOM has employed increasingly sophisticated Defensive Cyber Operations (DCO) to protect military networks from malicious cyber actors. Most recently, GEN Nakasone has advanced principles of a "persistent [cyber] force" that "defends forward" to neutralize threats at the source.[7] Such concepts, however, are still defensive in nature, with U.S. officials generally shying away from framing OCO as a component of deterrence. Retaliatory OCO is only one tool in an integrated deterrence posture, but it is a valuable tool that, openly and assertively leveraged, could benefit the United States. The U.S. OCO capability is robust and varied enough to conduct limited retaliatory actions while retaining its greatest capabilities for wartime.

Since the historic model of *absolute nuclear deterrence* has little to offer cyber warfare, and *deterrence by denial* has not quelled the onslaught of cyber aggression, a new framework for cyber deterrence is needed. This study proposes *selective cumulative deterrence* as that framework. “Selective” in this case refers to the notion that not every nation-state cyberattack will reach the threshold of a response, nor warrant public notification. “Cumulative” describes a model in which proportional OCO are conducted in response to aggressor cyberattacks repeatedly over time. Selective cumulative deterrence is based in part on a 2017 *Journal of Strategic Studies* article, in which Uri Tor presents a concept of cumulative cyber deterrence based on historic Israeli conventional deterrence. As Tor describes it, the concept depends upon “a short burst of violence, as an inherent part of the ‘learning process’ between the parties. This strategic interaction is meant to lead the deterred party to understand the ‘red lines’ of the deterring party.”[8] Far from being “absolute,” such a model of deterrence is highly flexible. It does, however, depend entirely upon the clear communication of red lines and a U.S. willingness to respond when they are crossed.

Cyber Red Lines and Responses

Essential to any concept of deterrence is an unambiguous understanding by all parties of what actions would result in retaliation. Red lines in the realm of nuclear deterrence are generally clear; a nuclear attack warrants a nuclear response. Likewise, the United States has demonstrated that any lethal attack on Americans may result in a lethal response. Such retaliation has most often been against terrorist groups, though the 2020 drone strike against Iranian Islamic Revolutionary Guard Corps-Quds Force commander Qasem Soleimani demonstrated a U.S. willingness to strike an individual in the direct employ of a nation-state.

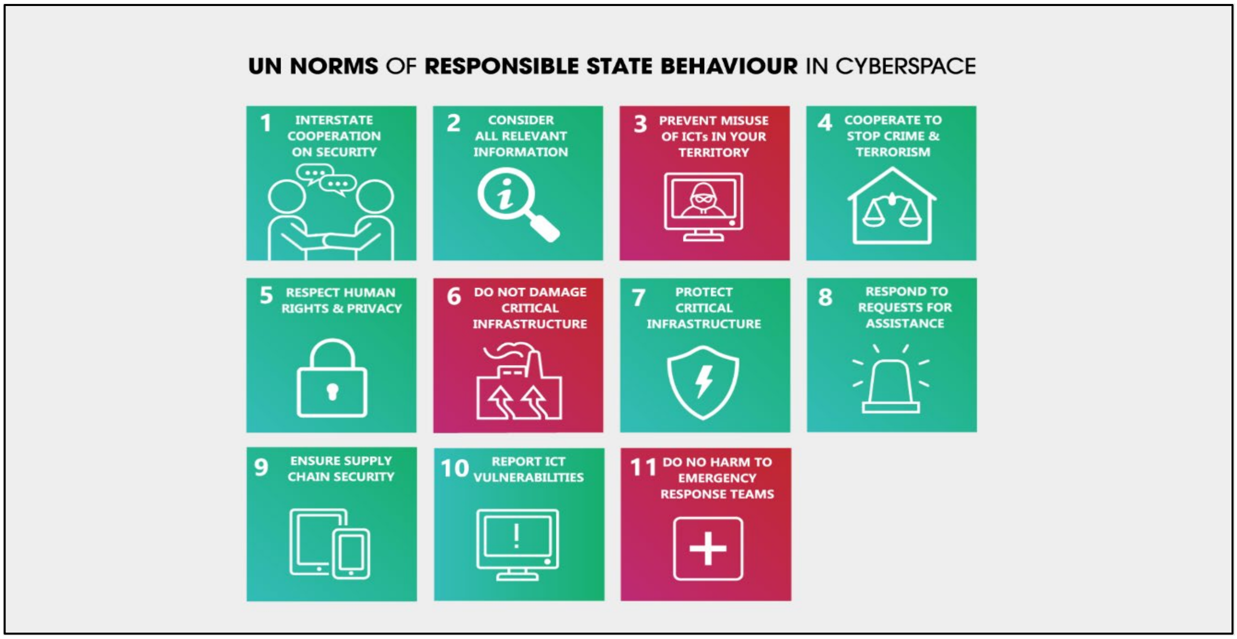
Setting red lines in cyberspace is more complicated. President Biden took steps in this direction in 2021, when he handed Vladimir Putin a list of 16 areas of U.S. infrastructure that should be “off limits to attack, period.”[9] Biden subsequently told the press: “I pointed out to him that we have significant cyber capability. And he knows it. He doesn’t know exactly what it is, but it’s significant. And if, in fact, they violate these basic norms, we will respond with cyber.”[10] This declaration is a meaningful step toward the central argument of this study, but the nuance of Biden’s threat to Putin lessens its value. Biden was referring to the 16 Critical Infrastructure Sectors identified by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which include such broad categories as “Communications,” “Financial Services,” and “Information Technology.”[11] Unless it was accompanied by more specific criteria, a broad warning to Putin to stay away from every corner of U.S. cyberspace may not serve as a credible deterrent. Political scientist and former Assistant Secretary of Defense Joseph Nye argues that Biden’s warning should have focused more on the “amount of damage done, not where or how it is done,” offering the analogy that one does not tell a party host to turn off all their music, “you warn them that if the noise becomes intolerably loud, you will call the police.”[12]

