Kybernao

Steering Toward the Nexus of Cyber Theory and Policy

Initiative Persistence as the Central Approach for US Cyber Strategy

Michael P. Fischerkeller, PhD

Richard J. Harknett, PhD

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Issue 1 July 2021

EXECUTIVE SUMMARY

Initiative Persistence as the Central Approach for US Cyber Strategy

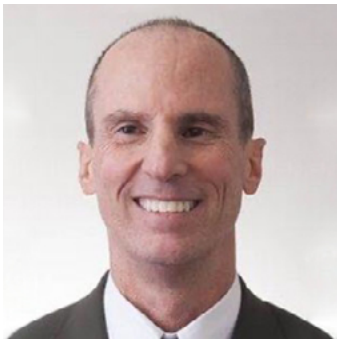
The Biden-Harris administration's recent focus on a strategic approach of defense to improve the cybersecurity of federal systems and networks, supply chains, and critical infrastructure is essential. However, it is a necessary but not a sufficient adjustment to U.S. cyber strategy. A more fundamental re-thinking is needed if the United States is to halt and ultimately reverse its loss of relative advantage from cyber campaigns targeting its political, economic, social, and organizational power.

In a new U.S. national cyber strategy, the central focus should be initiative persistence, a strategic approach to preclude, mitigate, and counter strategically consequential cyber action occurring continuously short of armed conflict. Acting together, defense, initiative persistence, and deterrence will provide cybersecurity across the full spectrum of strategic competition.

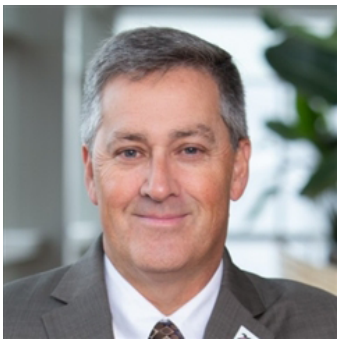
This strategy must be implemented through a Whole-of-Nation-Plus (WON+) framework connecting improved intergovernmental organization with more effective alignment of the public and private sectors, engagement of citizenry, and coordination of all three efforts with allies and international partners (the "plus" in WON+).

U.S. cyber strategy must pivot to the realities of the cyber strategic environment where initiative persistence, not ceding initiative, is the central strategic approach to achieving security.

About the Authors



Dr. Michael Fischerkeller is a research staff member in the Information, Technology and Systems Division at the Institute for Defense Analyses, a Federally Funded Research and Development Center. Michael has spent over 20 years supporting the Office of the Secretary of Defense, Joint Chiefs of Staff, and Combatant and Multi-National Force commanders. His areas of expertise are cyber strategy, strategic and operational concept development, and assessment.



Dr. Richard Harknett is professor and Head of the Department of Political Science at the University of Cincinnati. He co-directs the Ohio Cyber Range Institute and chairs the Center for Cyber Strategy and Policy. Professor Harknett has served as the inaugural scholar-in-residence at US Cyber Command and NSA and Fulbright Scholar at the University of Oxford, UK and the Diplomatic Academy, Austria. His published work covers international relations theory, cyber and international security studies.

This essay is a reprint of the Institute for Defense Analyses Publication NS D-22719, Initiative Persistence as the Central Approach for U.S. Cyber Strategy, Copyright 2021.

Introduction

The Biden-Harris administration's recent focus on a strategic approach of defense to improve the cybersecurity of federal systems and networks, supply chains, and critical infrastructure is essential.[1] However, it is a necessary but not a sufficient adjustment to U.S. cyber strategy, which has, for the better part of a decade, focused on deterrence as its central element. A more fundamental re-thinking is needed if the United States is to halt and ultimately reverse its loss of relative advantage from cyber campaigns targeting its political, economic, social, and organizational power. This must begin with a comprehensive national framework that aligns strategy effectively to the realities of the cyber strategic environment. In a new U.S. national cyber strategy, the central focus should be initiative persistence, a strategic approach to preclude, mitigate, and counter strategically consequential cyber action occurring continuously short of armed conflict. A complementary deterrence approach, no matter the adjective placed before it—conventional, cross-domain, multi-domain, integrated, cumulative, restrictive, or tailored—or the "ways" placed after it—punishment or denial—should be leveraged to support managing potential militarized crises and preventing armed conflict. Acting together, defense, initiative persistence, and deterrence will provide cybersecurity across the full spectrum of strategic competition.

In a new U.S. national cyber strategy, the central focus should be initiative persistence.

Cyber operations of armed-attack equivalence—important but "rare events"[2]—appear to be dissuaded through cross-domain deterrence.[3] However, the increasing scale and scope of strategically consequential cyber activity short of armed attack equivalence targeting the United States shows that deterrence with any adjective is failing to dissuade motivated adversaries cleverly seeking to cumulate strategic gains in this competitive space. Contrary to the views of some policymakers, ongoing strategic losses are not resulting from a poorly executed deterrence strategy or lack of effort, but rather from a poorly conceived overall framework (i.e., applying a strategic approach based on coercion to an environment of competition and exploitation).[4] U.S. efforts to adapt a deterrence strategy to quell competitive cyber behavior have resulted in an approach that defies the logic and findings of deterrence theory and supporting studies. The concept of deterrence is not merely being "stretched"; core axioms of deterrence theory addressing ambiguity and prohibitive costs are being

violated, leading to dangerous and persistent negative consequences for the United States and its allies as evidenced by the empirical record.[5] The policy implication is clear: deterrence should be applied where it can be effective—militarized crises and armed conflict—and not applied where it cannot—competition short of crises/armed conflict, the most common and strategically salient cyber activity.

U.S. cyber strategy must pivot to the realities of the cyber strategic environment where initiative persistence, not ceding initiative, is the central strategic approach to achieving security. If the United States continues to deny the imperative to engage persistently, it will continue to suffer negative strategic consequences. As cyber persistence theory predicts,[6] the United States has been punished through increasing losses to adversaries and will continue accruing losses without a re-balanced approach to cyber strategy that simultaneously allows it to gain the upper hand in the strategic competition short of armed conflict and deters armed attack-equivalent cyber operations.[7] It is time for a new chapter in U.S. national cyber strategy.

This strategy must be implemented through a Whole-of-Nation-Plus (WON+) framework connecting improved intergovernmental organization with more effective alignment of the public and private sectors, engagement of citizenry, and coordination of all three efforts with allies and international partners (the "plus" in WON+).

U.S. Cyber Command's (USCYBERCOM) doctrine of persistent engagement offers a guiding strategic principle derived from the characteristics of the cyber strategic environment that can be expanded to anchor U.S. national cyber strategy and a whole-of-nation-plus (WON+) framework for cybersecurity.[8] Whereas deterrence theory cedes initiative to adversaries, cyber persistence theory argues that the United States must seize and maintain the initiative to set the conditions of security in its favor in and through cyberspace. Initiative persistence is a continuous orientation toward anticipating the exploitation of vulnerability before it occurs, while simultaneously understanding how to exploit vulnerabilities of others to advance security interests. It is a principle that is equally valid for non-military instruments of national power and at strategic, operational, and tactical levels of engagement when applied to cyber-relevant activity. In addition, initiative persistence fosters better alignment between the public and private sectors in the United States. As such, seizing and maintaining the cyber initiative should be the guiding principle for U.S. national and department cyber strategies going forward, and it should be applied through a framework that institutionalizes initiative persistence across government, through improved alignment of the public and private sectors, through engagement of citizenry, and through coordination of all three efforts with allies and international partners (the "plus" in WON+).

