Forward Persistence in Great Power Cyber Competition

Military Assets in a Relative Power Erosion Framework

Dr. Thomas F. Lynch III

ABSTRACT

The United States, the People's Republic of China (PRC), and Russia are engaged in strategic competition below the threshold of armed conflict. Cyberspace is its principal medium, and unless indicated otherwise, all references herein will assume the context of "short of armed conflict." America's relative power stature is under non-stop cyber duress from these rivals. Protecting America's three main peacetime power sinews – its economic edge; domestic political cohesion and electoral system confidence; and public trust in protection of personal privacy and security – from the subversive and corrosive cyber activities by Great Power rivals requires an array of U.S. government agencies, especially the U.S. military. The new era of Great Power strategic competition has fragmented the internet and rendered inadequate America's historical preference for an orderly, law-based framework that manages cyber-competition. The U.S. needs to focus on a Relative Power Erosion Framework featuring persistent engagement and a hunt forward posture. USCYBERCOM-led cyber campaigns are necessary in the short-term for effective American strategic cyber competition. In the longer-term, unique American military capabilities for persistent cyber engagement should be replaced with those in selected civilian governmental agencies more befitting of a 'new normal' for endemic cyber-competitive interactions among the Great Powers.

CONTEMPORARY GREAT POWER COMPETITION – THE ALTERED GEOSTRATEGIC ENVIRONMENT AND INTEGRATED DETERRENCE

Today's geostrategic environment is dominated by Great Power rivalry and competition for relative power gains and advantages among the U.S., Russia, and the PRC during cyber interactions.[1] This environment differs fundamentally from the previous geostrategic era. For almost thirty years, from the 1990s to the early 2010s,

Dr. Thomas F. Lynch III is a Distinguished Research Fellow in the Center for Strategic Research (CSR) at the Institute of National Strategic Studies (INSS) of the National Defense University (NDU) in Washington, D.C. His ongoing research primarily focuses on contemporary Great Power Competition and on India's strategic rise and implications for Indo-Pacific security and stability. He joined NDU in 2010 after retiring as a Colonel from a 28-year career in the active-duty U.S. Army, serving in a variety of command and staff positions as an armor/cavalry officer and as a senior level politico-military analyst. He holds a B.S. from the U.S. Military Academy at West Point, a Masters in Public Administration (MPA) and a Masters (M.A.) and Ph.D. in International Relations from the School of Public & International Affairs at Princeton University.

the U.S. was globally dominant. It's rules, norms, and preferences heavily shaped the evolution of global patterns, procedures, and protocols for most state-to-state interactions, including those in the new domain of cyberspace.[2]

The Reality of Strategic Competition in the Altered Geostrategic Environment

Cyberspace evolved and dramatically expanded worldwide in an open and liberal global environment with a unified, U.S.-preferred system that featured cooperative economic and social interactions. For most of this thirty-year, U.S.-dominated period, emerging Great Power rivals, the PRC and Russia, generally acted in accordance with these basic U.S. preferences.[3] Since the late 2000s, the PRC and Russia have remained engaged with the U.S.-normed global internet if beneficial, but increasingly are using it in coercive and confrontational ways: constraining outsider access, manipulating internal content, conducting industrial scale economic espionage and data collection, and manipulating rival state political and social discord for competitive strategic advantage.[4]

Putin's Russia, the weakest of the three Great Powers, has turned to cyberspace as its primary vehicle to reduce relative American ideological power and information dominance. Russia's approach to strategic cyber-manipulation echoes the "Active Measures" campaigns run by the U.S.S.R. against the U.S. during the Cold War but with vastly improved technologies and tactics.[5] Cyberspace access to the internet and social media's global openness allows Moscow to directly manipulate critical aspects of the U.S.'s dominant relative power in key strategic areas: *political legitimacy* and *personal privacy & security*.[6]

> Since at least 2008, the Russian state has directed coercive peacetime cyber campaigns aimed at weakening America's relative power in four major areas public confidence in the safety

of American critical infrastructure, the integrity of the American electoral system, the social stability of American society, and average American trust in their government.[7]