Nye goes on to argue that the United States must identify the norms by which it will abide, and “[w]hen Russia crosses such a line… be prepared with targeted retaliation, such as emptying the bank accounts of some privileged oligarchs, releasing embarrassing information or disrupting Russian networks.” However, while Nye asserts that deterrent statements should be delivered through “a process of quiet communication,”[13] in some cases, in order to deter proscribed activities, overt and public deterrent statements could be more effective. While there is certainly value in private conversations (i.e., threats) between world leaders, there is also value in a Rose

Garden speech that lays it bare for all to see: *There are countries that are not following the rules . . . this is what they have done to us . . . this is what we will no longer tolerate . . . this is how we will respond.*

Identifying the norms from which a U.S. cyber deterrence policy might proceed is simple in theory, if a bit harder in practice. The first step is identification of intolerable malicious cyber activities that the United States would classify as "out of bounds," for example: stealing intellectual property to benefit private industry, targeting the finances of innocent citizens, covertly influencing democratic elections, shutting down infrastructure to cause human suffering, or (except in the context of open war) degrading critical military capabilities. It follows logically that there are "in-bounds" malicious cyber activities, such as cyber espionage against government networks, which may warrant a response but do not "break the rules" in the same way as the red lines.

While the United States must develop its own cyber red lines, it can certainly anchor them to norms already propagated by the United Nations (UN). Figure 1, below, shows a list of 11 non-binding norms for "responsible state behavior in cyberspace," as developed in 2015 by a UN body known as the Group of Government Experts (GGE).[14] The norms most relevant to this study are prohibitions on: (1) allowing one's territory to be used for "for internationally wrongful acts using ICTs [Information and Communication Technologies]," and (2) "ICT activity . . . that damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."


UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

1 INTERSTATE COOPERATION ON SECURITY

2 CONSIDER ALL RELEVANT INFORMATION

3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY

4 COOPERATE TO STOP CRIME & TERRORISM

5 RESPECT HUMAN RIGHTS & PRIVACY

6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE

7 PROTECT CRITICAL INFRASTRUCTURE

8 RESPOND TO REQUESTS FOR ASSISTANCE

9 ENSURE SUPPLY CHAIN SECURITY

10 REPORT ICT VULNERABILITIES

11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Figure 1: Non-Binding UN Norms for Responsible State Behavior in Cyberspace. Red blocks pertain to the use of offensive cyber operations. Source: Government of Australia, "UN Cyber Norms: Resources," Accessed on March 12, 2022, https://www.internationalcybertech.gov.au/un-cyber-norms-resources.