As the Biden-Harris administration deliberates over what its national cyber strategy should comprise, it should take stock of the untenable state of U.S. cyber deterrence strategy today, how matters got to this point, why they endure, and what the United States must do to ensure cybersecurity across the full spectrum of cyber strategic competition, from ongoing, continuous campaigns short of armed conflict through potential operations in militarized crises and war.

Where the United States Stands Today

The policy record of the past 15 years is unambiguous. U.S. cyber strategies have consistently prioritized deterring cyber operations and campaigns targeting U.S. national interests. Equally clear is that adversary cyber operations and campaigns targeting U.S. interests over that period have increased in frequency, scope, scale, and sophistication.

This trend is not lost on members of the U.S. Congress. One of the most vocal critics of U.S. cyber strategy and policy was then-Chairman of the Senate Armed Services Committee, Senator John McCain. During a March 2017 hearing, McCain complained that the U.S. was projecting weakness in cyberspace that "has emboldened our adversaries." He continued, "As America's enemies seized the initiative in cyberspace, the last administration offered no serious cyber deterrence policy and strategy."[9] McCain was not alone in this assessment. In 2018, Senator Dan Sullivan argued, "We really haven't retaliated at all, whether it be Iran, North Korea, China, Russia. … We seem to be the cyber punching bag of the world, and it's common knowledge."[10] Senator Ben Sasse noted, "We're four years into regular attacks against the United States to which we publicly admit we don't respond, or we don't respond in any way that's sufficient to change behavior."[11] And Senator Angus King stated, "We are under attack and our adversaries feel no consequences, they fear no results, fear no response." [12]

The general view of these policymakers is that this state of affairs is a consequence of executing a deterrence strategy poorly due to the absence of declaratory policy and/or not trying hard enough. Let us consider these two explanations.

Declaratory Policy

Senator King recently stated that the United States has been missing a "clear, declaratory policy" to deter adversary cyber operations and campaigns, a notable claim given that the 2018 National Defense Authorization Act called on the Secretary of Defense to provide a "declaratory policy relating to the responses of the United States to cyber attacks of significant consequence."[13] But when examined from a strategic communication perspective, the United States has, in fact, consistently made a choice to acknowledge a cyber deterrence declaratory policy that is firmly rooted in strategic ambiguity.[14] At a press conference following the

release of the 2011 Department of Defense Strategy for Operating in Cyberspace, when asked to define acts of cyberwar, Deputy Secretary of Defense William Lynn said, "there is some value in keeping it somewhat ambiguous, as a deterrent."[15] Four years later, this logic was expanded well beyond "acts of cyberwar." The Obama administration's 2015 report to Congress on cyber deterrence described an activity that supports deterrence: "Promoting a nuanced and graduated declaratory policy and strategic communications that highlight the United States Government commitment to using its capabilities to defend against cyberattacks, but remains ambiguous on thresholds for response and consequences to discourage preemption or malicious cyber activities just below the threshold for response."[16] The U.S. Department of State (DOS) has worked "to promote acceptance of and adherence to the U.S.-developed framework of responsible state behavior in cyberspace" and has been working within interagency and international partners to build a shared capacity to swiftly impose consequences when "adversaries transgress this framework."[17] Although the unclassified precis of the DOS' Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats calls for a policy to be declared publicly and privately that provides criteria for the types of malicious cyber activities that the U.S. government will seek to deter (read: thresholds), no such unambiguous declaration has been forthcoming. Presumably, the "framework" remains a reference to norms of state cyber behavior described in 2015 and 2021 United Nations Group of Government Experts reports.[18] The non-binding, voluntary nature and non-specific character of these norms is consistent with a U.S. preference for ambiguity. This preference also carries over to U.S. positions taken on international law applied to the context of cyberspace, specifically with regard to the United Nations Charter. Although U.S. leadership has agreed that the Charter applies, it has not been specific regarding how it applies, thereby foregoing an opportunity to reduce ambiguity by making clear any specific thresholds whose breach would be characterized as an internationally wrongful act.[19]

The U.S. declaratory policy of strategic ambiguity extends also to threats of punishment should adversaries breach its ambiguous thresholds. Over the past decade, threats have taken a similar form. The White House's 2011 International Strategy for Cyberspace states that, in response to hostile cyber acts, "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests."[20] In 2015, then-Secretary of Defense Ashton Carter noted that "President Obama has said that we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power."[21] And, most recently, when asked about the SolarWinds breach, White House Press Secretary Jennifer Psaki stated, "We've spoken about this previously...of course we reserve the right to respond at a time and manner of our choosing to any cyberattack."[22]

Not Trying Hard Enough

The second policymaker explanation for deterrence failure is that the United States is simply not trying hard enough. In the lexicon of deterrence theory, this would equate with a failure to threaten prohibitive costs. Importantly, it is not the mere promise of a threat to respond that deters, but rather a threat to exact costs that outweigh the gains a would-be attacker is seeking through a cyber operation or campaign. If a motivated actor cannot be persuaded those costs will be prohibitive, it will not be deterred. Likewise, if costs imposed after a cyber operation to re-set deterrence are not viewed as prohibitive, the actor will not be deterred. Merely imposing costs alone is not sufficient—they must be costs that outweigh the attacker's expected gain. If committed to the logic of a deterrence approach, U.S. policymakers must assume that adversaries persistently pursuing gains in and through cyberspace have factored in costs and will continue to act unless and until the costs threatened or imposed are not simply high but are prohibitively high.

Over the past several years, the United States has repeatedly applied the same cost-imposition playbook after being targeted by adversary cyber operations or campaigns short of armed conflict, including "smart" economic sanctions, indictments, naming and shaming through public attribution, diplomatic sanctions, and, on occasion, a cyber operation—with all response actions being consistent with U.S. values and international law, including, but not limited to proportional responses.[23] Guided by these principles, the United States has been imposing costs using all instruments of national power. That adversary behaviors continue largely unabated suggests that prohibitive costs have not been threatened or imposed, leading some U.S. policymakers to argue the U.S. is not trying hard enough. But other U.S. policymakers believe that costs will accumulate over time to a point of becoming prohibitive.[24] Such beliefs assume time is on one's side and that adversaries will not adapt to absorb and circumvent costs.[25]

Summary

The argument that the United States lacks a clear declaratory policy for cyberspace is unsupported. In statements and guidance over the last decade, U.S. policymakers have been deliberate, intentional, consistent, and clear regarding cyber deterrent declaratory policy—it is a policy of strategic ambiguity. Nor is the argument that the United States has not tried hard enough to impose prohibitive costs supported. Policymakers have used all instruments of national power guided by a moral and legal framework. This policy of ambiguity seems to be effective in dissuading cyber operations of armed attack equivalence as no state has yet attacked the United States in or through cyberspace at a scale, scope, and severity that could be considered armed conflict. The policy has failed, however, to deter states seeking to cumulate strategic gains through cyber-enabled ways and means short of armed conflict.