Russian military and intelligence services directly responsible for attacking the U.S. in these four areas include: the Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18; the Russian Foreign Intelligence Service (SVR); the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS); GRU's Main Center for Special Technologies (GTsST); and the Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM). The FSB has conducted malicious cyber operations targeting U.K. and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. The GRU has organized special military units to politically interfere in the U.S. and other western democracies. GRU Military Units 26265 and 74455 led the 2016 hack into Democratic National Committee computer systems. Unit 26265 developed the malicious software for that penetrated and Unit 74455 assisted in disseminating stolen documents and anti-Clinton narratives to online personas like DCLeaks and Guccifer 2.0. Unit 74455 also hacked into computers at U.S. state boards of elections and companies supplying election technologies.[8] Russian cyber interference in U.S. national elections continued into the 2024 cycle with a widening array of sophisticated online and social media influence campaigns exposed by the U.S. Justice Department with a public announcement of interference indictments in September 2024.[9]

Russian security agencies are also covertly tied to an array of domestic and international cyber ransomware and economic espionage groups that are gradually degrading American political comity, social cohesion, and confidence in its monetary and financial system. Russian state-sponsored cyber actors have demonstrated capabilities that compromise information technology (IT) networks, maintain long-term, persistent access to IT networks, extract sensitive data from IT and operational technology (OT) networks, and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware. The FSB also contracts criminal hackers for espionage-focused cyber activity, hackers that separately have launched disruptive ransomware and phishing campaigns.[10] Moscow provides sanctuary and protection to all of its state-controlled group members and most of its affiliated hacker groups, making fear of criminal indictment or international sanction a non-factor insofar as deterrence.

The PRC has competed since at least 2008 to improve relative strategic power vis-à-vis the U.S. by eroding Washington's status, stature, and innate advantages by targeting three primary areas:

- America's relative economic wealth and security;
- Trust and confidence in the U.S.'s ability to protect sensitive and private personal data (PII) from exploitation;
- America's international political legitimacy.

In early 2024, U.S. intelligence agencies and journalists reported that the PRC – applying

practices honed by Russian cyber-actors – were conducting an array of cyberspace misinformation and deception activities to influence the U.S. Presidential elections.[11] In September 2024, the U.S. research company Graphika demonstrated that a Chinese-linked cyber and social media campaign dubbed "Dragonbridge" had been impersonating U.S. voters while denigrating U.S. politicians and circulating false messages.[12] This report and subsequent U.S. government confirmation reflected the PRC's growing resolve to conduct cyber campaigns that *erode the sanctity of the American electoral system*. Revelations during 2024 confirmed that the PRC's cyber-competitive efforts against the U.S. have been growing in the political space. However, Beijing's primary malign cyber activity remains focused *on enhancing China's relative economic wealth*. The PRC's current cyber operations can be characterized as controlling information at home and stealing secrets abroad.[13]

For decades, the PRC has pursued a deliberate cyber espionage campaign against American firms and their partners both in China and abroad, focusing on the brazen theft of intellectual property and other sensitive commercial data and processes. PRC cyber campaigns include groups operating within the structure of the Chinese military and intelligence services and many People's Liberation Army (PLA) units (e.g., PLA Units 61398 and 78020). They also feature an array of PRC-affiliated private cyber espionage groups known as Advanced Persistent Threat (APT) entities like APT 41 (Double Dragon) and a host of others.

Leading cybersecurity analysts like James Lewis of the Center for Strategic and International Studies (CSIS) estimate that the U.S. lost between $20 – $30 billion annually from 2000 – 2017 and a cumulative total of $600 billion over the period as the result of the PRC's economic tradecraft, marketing practices, and intellectual property (IP) cyber theft.[14] The downstream economic multiplier impacts from IP cyber theft in lost markets and employment opportunities across the global marketplace drive this number much higher – and likely to more than $50 billion annually.[15] Estimates that explicitly incorporate PRC gains from counterfeited goods, in addition to IP theft, peg annual U.S. economic losses even higher – in a range between $225 billion to $600 billion.[16] Limited to pirated IP and put in context of the relative trajectory of the Sino-American Great Power economic rivalry, The World Bank estimated that the U.S. GDP in 2010 was $15 trillion, moving to $21 trillion in 2020, and Chinese GDP was $6 trillion in 2010, expanding to $14.75 trillion in 2020, a relative gain of approximately 30 percent. Other factors contributed to this relative wealth gain, but more than two decades of PRC cyber theft explains a non-trivial portion of Beijing's significant growth in strategic economic power vis-à-vis the United States.[17]