The United States, China, and Russia were among the twenty founding members of the GGE. While China and Russia have subsequently violated these norms, they have also publicly pushed for the UN to condemn even the mere development of OCO capabilities, denying that they themselves have such programs.[15] The United States, on the other hand, has advocated for speaking transparently about OCO.[16] While this study calls for a more explicit deterrence policy, it also acknowledges the United States' open inclusion of OCO in its military doctrine.[17] The ability of the United States to point to UN norms when establishing a cyber deterrence policy would be beneficial; U.S. policymakers might truthfully say: "We possess and will use OCO for our national defense, but we have not and will not, target critical infrastructure, support or condone criminal activity from within our borders, or otherwise violate the UN norms to which we all agreed. China and Russia, on the other hand, violate them daily."

Setting red lines, however, is only half of a deterrence policy; the more challenging half is enforcing those red lines in a way that is acceptable and effective. The United States cannot simply retaliate "in kind" to out-of-bounds cyberattacks if it hopes to maintain moral credibility and advance the types of norms described above. Given that restraint, it is necessary to ask: What OCO options are on the table? Figure 2 broadly categorizes the range of OCO effects as a starting point for considering that question.

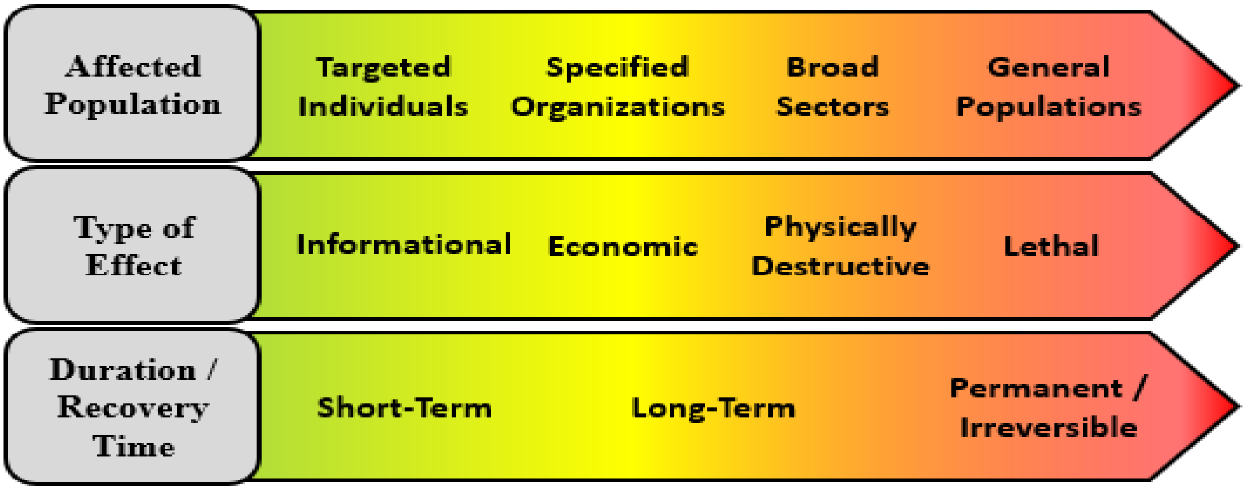


Figure 2: Spectrum of Offensive Cyber Operation Effects, where green imposes less cost and red imposes the most cost. Source: Kirk Pedersen.

While OCO effects must always be tailored to the adversary and situation at hand, in a very general sense, the effects at the left and center of the spectra above are suitable for U.S. cyber deterrence during strategic competition. OCO that damages critical public infrastructure is in contravention to GGE norms and is something the United States might wisely avoid in any deterrence policy. More broadly, OCO that indiscriminately impacts a civilian population is contrary to prevailing U.S. values and is likely to damage the United States' international reputation. On the other hand, OCO that responds to a cyberattack by targeting government or military leaders and organizations is not contrary to GGE norms and is likely to receive greater public support than the preceding examples. The previous hypothetical response options cited by Nye (emptying oligarch bank accounts, releasing embarrassing information, disrupting government networks) and OCO targeting military operations are examples of what the United States could credibly and acceptably threaten as part of a deterrence posture. Of course, USCYBERCOM must consider the gain and loss associated with any single-use cyber effect.

A significant risk in exercising cumulative deterrence in cyberspace is the possibility of escalation: What is to prevent an adversary from "retaliating to our retaliation," or graduating to a response in the physical domain? This is not an easy problem to solve, and one that warrants its own line of research. That said, there are two obvious ways to mitigate at least some of the associated risk.