How This State of Cyber Insecurity Came About

If deterrence failure short of armed conflict cannot be attributed to the factors identified by policymakers, what accounts for it? Two explanations stand out, both of which derive from the distinct features of the cyber strategic environment.[26] First, in efforts to adapt a deterrence-based approach to the cyber strategic environment, the logic of deterrence theory in regard to ambiguity has been contorted, thereby rendering the approach ineffectual. Second, assumptions that time is on the United States' side and that adversaries are incapable of adapting to sanctions are invalid in the cyber strategic environment that, in fact, inhibits the accrual of prohibitive costs and facilitates the circumvention of sanctions. We examine these explanations in turn.

Strategic ambiguity is a declaratory posture.

The concept of strategic ambiguity has played a central role in U.S. cyber deterrence policy. In his discussion of credible commitments in deterrence, Thomas Schelling argued that if a commitment is ill-defined and ambiguous—if it leaves the deterrer loopholes through which to exit—adversaries "will expect [the deterrer] to be under strong temptation to make a graceful exit (or even a somewhat graceless one)."[27] Ambiguity in this context signals primarily a desire to not respond or a lack of capacity to respond, as well as a hope that neither is tested. The attacker reads it more as bluff than resolve. Richard Ned Lebow made a similar argument, noting, "Flexible commitments, which appear to limit the would-be deterrer's cost of disengagement, are hardly likely to be interpreted as impressive indications of resolve."[28] In addition, Glenn Snyder and Paul Diesing argued that "maximum explicitness and clarity produce maximum credibility, because explicitness engages the national reputation while imprecision allows states to evade some of the ignominy of backing down."[29] These core deterrence studies reveal that ambiguity was never considered a central principle of deterrence effectiveness expressed in either (or both) the specification of a deterrence threshold or the threatened punishment that would occur should a threshold be breached.

In their empirical study of cases before the era of cyberspace, Snyder and Diesing found that, to avoid entrapment, states tend to choose ambiguity and flexibility even though specificity would increase deterrence credibility.[30] The underlying dynamic is providing a way out of a commitment, rather than increasing the likelihood of deterrence. When a state wishes to keep its

options open but also appear credible, it may choose to make its thresholds and punishments somewhat explicit in the hope of presenting at least the appearance of credible commitment. Snyder and Diesing described this trade-off approach to making commitments as "keeping them guessing."[31] The approach attempts to gain coercive leverage by introducing uncertainty into an opponent's calculations but comes with an important consequence—it invites probing and operations designed to avoid having to come close to "guessing." Schelling argued that ambiguity leads to "the low-level incident or probe, and tactics of erosion."[32] Given the nature of the cyber strategic environment, where states have learned they can cumulate strategic gains through such tactics, the consequences of deterrence failure resulting from ambiguity is becoming increasingly consequential.

Strategic ambiguity invites operations that come close but avoid nearing the ambiguous thresholds.

Whether a "keep them guessing" approach is effective relies on the aggressor's image of the deterrer as applied to the set of opportunities through which the aggressor is considering advancing its interests. If the deterrer has stockpiled credibility by compiling a record of effectively imposing prohibitive costs or of acting tougher than any previous declarations had indicated, the deterrer can get some coercive leverage out of ambiguous commitments. This, however, appears to hold in a very narrow set of conditions—essentially, to a recent victory in war or a salient punishment effectively applied. Schelling pointed to another image that may give pause to potential aggressors—a deterrer having a reputation for impetuosity, irrationality, or not being in control of the foreign policy action of one's state.[33] As applied to the United States, he noted that "it is hard for a government, particularly a responsible government, to appear irrational whenever such an appearance is expedient."[34] Moreover, he argued that "the American government ought to be mature enough and rich enough to arrange a persuasive sequence of threatened responses that are not wholly a matter of guessing a president's temper."[35] In addition, "We ought to get something a little less idiosyncratic for 50 billion dollars a year of defense expenditure [$714B in 2020]."[36] Thus, he noted, "We have to substitute brains and skill for obstinacy or insanity."[37] While originally published in 1966, Schelling's arguments still resonate today.

Views of the United States

In a deterrence dynamic, the credibility of a deterrer is in the eyes of the aggressor. Given that some U.S. Congressional leaders do not view the United States as a credible foe, it should not be surprising that U.S. adversaries hold the same view. James Lewis noted that, in discussions with an interlocutor with ties to the Russian Federal Security Service, the individual shared, "After the [2016] election interference, we waited for the U.S. response and were surprised when nothing happened." Similarly, Lewis noted that a Chinese general, when asked about the risk of engaging with the United States in cyberspace, replied that it [the United States] had "great capabilities, no will."[38] These are overstatements, of course; something did happen after 2016, the United States does have will, and neither Russia nor China have paused ("waited") the operational tempo of their cyber activities. That said, the inference cannot be ignored—the United States has not been viewed as credible in the cyber competitive space short of armed conflict. Three sources of this perception are likely the ambiguity of the U.S. commitment, a conclusion that prohibitive costs have yet to be imposed for strategic cyber activity short of armed conflict, and a publicly stated concern by U.S. policymakers that U.S. national interests are asymmetrically vulnerable in and through cyberspace. We have already addressed the first source, and so we now focus on prohibitive costs and asymmetric vulnerability.

As noted previously, the United States has consistently gone to the same well for punishments after being targeted by malicious cyber activities: "smart" economic sanctions, indictments, naming and shaming through public attribution, diplomatic sanctions, and episodic cyber actions. Also noted previously is that decision makers, if acting strategically, must be concluding that the impact of such sanctions will cumulate over time to a point of presenting prohibitive costs. The cyber strategic environment, however, rewards operational persistence, not operational restraint, and so sanctioned states do not sit idly by as time passes. Consequently, the cumulative effects of sanctions simply do not, and arguably cannot, offset the cumulative gains adversaries accrue through continuous cyber operations short of armed conflict. Indeed, the trajectories of the two over time are mirror images. With the strategic value of imposed costs diminishing over time and the strategic value of cumulative gains increasing, a prohibitive cost threshold that might deter future behavior will never be reached.[39] Moreover, the advent of cyberspace has provided creative states with novel ways and means to directly circumvent the impact of sanctions, a troubling development given their already weak empirical track record.