Malicious PRC cyber activities target a variety of U.S. industries, agencies and organizations including: healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms. PRC state-sponsored cyber actors aggressively target military, educational, and critical infrastructure (CI) personnel and organizations to

steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII). Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. These cyber operations support the PRC's long-term economic and military development objectives.[18] Like Moscow, Beijing affords broad sanctuary and protection to the members of its state-controlled group members and private hacker agents and will not extradite them. This sanctuary explains why the U.S. Department of Justice (DoJ) and the FBI have indicted dozens of Chinese state hackers but there have been no noteworthy apprehensions or prosecutions and no measurable alteration in malevolent Chinese cyber-behavior. Because of the fundamentally altered geostrategic power structure, Chinese hackers have little fear from criminal indictment or meaningful sanction by traditional U.S. or international legal and law enforcement activities.[19]

This fragmentation of cyberspace with the return of Great Power rivalry and the use of cyber for strategically significant competition is consistent with the history of fragmentation and separation of global domains of state-to-state interaction under growing geostrategic duress. As with the electronic warfare (EW) and the air domains before it, the cyber domain promises to continue a trajectory of increasing fragmentation until a major geostrategic shock – like an armed conflict between the Great Powers – re-frames global power relationships in a manner enabling return to a more cooperative and collaborative norm.[20] Clint Watts, an American cyberspace analyst, noted the world is now comprised of three distinct cyber domains: a highly manipulated and coercive one preferred by Russia, a tightly constrained, mostly closed, self-interested one preferred by the PRC, and an open and free one preferred by the U.S. and its partners.[21] A U.S. Council on Foreign Relations report from mid-2022 concluded that the competition for internet data in cyberspace is the primary dynamic of Great Power strategic competition and is responsible for accelerating cyberspace fragmentation that will not be reversed.[22]

The Waning Relevance of a Legal/Law Enforcement Framework for Competing in Cyberspace

Despite the relative comity and cooperation just after the advent of the internet, the international arena has yet to develop enforceable legal standards that govern acceptable conduct in cyberspace. Even during the 1990s and early 2000s, the level of distrust among major states was too high to conceive of a legally binding multi-state cyber treaty. Alternative efforts to generate a set of nonbinding norms and confidence-building measures (CBMs) produced a 2010 U.N. Report with five recommendations for negotiating safety and security in international cyberspace, but without follow-on success.[23] The ambitious collective effort that resulted in the *Tallinn 2.0 Manual on the International Law Applicable to Cyber Operations* (2017) was a forward-looking effort to grope with applying international law to cyberspace operations. But this non-legally binding academic manual by western legal scholars and cyber analysts has yet to gain universal policy traction.[24] There remains an imperative for the U.S. to stand with like-minded allies on commitment to a single, interconnected cyber system for all of humanity

that fosters innovation, economic growth, creativity, democratic governance, and unfettered access to knowledge. At least within this group, the U.S. may be able to collectively frame and enforce norms against destructive cyber-attacks and coercive cyber campaigns designed for strategically significant power erosion of state rivals.[25]

And within this network, institutions and protocols can be enhanced and extended under an agreed framework that effectively sanctions private and government-sponsored criminal or destructive activities. American legal and law enforcement traditions for safeguarding strategically critical economic, political, and social functions can continue within this collaborative cyber network. The Department of Homeland Security, the DoJ, and the FBI partnering with the Department of State and the CIA – with improved funding and cyber-tools – can pursue warrants, apprehension, standards of evidence, and traditional means for bringing to justice those threatening the norms and laws governing a free and responsible internet.[26]