First, U.S. policymakers must communicate red lines and response options plainly and publicly, along with a clear assertion that any escalation with further out-of-bounds cyber or physical effects would be viewed as blatantly hostile, potentially as an act of war. Ideally, such communication would occur jointly with allies and in the context of burgeoning international norms. This is not to suggest that public pressure alone will eliminate rogue nations' tendency to disregard those norms, but a U.S. deterrence message with unprecedented clarity, specificity, and gravity might at least give them pause. Second, the risk of escalation can be mitigated with anticipatory DCO that reduces risk from the most catastrophic cyber retaliations. As early as 2006, U.S. military strategy specified that OCO should be deployed in conjunction with mutually supportive DCO to protect against "reverse operations."[18] USCYBERCOM and others involved in national-level cybersecurity, such as DHS and the Federal Bureau of Investigation (FBI), must anticipate most-likely adversary escalations and integrate tailored DCO (to include defending forward) into OCO planning. Indeed, superior U.S. DCO capability is as crucial as OCO in pursuing a cumulative cyber deterrence posture.

Political Considerations

Having explored a basic framework for U.S. cumulative cyber deterrence, it is necessary to ask whether such a posture is politically realistic. Past reticence by U.S. policymakers on the topic of OCO suggests a challenge. Excepting President Trump's 2018 confirmation that the U.S. government targeted a Russian troll farm and GEN Nakasone's 2021 acknowledgment that USCYBERCOM acted against criminal ransomware groups, the United States rarely acknowledges specific uses of OCO.[19] U.S. involvement in state-on-state cyberattacks like Stuxnet remains a tacit implication only. This reticence is consistent with official U.S. strategy, which leans into the concepts of defending forward and imposing cost without ever casting OCO as a means of doing so.[20] The congressional Solarium Commission addressed this challenge in its 2020 report, stating: "America's commitment to international law appropriately places constraints on its willingness to implement deterrence by punishment in cyberspace." Although, the commission noted that if OCO were used in a retaliatory fashion, a "preferred punishment strategy" would entail targeting only government networks.[21] This inclination is consistent with the recommendations of this study.

Policymaker skittishness on the topic of OCO is unsurprising, given historic statements by U.S. officials warning of a "cyber 9/11," "cyber Pearl Harbor," and "cyber Armageddon."[22] Such hyperbolic narratives, coupled with the fact that many Americans have experienced cyber effects like ransomware and identity theft, have undoubtedly fostered a perception that OCO are "dirty tricks" best left to our adversaries. As savvy U.S. leaders seek to normalize the idea of cyber as a domain of warfare (akin to land, sea, air, and space),[23] they struggle against a visceral discomfort among others. That said, incessant cyberattacks that harm the interests of ordinary U.S. citizens but fall far short of doomsday warnings undoubtedly affect public opinion; "fighting back" may be more broadly acceptable than it once was. It is reasonable to expect that strong public support or opposition would bear upon the viability of a cumulative cyber deterrence policy, though public opinion does not develop apart from government messaging; the two shape one another. The question is: Could policymakers persuade Americans to support a cumulative cyber deterrence policy?

There is limited data to answer this question. Literature that specifically explores public opinion about cyber deterrence is non-existent, and literature that more broadly explores public opinion about cyber warfare is rare and tends to focus on cyberterrorism and cybercrime. That said, some survey experiments do provide relevant data. Tomz and Weeks found high levels of support for retaliation against nations that covertly influence U.S. elections, with a strong preference for sanctions over military strikes.[24] Shandler, et al. queried levels of support for retaliation to both cyber and conventional terrorism and found that retaliatory cyber strikes were universally preferred to missile strikes, even in response to conventional terror attacks.[25] Hedgecock and Sukin found generally high levels of support for retaliation to cyberterrorism, but noted that certainty of attribution was a significant factor.[26] While these studies do not address the precise issue at-hand, their conclusions do support two broad assumptions when viewed in the political context described above.

First, there is no reason to believe that Americans fundamentally oppose the use of retaliatory OCO, though public support for cumulative deterrence would depend upon the case made by policymakers. To bolster support, U.S. officials could more clearly describe the implications of Chinese and Russian malicious activities. President Biden's ultimatum to Putin, his more recent condemnation of Chinese cyberattacks,[27] and GEN Nakasone's statements about hostile "strategic campaigns" show that such a narrative shift has begun – but the case could certainly be louder and more persuasive.