A study of the effectiveness of U.S. economic sanctions generally (nearly 200 cases over a 30-year period) concludes that they achieve their policy goals only 30% of the time and that their impact diminishes over time as the targeted state devises sanction evasion techniques.[40] A United Nations study of "smart" economic sanctions finds that their overall effectiveness is less than 25% and that their effectiveness at coercing a change in behavior is only 10%.[41] Case studies of extraordinary levels of sanctions against North Korea and Iran show no correlation between "smart" sanctions and changes in those states' cyber behaviors. In fact, North Korea evades the impact of sanctions primarily through cyber campaigns targeting international and crypto currency exchanges and reportedly accumulated $2 billion from 2016–2019 via such campaigns to support nuclear and intercontinental ballistic programs. This is more than three times the amount of currency it was able

to generate through counterfeit activity over the four decades prior.[42] Economic sanctions may also impose costs on U.S. firms. Similarly, diplomatic sanctions entail several often-overlooked costs for the United States, including a substantial loss of information and intelligence and a reduction in communication capacity and ability to influence the targeted state. Diplomatic sanctions may even undermine the effectiveness of other coercive policy tools, such as economic sanctions.[43]

Public attribution tends to lead to more careful tailoring of cyber operations.

Additionally, in announcing the Department of Justice's (DOJ) 2018 Cyber Digital Task Force strategy, Deputy Attorney General Rod Rosenstein argued that public indictments achieve deterrence.[44] However, Garrett Hinck and Tim Maurer concluded that "[b]ased on the existing record, bringing criminal charges against foreign hackers and online influence operators does not appear to impose enough costs on adversaries to convince them to cease from further malicious activity."[45] Similarly, Jack Goldsmith and Peter Machtiger argued that after five years of high profile indictments of foreign cyber operators, there is little evidence to support Rosenstein's argument that DOJ indictments "stop or even slow these activities."[46]

A study of the effects of public attribution on future state cyber behavior concludes that, although some states may have concerns about this, the consequence for those states will be "a more careful tailoring of their offensive operations." For states still building up their offensive capabilities, the effect will be to "adapt their policies and procedures to prevent indiscriminately delivering effects."[47] Neither of these is indicative of a deterrence effect and, of course, some states are not at all concerned with public attribution. When discussing the issue of Russian cyber operations seeking to influence the U.S. presidential election, for example, then-U.S. President Obama stated, "[T]he idea that somehow public shaming is going to be effective, I think doesn't read the thought process in Russia very well."[48]

In sum, the weak record of the effectiveness of sanctions combined with the logic of cyber strategic competition short of armed conflict suggests that the sanctions playbook is not and will not be effective.

The third explanation for adversaries' image of a yielding United States is informed by U.S. policymakers concerns regarding asymmetric vulnerability in and through cyberspace.[49] For example, Eric Rosenbach, former Assistant Secretary of Defense for Homeland Defense and Global Security, noted that the United States lives in a digital "glass house" and that, consequently, "the U.S. has more to lose from an escalation in cyber-initiated conflict."[50] If committed to the logic of deterrence, success in crisis environments is dependent on establishing escalation dominance. As Thomas Schelling argued, leaving the opponent with one "last clear chance" to avoid disaster so that they must acquiesce is the key to winning the escalation contest. Rosenbach argued, however, that given the "glass house" effect "we should be careful about responding to cyberattacks with military options."[51] Thus, adversaries are reasonably concluding that kinetic force is an unlikely response option to their cyber operations and campaigns short of armed conflict. The 2018 DoD Cyber Strategy acknowledges this dynamic by noting, "Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations [short of armed conflict] to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure."[52] By removing kinetic responses as a potential means to impose prohibitive costs, the United States appears unwilling to commit to deterrence's logic of escalation dominance. Additionally, if the United States did threaten a kinetic response for cyber-enabled intellectual property theft, for example, the threat would likely not be viewed as credible from a political will perspective.[53] For addressing adversary cyber activity short of armed conflict, kinetic responses present the United States with a "catch 22" situation, and adversaries know this.

In sum, U.S. cyber deterrence policy is caught in a vicious cycle—it is premised on an approach of strategic ambiguity in thresholds and punishments, which requires that an adversary view the United States as credible. However, U.S. adversaries do not view the U.S. as credible, a likely consequence of its strategic ambiguity policy as well as a failure to impose prohibitive costs, which in turn, is a consequence of the unprecedented opportunities for cumulative gains from continuous cyber campaigns and cyberspace's facilitation of sanctions circumvention. Additionally, when punishments have been levied, they have not been accompanied by details of specific thresholds that were breached, thereby sustaining both strategic ambiguity in thresholds and, as a consequence, a lack of credibility. Thus, what is being applied as a strategy of deterrence is not deterring the most common and strategically salient cyber actions (i.e., operations and campaigns short of armed conflict). The United States is following a reactive self-reinforcing policy leading to strategic loss.

Why These Strategic Choices Endure

All of this begs the question of why so many U. S. policymakers remain wedded to the central placement of a deterrence-based strategic approach to addressing adversary cyber operations short of armed conflict. It may be, of course, that some policymakers feel that the flexibility gained in ambiguity is worth the strategic costs. As noted previously, however, this view risks strategic loss, and the last decade of adversaries' gains in and through cyberspace makes clear that, without comprehensive change, the United States is losing relative strategic advantage. An alternative explanation is suggested by the 2017 testimony of Ken Rapuano, then-Assistant Secretary of Homeland Defense and Global Security. In response to a query regarding the status of the development of U.S. cyber doctrine, Rapuano said, "I certainly agree that both the demonstrated will and ability to respond to provocations in general and cyber in specific is critical to effective deterrence. I think the challenge that we have that is somewhat unique in cyber is defining a threshold that then does not invite adversaries to inch up close but short of it. And therefore, the criteria – it is very difficult to make them highly specific versus more general, and then the downside of the general is it is too ambiguous to be meaningful …."[54] A North Atlantic Treaty Organization report on cybersecurity highlighted the same challenge: "If the Alliance were to set a clear threshold, the opponent would better understand how to stay below that threshold. This would strengthen deterrence of threats above the threshold but would encourage the opponent to increase attacks just below the threshold."[55]

In the competitive space short of armed conflict, relying on a deterrence strategy for cybersecurity based on specific thresholds and prohibitive costs is not feasible.

The United States, it seems, has chosen strategic ambiguity over specificity not because it feels confident in its image of credibility, but because, despite its best efforts, it cannot ascertain where, short of armed conflict, to set thresholds at which it could credibly threaten or exact prohibitive costs without also inviting adversaries to design around the deterrent threat. This is certainly not a consequence of a lack of effort, as Congress has been prodding DoD for such details for years. Instead, it is better understood as an illustration of the powerful impact the cyber strategic environment has had on the mis-development of U.S. cyber strategy. It is also an implicit recognition that, in the competitive space short of armed conflict, a deterrence strategy for cybersecurity based on specific thresholds and prohibitive costs is not feasible.