However, the perverse and persistent use of cyberspace against America and its allies by Russian and PRC state-run and state-protected malevolent actors seeking strategic advantage over time is not today – and cannot for the foreseeable future be – optimally managed by legal and law enforcement traditions and protocols. Specifically, Russian and PRC refusal to extradite those indicted for abusive cyber behavior has been consistently demonstrated for almost a decade. At the end 2021, there had been no major apprehensions of the indicted, no trials, and no significant indication that malevolent cyber intentions or behaviors have been altered nor were there any growing public and private concerns about the effectiveness of indictments as a tool of deterrence.[27] In late 2024, no compelling information exists to attenuate these concerns. Effective sanctuary for these persistent cyber actors seeking the long-term erosion of American power renders them untouchable by ethically won legal indictments or national sanctions. In addition, evidence from Russia indicates that cyber-entrepreneurialism and experimentation continue to thrive in a sanctions-constrained, and indictment-ladened environment at least in part because Russian government and private-sector ties are tightening.[28] Legal frameworks and law enforcement protocols against Great Power actors remains necessary, but a different framework for effective competition in cyberspace is required.

The Growing Importance of a Relative Power Erosion Framework for Competing in Cyberspace

Indictments and sanctions of foreign cybercriminals remains necessary for consistent application of cyber-norms, but alone are insufficient insofar as meaningful deterrence or disruption of adversary Great Power cyber organizations and their affiliates. A necessary and sufficient framework is required – one that better aligns with the realities of a fragmenting and strategically abused cyberspace.

An era of strategic Great Power competition requires a more holistic and aggressive approach

to blunt rival cyber activities that erode American power, bleed American economic wealth and know-how, compromise major American interests, or corrode American political and social cohesion. Multiple American agencies should participate in strategic competition in cyberspace given that the cyber domain has fragmented and the threat from America's cyber rivals require a different competitive framework.

Competition with America's Great Power rivals requires a ***Relative Power Erosion Framework*** in response to the increasingly fragmented cyber domain and its unique nature. In turn this ***Relative Power Erosion Framework*** rests comfortably on the foundational logic of persistence-as-deterrence in cyberspace, or **cyber persistence theory**.[29]

The **cyber persistence theory** construct derives from the cyber-strategic environment, which differs from conventional and nuclear deterrence, and requires continuous interaction, cumulative strategic effect, ***persistent engagement***, and ***forward defense***.[30] **Cyber persistence theory** views as normal certain occurrences that would be failures in other domains. Cyber aggression, rather than an anomaly, signals emergence of a new competitive space wherein "agreement over the substantive character of acceptable and unacceptable behaviors ... is currently immature," thereby recasting what is "normal."[31]

Classic deterrence theory – with its core concepts of denial, cost imposition, signaling, and attacks of significant consequence – now sits side-by-side with a paradigm/construct more aptly tailored to the cyber environment: ***cyber persistence***. Cyber persistence features continuous interaction, cumulative strategic effect, persistent engagement, and forward defense.[32] The core question for the cyber persistence paradigm is how to secure when you cannot deter.

Since just after the mid-2000s, deterrence in cyberspace has been contrasted from classic military deterrence and nuclear weapons deterrence. A renowned RAND study from this era described cyberspace as a unique medium of global interaction with its own rules, with attacks enabled through the exploitation of vulnerabilities instead of force, where permanent effects are harder to produce. It also is a medium fraught with ambiguities about who attacked, why, what they achieved and whether they can do so again even if – and often because – of successful attacks.[33]

Throughout the 2010s and into the 2020s, the limitations of deterrence formulations in cyberspace have been intensely debated. Increasingly, prominent analysts argue that traditional deterrence constructs are less relevant in cyberspace, and that a new construct was needed.[34] Others, including Harvard political scientist Joseph Nye, have argued that classic deterrence thinking has utility in cyberspace, but that this thinking must be "stretched" logically and creatively to move beyond it,[35] and preventing harm in cyberspace involves four formal mechanisms: denial, punishment, entanglement and norms.[36]