Second, public concerns about retaliation, collateral damage, and attribution may impact support for cumulative cyber deterrence. As proposed above, clarifying acceptable norms while strengthening DCO capabilities could reduce some of the risk associated with retaliation. With respect to collateral damage, the avoidance of civilian casualties is indeed the greatest selling point for military OCO. The desire to avoid casualties likely drove the preference for sanctions over kinetic military action in *Tomz* and the preference for cyber retaliation over missile strikes in *Shandler*. When it comes to avoiding collateral damage in a U.S. OCO retaliation, that is simply a matter of sticking to the acceptable response options stipulated in the deterrence policy. The U.S. preference to focus cyber effects on military or government targets creates an uneven playing field, but knowing this, USCYBERCOM can focus its tradecraft and access development efforts on such targets.

Regarding attribution, definitively identifying the perpetrator of a cyberattack remains an obvious prerequisite to mounting a response. That said, a 2022 Congressional Research Study paper pointed to the increasing speed and confidence of recent attributions, noting "it appears that attribution is no longer the barrier it used to be."[28] Further, on the question of whether to pursue declaratory deterrence, attribution is really a non-issue; any policy would simply need to specify that retaliation only occurs when attribution is certain, or of a high degree of certainty, or whatever confidence level meets public requirements. Meanwhile, USCYBERCOM and the intelligence and law enforcement communities can continue to focus on improving attribution capabilities. It is worth noting, however, that in the case of deterrence against nation-states, it is not always necessary to depend on technical capabilities for attribution, or to definitively tie a cyberattack to a specific location or group of individuals. As Rid and Buchanan (2015) put it, "attribution is an art as much as a science . . . [and] a function of what is at stake politically."[29] Strategic cues and context, bolstered by human intelligence or other non-technical evidence, may be all that is required to tie an attack to Chinese or Russian backing. Retaliatory OCO in such a case need not strike the specific point of origin of an attack to serve a deterrent purpose.

A final consideration relates to international political implications: How would the world react to a U.S. cyber posture that includes deterrence by punishment? Besides likely cries of hypocrisy from U.S. adversaries, it's possible that U.S. OCO could be viewed as contrary to GGE norms. It is important here to note that the GGE stipulated that its norms "do not seek to limit or prohibit action that is otherwise consistent with international law."[30] As described earlier, the United States openly acknowledges its OCO capabilities, pushing for universal acceptance of the GGE norms while simultaneously affirming its legal right to use OCO as a tool of national defense.[31] So long as the response falls within the bounds recommended by this study, it would be hard to argue that retaliation to a cyberattack violates any of the norms to which the United States or its allies have agreed. In the end, U.S. policymakers care most about the continued support of allies.

Fortunately, there is every indication that the United States' closest allies share its cyber worldview and might be willing partners in a shift to cumulative deterrence. Of particular note, the United Kingdom (UK) and Australia have significant, acknowledged OCO capabilities, and both have acted in general lockstep with the United States on all matters of cybersecurity. A 2020 study by the NATO Cooperative Cyber Defense Center of Excellence examined the OCO capabilities of the "Five Eyes" intelligence partnership (Australia, Canada, Great Britain, New Zealand, and the United States), finding a growing trend toward "collective response" to cyber threats.[32] The UK has recently moved in the direction of a more assertive cyber posture, publishing a 2022 National Cyber Strategy that is objectively more "offense-forward" than the 2018 U.S. strategy. This UK strategy notes a significant increase in UK OCO capability since establishment of a National Cyber Force (NCF) in 2020, and even makes the case (so elusive in U.S. strategy) that OCO is a way to impose cost and "deter and disrupt state, criminal and other malicious cyber actors."[33] Any U.S. policymaker willing to consider a change in cyber deterrence posture might look to UK and Australian collaboration as a means of shoring up political support, increasing access, and presenting a more defensible multinational face on the world stage.

Conclusion

In summary, the United States is under attack in the cyber domain, and a defensive posture alone has failed to dissuade competitors like China, Russia, North Korea, and Iran. It is time to make OCO a central part of U.S. integrated deterrence in the gray zone. A declaratory selective cumulative deterrence policy, based on a limited number of clearly articulated red lines, is the only way to drive toward a set of strategic competition norms in cyberspace. Cumulative cyber deterrence will not be an academic notion. It will entail actual retaliation, and a risk of escalation; however, clarity about red lines and acceptable responses, along with a U.S.-led effort to build multinational consensus on these norms, can help mitigate some of that risk. So too can superior DCO – the United States can never stop defending forward, and OCO must be paired with tailored, anticipatory DCO to protect against escalatory retaliations. Such a policy is only politically feasible if U.S. policymakers change the public narrative, moving away from a language of fear and toward a notion of cyber as a domain of warfare. Finally, this is an effort best pursued as a coalition; the United States has strong and willing allies who face the same threats and give every indication that they too are ready to fight back.