The unsoundness of this approach can be illustrated through one well-known series of cyber intrusions that followed the public appearance of the Eternal Blue exploit (CVE-2017-0144 in the Common Vulnerabilities and Exposures catalog). Within two months of its appearance (April 2017), an exploit of the vulnerability manifested as Wannacry ransomware. One month later, it manifested as Notpetya, a purely destructive attack disguised as ransomware; a couple of months later as Retefe, a banking trojan that routes traffic to and from the targeted banks through various proxy servers often hosted on the TOR network; and again in October 2017 as Wannamine, a cryptocurrency miner. This is a common phenomenon with exploits, and it presents implementation challenges that a cybersecurity approach based on deterrence short of armed conflict perpetually struggles inherently to overcome.

The above leads to another question: If this condition is obvious, why do policymakers continue to default to equating security (in the cyber strategic environment) with deterrence? Two explanations come to the fore. First, far more often than not, assessments preceding the drafting of national security strategies conclude that the world is rich in dangers and risks and that U.S. defensive capabilities are already stretched too thin. This reasoning consistently leads to deterrence as the default central strategic approach for most strategic challenges. From this perspective, it is unsurprising that deterrence is the central strategic concept in U.S. national and DoD cyber strategies published since 2011, when then-Deputy Secretary of Defense William Lynne III first declared cyberspace an operating environment.

A second explanation is that U.S. policymakers believe they have no other strategic approach to consider. Although frustration with the failure of deterrence has led some to conclude that the logic of competition differs from the logic of deterrence, since alternative strategic approaches are only slowly being recognized and accepted, policymakers continue to stretch deterrence in ways described in this essay. But this need not continue to be the case. Based on analyses of the cyber strategic environment and adversary behavior therein, a new strategic logic has emerged in the form of cyber persistence theory, which was operationalized by USCYBERCOM in 2018 to support DoD's defend forward cyber strategy. This new theory prescribes a strategic approach that should stand alongside defense and deterrence of militarized crises and armed conflict to secure U.S. interests across the full spectrum of strategic competition in and through the cyber strategic environment. To quote Schelling, it is time to "substitute brains and skill" for obstinacy (and inertia) and match strategy to the reality of the security challenges the United States faces.

What Must Be Done

Cyber Persistence Theory: A New Approach to Cybersecurity

There is a strategic imperative to act persistently to achieve security, not merely an incentive to do so.

A key assumption behind U.S. efforts to adapt deterrence theory to halt, meter the severity, or reduce the frequency of state cyber behaviors short of armed conflict is that the incentive behind a state's strategic choices to act in cyberspace is a function of others' declaratory policies. Although that may be a factor, it is not the primary one. State behavior in cyberspace derives from a core set of characteristics that define the cyber strategic environment: interconnectedness, constant contact, an abundance of organic vulnerabilities, and recognitions that exploitation of those vulnerabilities can occur at scale without crossing from competition to the conflict domain and that such campaigns can return strategic gains.[56] Cyber persistence theory argues that, taken together, these features produce a strategic imperative to act persistently to achieve security, not merely an incentive to do so.[57] When understood in this manner, the cyber strategic environment precludes the effectiveness of a deterrence strategy, because in this environment, restraint is punished rather than rewarded, and initiative is rewarded rather than punished. With regard to restraint and initiative, the cyber environment and the nuclear environment (from which deterrence theory is derived) are, in fact, mirror opposites.

This understanding logically leads to a strategic reorientation away from the centrality of deterrence and toward initiative persistence. Security must be sought through a commitment to set and maintain the conditions of security in one's favor by reducing the potential exploitation of one's own vulnerabilities and exploiting the vulnerabilities of others.[58] This is a guiding strategic principle for USCYBERCOM's doctrine of persistent engagement.[59] However, it need not be limited to only the military instrument of national power, to the operational and tactical levels where USCYBERCOM operates, or to just the U.S. government. Initiative persistence is as much a mindset orientation as an implementable operational approach.

There are examples to build upon at the interagency level. There are indications that the logic of persistence and seizing initiative has been adopted outside the DoD (though perhaps only implicitly and in an ad hoc, uncoordinated fashion).

At the strategic level, the DOS reinforced operational needs and seized the diplomatic initiative in early 2020 through an assertive diplomatic campaign to help ensure the defeat of China's nominee to lead the United Nation's World Intellectual Property Organization.[60] In so doing, the DOS denied China the opportunity to legitimize in a global forum its practice of cyber-enabled IP theft. Likewise, since 2018, the interagency Committee on Foreign Investment in the U.S. (CFIUS) disrupted the planned acquisition of MoneyGram International Inc. by Ant Financial, a Chinese financial-services form, due to concerns of Chinese access to personally identifiable information (PII).[61] This activity denied China a future opportunity to leverage PII against U.S. national interests as China had done following an earlier cyber-enabled campaign illicitly targeting PII. At the operational level, the DOJ's Federal Bureau of Investigation (FBI) recently leveraged a paid collaborator to market to alleged-criminal organizations custom cellphones bought on the black market and installed with the FBI-controlled platform called Anom, which was described as an encrypted messaging platform. The platform shared all communications with the FBI, supporting the arrest of more than 800 people and enabling "an unprecedented understanding into the functioning of modern criminal networks."[63]

These interagency examples illustrate how initiative persistence results in the United States, at a minimum, avoiding strategic losses in and through the cyber strategic environment and, in some cases, gaining the upper hand or actually achieving strategic gains. Applying the principle of persistently seeking the cyber initiative throughout the interagency is not enough, however. The current administration's Executive Order on Improving the Nation's Cyber Security calls for better public-private collaboration, as have many previous studies, commissions, and cyber strategies.[64] The elusiveness of that goal to-date can arguably be attributed to the absence of a shared strategic principle guiding the collaboration of government officials who provide public goods and private actors motivated by a huge diversity of incentives including, but not limited to, turning a profit. Moreover, the "private sector" label includes entities with very different and sometimes competing or even conflicting interests.[65] Seizing the initiative must be the key shared strategic principle. Seizing initiative in competition, after all, is at the heart of corporate approaches to turbulent competitive environments, where competent and resourceful opponents risk eroding any advantage one currently holds.[66] The corporate strategist must constantly strive "[f]irst, to seize initiative—by securing and maintaining the strategic initiative; and second, to anticipate competitively—by anticipating the responses of each of the various competitors."[67]

Notable collaboration and coordination efforts that serve as evidence of this principle as a viable connective tissue for a WON+ framework include the response to the potential threat posed by Russia's VPNFilter malware. Cisco Talos was sharing information about the malware with the FBI and, on May 23, 2018, three things happened simultaneously: The FBI seized infected Web domains it suspected the Russian hackers would exploit, Cisco published its findings globally in a blog post, and all members of the Cyber Threat Alliance (a non-profit forum) were sent simultaneous urgent notices describing how to protect against the Russian exploit.[68] Additionally, in September 2019, representatives from Facebook, Google, Microsoft, and Twitter met with U.S. government officials from the FBI, the Department of Homeland Security, and the Office of the Director of National Intelligence to discuss their preparations for the presidential election. "Participants discussed their respective work, explored potential threats, and identified further steps to improve planning and coordination."[69] Institutionalizing and expanding such efforts in coordination with allies and global partners anchored on a guiding principle of initiative persistence will be key to success.