By the end of the 2010s, most experts on cyber-theory began to coalesce around a consensus

that classic deterrence premises ill-fitted to challenges in cyberspace. Deterrence theory's core concepts of denial, cost imposition, signaling and discrete attacks of major strategic consequence would not accurately address the emerging pattern of coercive Great Power interactions in cyberspace, with the exception of cyber interactions in the context of armed conflict, especially those triggering nuclear weapons. At all other times during rivalrous state-to-state activities involving strategic competition, confrontation, and other crisis management, the unique interdependences of cyberspace and the inherent challenges of attributing malevolent activities undermined the efficacy of deterrence by punishment or denial, and made a mockery of deterrence by entanglement. The bulk of cyberspace exchanges featured concepts of continuous interaction, cumulative strategic effect, persistent engagement, and forward defense. Cyber competition expert Emily Goldman put it this way in a 2020 book chapter on the topic,

> ... the frustration (crisis) was not that deterrence was not working at all but that it was not stopping the burgeoning numbers of attacks below the threshold of armed conflict and that these attacks cumulatively were leading to relative power loss. Deterrence arguably has been effective in the cyber strategic space of armed conflict. States, it would appear, are choosing to abide by conventions codified in United Nations Charter articles 2(4) and 51, which speak to the use of force and the right of self-defense in the event of armed attack. They also recognize that the United States can respond across domains (using its advantages) to a cyber-attack should they violate those conventions. The failures have been in assuming that deterrence would also be successful in the strategic space short of armed conflict, and, more fundamentally, in not understanding that those two strategic spaces even existed. Decision makers needed a paradigm shift to recognize the existence of distinct strategic spaces that had opened a seam in great power competition that in turn others were exploiting, to explain why this dynamic came about, and to offer a new strategy better aligned to cyberspace's structural and operational imperatives.[37]

The core challenge for deterrence and cyberspace is one of how to deter cyberattacks when they cannot be defended against and when attribution is ambiguous. Dr. Goldman and kindred cyberspace experts posited the existence of a new framework for securing strategic national interests in cyberspace: cyber-persistence theory. Persistence theory asks how to secure when you cannot deter.[38]

The **cyber persistence theory** paradigm does not deny the viability of deterrence in cyberspace. Indeed, the persistence paradigm agrees that classic framing of deterrence theory has applicability, but only if applied in enlightened and extended ways.[39] ***Cyber persistence theory*** restricts historic definitions of deterrence to where they logically reside – during cyber operations paired with armed attacks or equivalent to armed attacks. Persistence theory eschews overarching focus on specific "significant cyber incidents." Instead, it asserts that the realities of cyberspace mean that constant contact between rivals is omnipresent and

where "strategic significance" happens not as the result of any single event but rather emerges from the cumulative effect of a coercive cyber campaign compromising many individually less consequential operations carried out towards a coherent strategic end.[40]

Cyber persistence theory comports well with the realities of Great Power strategic competition where cumulative strategic effects can matter even more to relative power gains and losses than the risks from any one destructive cyber act. As American cyber expert James Lewis wrote recently,

> The most damaging cyber incidents are actions by states as part of some larger interstate confrontation or conflict. We will only see physical destruction and casualties from cyber operations when they are part of some larger armed conflict...This is important because, in the absence of the risk of significant damage that armed conflict brings, there is little incentive for states with offensive cyber capabilities to make concessions in their use, much less agree to disarm.[41]

Grounded in **cyber persistence theory**, a ***Relative Power Erosion Framework*** for successful Great Power Competition understands cyberspace that is micro-vulnerable but macro-resilient. The contested, fragmenting cyber domain is inherently exploitable but simultaneously stable in that states are unlikely to sustain a knock-out blow from a peacetime cyber-strike alone. Great Powers also are disinclined to escalate from cyber exchanges to armed conflict because the strategic risks from such escalation are infinitely more destructive and worrisome than those found alone in the cyber domain. Analysts who fear triggering armed conflict from persistent cyber operations and activities face a burden of proof that has not yet been evident in the cyber domain.[42]