Notes

[1] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92, no. 1 (2019): 10-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

[2] Sean Monaghan, "Countering Hybrid Warfare So What for the Future Joint Force?" *PRISM* 8, no. 2 (2019): 82-99, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf.

[3] Jim Garamone, "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says," U.S. Department of Defense, December 8, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

[4] Laura B. West, "Building Cyber Walls: Executive Emergency Powers in Cyberspace," *Journal of National Security Law & Policy* 11 (2020): 591-633, https://jnslp.com/wp-content/uploads/2021/09/Building_Cyber_Walls_Executive_Emergency_Powers-in_Cyberspace_2.pdf.

[5] Ibid.

[6] Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity, 3 C.F.R. 26633-26647 (2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[7] Nakasone, "A Cyber Force."

[8] Uri Tor, "'Cumulative deterrence' as a new paradigm for cyber deterrence," *Journal of Strategic Studies* 40, no. 1-2 (2017): 92-117.

[9] Joseph S. Nye, "Will Biden's Red Lines Change Russia's Behaviour in Cyberspace?" *Australian Strategic Policy Institute: The Strategist,* July 8, 2021, https://www.aspistrategist.org.au/will-bidens-red-lines-change-russias-behaviour-in-cyberspace/.

[10] Ibid.

[11] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors," Last modified October 21, 2020, https://www.cisa.gov/critical-infrastructure-sectors.

[12] Nye, "Red Lines."

[13] Ibid.

[14] GGE, UN, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Seventieth Session, A/70/174, https://undocs.org/A/70/174 (2015).

[15] Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'," 2020, https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf.

[16] Ibid, 11.

[17] Joint Chiefs of Staff, *Cyberspace Operations,* JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[18] U.S. Department of Defense, *National Military Strategy for Cyberspace Operations* (Washington, DC: Pentagon, 2006), https://www.hsdl.org/?%20abstract&did=35693.

[19] David E. Sanger, "Trump Claims Credit for 2018 Cyberattack on Russia," *New York Times*, July 11, 2020, https://www.nytimes.com/2020/07/11/us/politics/trump-russia-cyber-attack.html; Julian E. Barnes, "U.S. Military Has Acted against Ransomware Groups, General Acknowledges," *New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.

[20] White House, *National Cyber Strategy of the United States of America* (Washington, DC: White House, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; U.S. Department of Defense, *Department of Defense Cyber Strategy* (Washington, DC: Pentagon, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[21] U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, DC: Solarium Commission, 2020), https://www.solarium.gov/report.

[22] Jacqueline Schneider, "A World Without Trust: The Insidious Cyberthreat," *Foreign Affairs* 101, no. 1 (2022): 22, https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust.

[23] Glenn A. Crowther, "The Cyber Domain," *Cyber Defense Review* 2, no. 3 (2017): 63, http://www.jstor.org/stable/26267386.

[24] Michael Tomz and Jessica L. P. Weeks, "Public Opinion and Foreign Electoral Intervention," *American Political Science Review* 114, no. 3 (2020): 868, https://www.cambridge.org/core/journals/american-political-science-review/article/public-opinion-and-foreign-electoral-intervention/AC34B6090EACF336D08713AF69BF7904.

[25] Ryan Shandler, Michael L. Gross and Daphne Canetti, "A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel," *Contemporary Security Policy* 42, no. 2 (2021): 145, https://www.tandfonline.com/doi/pdf/10.1080/13523260.2020.1868836.

[26] Kathryn Hedgecock and Lauren Sukin, "Responding to Uncertainty: The Importance of Covertness in Support for Retaliation to Cyber and Kinetic Attacks," February 26, 2022, http://laurensukin.com/Cyber.pdf.

[27] White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[28] Chris Jaikaran, *Cybersecurity: Deterrence Policy*, CRS Report No. R47011 (Washington, DC: Congressional Research Service, 2022), https://crsreports.congress.gov/product/pdf/R/R47011.

[29] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (December 2014), https://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.977382.

[30] GGE, UN.

[31] Gold, "Five Eyes," 11.

[32] Ibid, 24.

[33] Government of the United Kingdom, *National Cyber Strategy 2022* (London: HM Government, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.