Conclusion

Strategic competition in and through cyberspace is characterized by exploitation, not coercion; and a strategic approach of initiative persistence, not reactive threat and restraint, must be the central security element of a national cyber strategy. Moreover, a persistent focus on leveraging initiative in and through cyberspace must be integrated across all U.S. national security thinking.

Despite policymakers' best efforts over the last decade to adapt deterrence theory to the cyber competitive space short of armed conflict, the cyber strategic environment inescapably forces the United States to play the wrong hand and even the wrong game. The environment drives policymakers to adopt a declaratory policy of strategic ambiguity when it does not have credibility to stand on, and it obliges sanctions as the "go-to" approach for imposing prohibitive costs while concomitantly invalidating two key assumptions of sanctions theory (i.e., that costs will cumulate over time to the point of being prohibitive and that sanctioned actors cannot adapt). If this approach continues, the United States will continue to suffer strategic losses in and through cyberspace.

A strategic approach of deterrence has a place in a national cyber strategy as a coercive approach that dissuades adversary use of armed-attack equivalent cyber operations or other military uses of force in militarized crises and armed conflict.[70] This, in fact, is consistent with the concept of integrated deterrence, first espoused by U.S. Secretary of Defense Lloyd Austin on April 30, 2021.[71] Secretary Austin described integrated deterrence as using all military capabilities in concert with other instruments of national power to deter states with revisionist aims. Its comprehensive substance is consistent with the strategy the U.S. government has pursued in the cyber competitive space short of armed conflict for the last decade—a space for which the strategy is misaligned and failing badly, for reasons described in this essay. To avoid sustaining this historical error, the U.S. administration must accept that, although integrated deterrence will dissuade U.S. adversaries from considering achieving potential gains through militarized crises and armed conflict, adversaries are with certainty realizing strategic gains today by engaging in ongoing, continuous cyber campaigns and operations short of armed conflict where integrated deterrence cannot effectively be applied. In this particular strategic competitive space, initiative persistence must anchor the integration of all sources of national power (just as deterrence can in conditions of crisis and war). The strategic principle of cyber persistence theory, a strategic theory derived from the core features of cyberspace, is the appropriate principle around which to draft a new U.S. national cyber strategy—seizing and maintaining the initiative to set the conditions of security in the U.S.'s favor. There is some evidence that departments have recognized that this is a more effective approach, but their efforts are not coordinated through national strategic guidance. The next U.S. national cyber strategy, therefore, should be drafted as a capstone document centered on this principle to ensure that it guides whole-of-government and WON+ efforts. It is time to persistently and comprehensively seize the initiative.

Endnotes

1 The White House, FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks, May 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ and The White House, Executive Order on Improving the Nation's Cyber Security, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. While some may want to argue the Executive Order supports deterrence by denial, the document clearly focuses on reducing the ability of adversaries' cyber operations to "damage or deprive" the United States rather than reducing the likelihood of adversary cyber operations. For a discussion of the differences between defense and deterrence, see Glenn H. Snyder, Deterrence and Defense: Toward a Theory of National Security (Princeton University Press: Princeton, NJ, 1961).

2 Gary King and Langche Zeng, "Explaining Rare Events in International Relations," International Organization (55: 2001), pp. 693–715, https://j.mp/2oTjnM4.

3 Policymakers should consider that the United States possesses a significant set of kinetic capabilities already serving this purpose and that using cyber capabilities for the same end sub-optimizes their distinct value to strategic competition short of armed conflict.

4 Exploitation is defined as gaining advantage by making use of others' vulnerabilities in and through cyberspace, whereas vulnerability is defined as a weakness or bias in an information system, system security procedures, internal controls, implementation, data, or users that could be exploited by a threat source. These definitions are consistent with the lexicon of cybersecurity and state behavior in and through cyberspace and are more comprehensive than other definitions narrowly focusing on intelligence operations. See, for example, Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," Journal of National Security Law and Policy (4:63, 2010), pp. 63–86, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf and U.S. Department of Defense, Joint Publication 3-12, Cyberspace Operations, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Endnotes

5 Concept stretching is a practice that seeks to extend the explanatory value of a concept to fit new contexts. A common "stretching" tactic is to precede the original concept with an adjective. Consider all of the adjectives that often now precede "deterrence" as an example. See Giovanni Sartori, "Concept Misinformation in Comparative Politics," The American Political Science Review (64:4, 1970), pp. 1033–1053, https://www.jstor.org/stable/1958356?seq=1#metadata_info_tab_contents, and David Collier and James E. Mahon, Jr., "Conceptual 'Stretching' Revisited: Adapting Categories in Comparative Analyses," The American Political Science Review (87:4, 1993), pp. 845–855, https://www.jstor.org/stable/2938818?seq=1#metadata_info_tab_contents. For a proponent of "stretching" deterrence to facilitate its application to the cyber context, see Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," International Security (41:3 2016/17), pp. 44–71, https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

6 Cyber persistence theory is the strategic theory underpinning U.S. Cyber Command's doctrine of persistent engagement. See Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence Theory, Intelligence Contests, and Strategic Competition," Texas National Security Review: Special Issue – Cyber Competition, September 17, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/, and Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence: Redefining National Security in Cyberspace (book manuscript under review).

7 In the parlance of the White House, armed-attack equivalent cyber operations would be considered "significant cyber incidents," which are defined as "[a] cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." Presidential Policy Directive -- United States Cyber Incident Coordination, July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

8 Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," Foreign Affairs, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Endnotes

9 Joseph Marks, "McCain Leaves a Rich Cyber Legacy," Nextgov, August 27, 2018, https://www.nextgov.com/cybersecurity/2018/08/mccain-leaves-rich-cyber-legacy/150847/; Morgan Chalfant, "McCain Hits Trump over Lack of Cyber Policy," The Hill, August 23, 2017, https://thehill.com/policy/cybersecurity/347660-mccain-hits-trump-over-lack-of-cyber-policy.

10 Senate Armed Services Committee, March 1, 2018, https://www.c-span.org/video/?441917-1/nsa-nominee-testifies-senate-armed-services-committee @ 00:52.

11 Ibid, @ 1:03.

12 Ibid, @ 1:30.

13 See Joseph Marks with Aaron Schaffer, "The Cybersecurity 202: Angus King Says it's Time to Get Tougher on Russian Hackers," The Washington Post, June 30, 2021, https://www.washingtonpost.com/politics/2021/06/30/cybersecurity-202-angus-king-says-its-time-get-tougher-russian-hackers/ and U.S. Public Law 115-91, December 12, 2017, https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf.

14 Strategic ambiguity has also been referred to as constructive ambiguity.

15 See Ellen Nakashima, "U.S. Cyber Approach 'Too Predictable' for One Top General," The Washington Post, Jul 14, 2011, https://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html and Chris Carroll, "Congress Demands Cyber Details while DoD Aims for Ambiguity," Stars and Stripes, July 21, 2011, https://www.stripes.com/news/congress-demands-cyber-details-while-dod-aims-for-ambiguity-1.149790.