Integrated Deterrence and Cyber Campaigning: Cyber Persistence and Hunt Forward

Cyberspace already features Great Power strategic campaigning - Russia and the PRC strategic cyber campaigns, often leveraging private hackers and criminals in addition to national security, intelligence, and military organizations and their operatives, for more than a decade. Meaningful consequences to these coercive strategic cyberspace activities by America's Great Power rivals has been too low. Although attribution of PRC and Russian strategic cyber coercion has improved over the past decade, the U.S. remains bereft of any meaningful ability to: remove options and opportunities for this coercion, create significant friction in their coercion attempts, or threaten them with credible and meaningful responses.[43]

It took Washington until 2018 to recognize the serious consequences from persistent strategic competition in the cyber domain. It then generated a limited, targeted, but credible response by endowing USCYBERCOM and the NSA with necessary authorities to protect the sanctity of U.S. national elections from external cyber-enabled manipulation and disruption. The USCYBERCOM-NSA strategy to counter strategic cyber-rivalry featured the twinned concepts of "persistent cyber engagement" and "hunt forward."[44]

USCYBERCOM and NSA's pursuit of persistent cyber engagement with forward-deployed hunt forward teams was unique in 2018 and remains so today. Working with U.S. partners and allies, hunt forward teams establish attribution and identify means and mechanisms involved in adversarial cyber campaigns that are far more than discrete malicious cyber activities. Forward USCYBERCOM teams integrate offensive and defensive operations to attain and maintain a cyberspace superiority over rivals conducting coercive cyber campaigns. Hunt forward teams are equipped for counter- cyber missions that can disrupt, negate, and/or destroy adversarial cyberspace activities and capabilities, both before and after their employment.[45]

The 2022 National Defense Strategy (NDS) Fact Sheet focuses on "integrated deterrence" as one of three primary ways that the Department of Defense (DoD) will advance national goals against its major rivals in the new era of Great Power Competition. It calls for developing and combining DoD strengths with other elements of national and international partner power across all warfighting domains and the spectrum of conflict.[46] Implicit in the "integrated deterrence" construct is that DoD must possess cyber assets with comparative advantages over those found in other government or private entities; thus, DoD cyber assets can be used effectively and efficiently across the range of strategically competitive activities with American Great Power rivals including those below the threshold of armed conflict.[47]

Integrated deterrence has been discussed during 2021 – 2022 as an effort in the modern era for the United States to frame deterrence across a number of different conceptual categories: the many domains of state-to-state interaction, *the broad spectrum of conflict*; all the instruments of national power, and with allies and partner states. Proponents suggest that modern era deterrence be integrated across multiple domains: conventional, nuclear, space, and cyber. They seek deterrence in these domains across an integrated spectrum of conflict from "high end" nuclear weapons conflict, conventional weapons conflict, and into the hybrid or gray zone spectrum of conflict where non-kinetic weapons and irregular tactics are utilized. They seek deterrence that is integrated across all instruments of national power – not just military – to dissuade would-be aggression including: military, diplomatic, economic, social, cultural, and information. They also aspire that integrated deterrence be constructed in a framework engaging allies and partner states in the processes.

The U.S. Cyberspace Solarium Commission Report of early 2020 recommended a national cyber strategy of ***layered cyber deterrence***.[48] Layered cyber deterrence aims in three ways to lower – not eliminate – the probability and adverse consequences of cyberattacks. The first is to deny benefits to cyber attackers by securing critical networks in a public-private partnership that promotes network security and national resilience. The second is to impose costs and the third deterrence layer is to shape behavior. Costs and shaping both require network ***persistence*** – the constant engagement and interaction of cyber entities across the international cyber environment.[49]

The 2022 NDS identifies "campaigning" as a critical component of DoD activity and aligns three DoD campaigning activities with other instruments of national power: (1) undermining acute forms of competitor coercion, (2) complicating competitor military preparations, and (3) developing/testing warfighting capabilities with allies and partners.[50]

Persistent Cyber Operations featuring ***hunt forward*** teams is fully consistent with the construct of layered cyber deterrence and strategic campaigning. Thus, a ***Relative Power Erosion Framework*** featuring *persistent engagement* and *hunt forward* USCYBERCOM teams should be key features of U.S. national integrated deterrence.