16 Obama administration's December 2015 report to Congress on cyber deterrence, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/dec2015/cs2015_0133.pdf.

17 Dr. Christopher Ashley Ford, U.S. Department of States Assistant Secretary-Bureau of International Security and Nonproliferation, "Responding to Modern Cyber Threats with Diplomacy and Deterrence," October 19, 2020, https://2017-2021.state.gov/responding-to-modern-cyber-threats-with-diplomacy-and-deterrence/index.html.

Endnotes

18 See U.S. Department of State, Office of the Coordinator for Cyber Issues, Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats, May 31, 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 and "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. It should be noted that at least one DOS official claims the consequence matrix is intended for cyber operations short of use of force. See "Discussing the UN OEWG with the Mother of Norms," Center for Strategic and International Studies podcast with James Andrew Lewis, Christopher Painter, and Michele Markoff, https://www.csis.org/podcasts/inside-cyber-diplomacy/discussing-un-oewg-mother-norms.

19 Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

20 The White House, International Strategy for Cyberspace (May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

21 See James Andrew Lewis, Cyber Deterrence Declaratory Policy, 2011–2015, https://www.csis.org/blogs/strategic-technologies-blog/cyber-deterrence-declaratory-policy-2011-2015.

22 Catalin Cimpanu, "FSB Warns of US Cyberattacks after Biden Administration Comments," ZDNet, January 22, 2021, https://www.zdnet.com/article/fsb-warns-of-us-cyberattacks-after-biden-administration-comments/.

23 These instruments have been applied in different ways, both individually and in combination, to construct tailored deterrence responses.

24 For example, the U.S. Department of Justice adopts this long-term view with regard to indicting foreign cyber operators. See Elias Groll, "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked," Foreign Policy, September 2, 2015, https://foreignpolicy.com/2015/09/02/the-u-s-hoped-indicting-5-chinese-hackers-would-deter-beijings-cyberwarriors-it-hasnt-worked/.

Endnotes

25 Peter A. G. van Bergeijk and Charles van Marrewijk, "Why Do Sanctions Need Time to Work? Adjustment, Learning and Anticipation," Economic Modelling (12:2, 1995), pp. 75–86, https://core.ac.uk/download/pdf/204634656.pdf.

26 For a comprehensive discussion of the core features of the cyber strategic environment as they relate generally to a deterrence strategy, see Michael P. Fischerkeller, Richard J. Harknett, and Jelena Vicic, "The Limits of Deterrence and the Need for Persistence" in Aaron Brantly, ed., The Cyber Deterrence Problem (Rowman & Littlefield Ltd, 2020) and Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is not a Credible Strategy for Cyberspace," Orbis (Summer 2017), https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/.

27 Thomas C. Schelling, Arms and Influence, op. cit., p. 48.

28 Richard Ned Lebow, Between Peace and War (The Johns Hopkins University Press: Baltimore, 1977), p. 85.

29 Glenn Herald Snyder and Paul Diesing, Conflict Among Nations: Bargaining, Decision Making, and System Structure in Crises (Princeton University Press, Princeton, 1978), p. 216.

30 Ibid, pp. 216–218.

31 Ibid.

32 Thomas C. Schelling, Arms and Influence, op. cit., p. 67.

33 Thomas C. Schelling, Arms and Influence, op. cit., p. 40. Schelling also discussed this image, sometimes referred to as the "madman theory," within the strategic context of nuclear compellence, a significantly different dynamic than deterrence. Thus, those arguments should not necessarily be considered relevant to deterrence. Those who feel otherwise, however, should consider the scholarship of Sescher and Furman who, based on their empirical study of nuclear compellence, concluded that this approach has a "poor track record of real-world success." Todd S. Sechser and Matthew Fuhrmann, Nuclear Weapons and Coercive Diplomacy (Cambridge University Press: London, 2017).

Endnotes

34 Thomas C. Schelling, Arms and Influence, op. cit., p. 41.

35 Ibid.

36 Ibid. For the 2020 defense expenditure figure, see U.S. Government Accountability Office, Defense Budget: Opportunities Exist to Improve DOD's Management of Defense Spending, GAO-21-415T, February 24, 2021, https://www.gao.gov/products/gao-21-415t.

37 Thomas C. Schelling, Arms and Influence, op. cit., p. 42.

38 James Andrew Lewis, "Strategy After Deterrence," March 11, 2020, https://www.csis.org/analysis/strategy-after-deterrence.

39 Additionally, because the sanctioned actor continues to operate in and through cyberspace, the deterrer continues to accrue losses.

40 See Gary Hufbauer, Jeffrey Schott, Kimberly Elliott and Barbara Oegg, Economic Sanctions Reconsidered, 3rd Edition (Washington, DC: Peterson Institute for International Economics, 2007). Also, see Clifton Morgan, Navin Bapat, and Valentina Krustev, "The Threat and Imposition of Economic Sanctions, 1971–2000," Conflict Management and Peace Science (28:1, 2008), pp. 92–110.

41 Thomas Bierstecker, Zuzana Hudokova, Marcos Tourinho, "The Effectiveness of UN Targeted Sanctions: Findings from the Targeted Sanctions Consortium," https://www.academia.edu/8406764/The_Effectiveness_of_UN_Targeted_Sanctions_Findings_from_the_Targeted_Sanctions_Consortium_TSC_

42 Tim Maurer and Arthur Nelson, "COVID-19's Other Virus: Targeting the Financial System," Strategic Europe, April 21, 2020, https://carnegieeurope.eu/strategiceurope/81599.

43 Tara Maller, "Diplomacy Derailed: The Consequences of Diplomatic Sanctions," The Washington Quarterly (33:3, July 2010), pp. 61–79, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/twq10julymaller.pdf.

Endnotes

44 Patrick Howell O'Neill, "DOJ Drops Massive Report on Its Efforts to Protect U.S. from Cyberattacks," CyberScoop, July 19, 2018, https://www.cyberscoop.com/department-of-justice-internal-cyber-digital-task-force-report/.

45 Garrett Hinck and Tim Maurer, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," Journal of National Security Law and Policy (January 24, 2020), https://carnegieendowment.org/2020/01/24/persistent-enforcement-criminal-charges-as-response-to-nation-state-malicious-cyber-activity-pub-80885.

46 See, respectively, Jack Goldsmith, "The Puzzle of the GRU Indictment," Lawfare, October 21, 2020, https://www.lawfareblog.com/puzzle-gru-indictment and Peter Machtiger, "The Latest GRU Indictment: A Failed Exercise in Deterrence," JustSecurity, October 29, 2020, https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/. Additionally, two former NSA analysts, Blake Darché and Mark Kuhr, agreed that Russian indictments will have little to no impact on the pace and volume of Russian cyberattacks on the U.S. See Chris Bing, "Former NSA Hackers: Yahoo Indictments Won't Slow Down Russian Cyberattacks," CyberScoop, March 17, 2017, https://perma.cc/M7G7-ANKP. Finally, John Demers, former assistant attorney general of the DOJ's National Security Division, has acknowledged that indictments had done little to deter the cyber activity of Russia, China, Iran, and North Korea. See Joseph Marks with Aaron Schaffer, "The Cybersecurity 202: DOJ's Future is in Disrupting Hackers, Not Just Indicting Them," The Washington Post, July 1, 2021, https://www.washingtonpost.com/politics/2021/07/01/cybersecurity-202-dojs-future-is-disrupting-hackers-not-just-indicting-them/.

47 Florian J. Egloff, "Public Attribution of Cyber Intrusions," Journal of Cybersecurity, (6, 2020), https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454.

48 "Full Transcript: President Obama's Final End-of-Year Press Conference," Politico, December 16, 2016, https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763.

49 For a reporting of how this concern informed the Obama administration's response to Russian efforts to influence the 2016 U.S. presidential election, see Michael Isikoff and David Corn, Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump (Twelve: 2018).

Endnotes

50 Eric Rosenbach, "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks," June 12, 2017, https://www.belfercenter.org/publication/living-glass-house-united-states-must-better-defend-against-cyber-and-information.

51 Ibid.

52 U.S. Department of Defense, "Department of Defense Cyber Strategy: Summary" (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

53 This argument finds support in the oft-stated U.S. stance of adhering to international law in cyberspace where kinetic responses to cyber operational effects short of armed-attack equivalence would likely be considered an internationally wrongful act.

54 Committee on Armed Services, United States Senate, Hearing to Receive Testimony on the Roles and Responsibilities for Defending the Nation from Cyber Attack, October 19, 2017, https://www.armed-services.senate.gov/imo/media/doc/17-83_10-19-17.pdf.

55 NATO Parliamentary Assembly, Science and Technology Committee, NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence, April 18, 2019, https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf.

56 Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence Theory, Intelligence Contests, and Strategic Competition," op. cit.

57 Ibid.

58 Ibid.

59 "An Interview with Paul M. Nakasone," Joint Force Quarterly (92, 1st Quarter, 2019), pp. 4–9, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

Endnotes

60 Colum Lynch, "U.S. State Department Appoints Envoy to Counter Chinese Influence at the U.N.," ForeignPolicy, January 22, 2020, https://foreignpolicy.com/2020/01/22/us-state-department-appoints-envoy-counter-chinese-influence-un-trump/ and Nick Cumming-Bruce, "U.S.-backed Candidate for Global Tech Post Beats China's Nominee," The New York Times, March 4, 2020, https://www.nytimes.com/2020/03/04/business/economy/un-world-intellectual-property-organization.html.

61 U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

62 Zach Dorfmann, "China Use Stolen Data to Expose CIA Operatives in Africa and Europe," ForeignPolicy, December 21, 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

63 Rachel Pannett and Michael Birnbaum, "FBI-controlled Anom App Ensnares Scores of Alleged Criminals in Global Police Sting," The Washington Post, June 8, 2021, https://www.washingtonpost.com/world/2021/06/08/fbi-app-arrests-australia-crime/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202&carta-url=https%3A%2F%2Fs2.washingtonpost.com%2Fcar-ln-tr%2F3359f68%2F60c9dc3d9d2fdae30280f899%2F596d89b2ae7e8a1845f8a301%2F11%2F64%2F60c9dc3d9d2fdae30280f899.

64 For an overview, see Megan Brown, "Cyber Imperative: Preserve and Strengthen Public-Private Partnerships" (The National Security Institute at George Mason University's Antonin Scalia Law School, 2018), https://nationalsecurity.gmu.edu/2018/10/nsi-policy-paper-cyber-imperative-preserve-and-strengthen-public-private-partnerships/.

65 Emily Goldman and Eduardo Monarez, "Persistent Engagement and the Private Sector," Journal of Information Warfare (20, 2:1, Spring 2021), pp. 107–121, https://www.jinfowar.com/journal/volume-20-issue-2/persistent-engagement-private-sector.

66 Ibid, p. 110.

Endnotes

67 Ian C. MacMillan, "Controlling Competitive Dynamics by Taking Strategic Initiative," The Academy of Management Perspectives (2:2, May 1, 1988), pp. 111–118, 112, https://www.jstor.org/stable/4164812?seq=1#metadata_info_tab_contents.

68 "The Cybersecurity 202: Top Cybersecurity Companies Are Pooling Their Intel to Stop Cyberattacks," The Washington Post, May 23, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/23/the-cybersecurity-202-top-cybersecurity-companies-are-pooling-their-intel-to-stop-cyberattacks/5ce5ef73a7a0a46b92a3fd95/.

69 Salvador Rodriguez, "The FBI Visits Facebook to Talk about 2020 Election Security, with Google, Microsoft and Twitter Joining," CNBC, September 24, 2019, https://www.cnbc.com/amp/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.

70 For example, at the June 16, 2021, Biden-Putin Summit in Geneva, President Biden made clear to President Putin that 16 U.S. critical infrastructures sectors were "off limits" to "destructive" attacks, cyber or otherwise. Such cyber operations would be considered as armed-attack equivalent and thus fall within the bounds of militarized crises and war, the environment for which deterrence is an appropriate strategy. Vladimir Soldatkin and Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off-Limits,'" Reuters, June 16, 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

71 Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command, April 30, 2021, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/.

About

Kybernao seeks to publish academic-based research applied to real-world policy and strategy questions. These short pieces (2500-8000) will be published on an occasional basis as an Issue Briefing/Policy Briefing with the goal of connecting academics with policymakers to improve security in cyberspace.

Kybernao is the Greek verb "to steer" (κυβερνάω, the first person singular present). The Greek noun for "steersmen" or "helmsman" is kybernetes (κυβηρνήτης), which many point to as the etymology behind the term cyber as it related to the concept of cybernetics, which focused on the relationship between communication and automatic control systems of both machines and humans. Our image is inspired from ancient Greek pottery and depicts the guide navigating by the contours of the network (stars) through the core code that both serves as the terrain of cyberspace (seas) and the way one moves across the network.

The Center for Cyber Strategy and Policy (CCSP) image captures the challenge of securing cyberspace. The use of chess pieces is to emphasize the notion of strategy. The multiplying knights depicts the ever-changing character of malware that can morph into new versions and take advantage of new vectors for exploitation of vulnerabilities. The shadows depict the ever-present opportunity to leverage uncertainty regarding network intrusion, intruder, an intruder's intent, the scale and scope of a campaign, and even the game being played (perhaps you are playing GO instead of chess)--you may think you are playing against the knight and can anticipate those moves, when in fact you are playing against a bishop with very different operational capabilities and potential for strategic gain. The defeated pawn acknowledges the potential to win and lose in cyberspace (note that a draw is possible in chess, Go, and in cyberspace).

For more on the CCSP visit our website

For inquiries about the Kybernao series or CCSP in general, contact: cyberstrategy@uc.edu