Whenever Cyber Persistence or defending forward conflates or even overlaps with offense, the legitimately defensive role inherent played by persistent engagement is imperiled. Objections to escalation and escalation dominance presuppose a spiraling interaction dynamic that inevitably leads offensive cyber operations to armed conflict. Yet contemporary academic literature views persistent cyber engagement, and even some offensive cyber activities as non-violent alternatives to conventional armed conflict, and hence less escalatory than activities involving conventional or nuclear weapons.[51] Moreover, focus upon "significant cyber incidents" traces back to the *model of episodic contact* dominant in nuclear and conventional deterrence.[52] "Strategic significance" in cyberspace seldom results from a single event, but rather, from the cumulative effect of a deliberate campaign comprising many individual operations/activities carried out toward a coherent strategic end.[53] None of the known cases of proactive, defend forward strategic cyber operations conducted against rival state-run or state-sponsored malicious cyber actors since 2018 have provoked dangerous escalation dynamics.[54] Thus, the burden of proof is on those concerned that offensive cyber actions could dangerously escalate, not the other way around.

THE WAY AHEAD FOR USCYBERCOM IN GREAT POWER COMPETITION

In the cyber-environment, as in all domains of state-to-state interactions, Great Power rivals compete over three strategic "prizes:" (1) intellectual property that contributes to how innovation occurs and how wealth is generated; (2) legitimacy – political and social; and (3) privacy of personal information.[55]

Cyberspace is a domain of economic, diplomatic, informational, and military interaction and persistent, integrated Great Power campaigns up to the very brink of armed conflict. Well before crises arise, robust cyberspace campaigns and counter-campaigns, must integrate the best government-wide and private sector tools, techniques and procedures and thereby deter. At the same time if deterrence fails, the ability to counter adversaries that opt for kinetic warfare remains an ongoing imperative.[56] The construct of campaigning lends itself inherently to incorporation of key U.S. military cyber assets – especially those uniquely well-developed already for "hunt forward" and "cyber persistence" into the competitive framework of cyber activities amongst and between America and its Great Power rivals.

Beginning in the early 2010s, and accelerating over the past half-decade, USCYBERCOM has been granted limited and important authorizations to conduct non-combat, persistent cyber offensive operations.[57] Since at least 2017, the USCYBERCOM-NSA nexus reportedly has participated in limited, time-constrained persistent engagement peacetime operations from forward locations – operations that penetrate, exploit data, disrupt, or retaliate against rival non-state groups (like ISIS) and hostile states (e.g., Russia and Iran), and others that threaten the U.S., our allies, or major global security and sovereignty norms.[58]

Over the past decade, and especially since 2017/2018, USCYBERCOM has shifted from a response force focused on defending DoD networks and supporting counterterrorism and conventional force activities, to one featuring ***persistent engagement***. Since its March 2018 vision document, USCYBERCOM has featured a strategic concept of ***cyber persistence***, recognizing that successful Great Power Competition requires actively contesting and confronting adversary efforts to enhance relative power and achieve decisive strategic outcomes from cumulative tactical impacts in cyberspace.[59] To meet this challenge, USCYBERCOM must operate continuously both *forward* – in physical and virtual realms – and at increasing scale. Thus, the 2018 cyber-strategic command vision formalizes a framework for operations to secure U.S. cyberspace by influencing and shaping adversary behavior through ***Persistent and Integrated Forward Engagement***.[60]

In adopting ***Persistent Forward Engagement***, USCYBERCOM acknowledged that deterrence of adversary malevolent actions *within the cyberspace domain*, while feasible, requires a different kind of operational framework.[61] Helpfully, the FY2019 National Defense Authorization Act (NDAA) designated cyber reconnaissance and surveillance as a traditional military activity – providing enhanced authority for offensive cyber operations in campaign planning and responses to malign adversary activities.[62]

USCYBERCOM military units and procedures have provided vital and unreplaceable support to U.S. civilian authorities and agencies in a number of campaigns including ones in Montenegro that improved American cyber defenses ahead of the 2020 elections and ongoing actions from forward locations to inoculate the U.S. and our allies from the persistent threat from Russian cyber actors and their proxies supporting war against Ukraine.[63]

Together, the limited USCYBERCOM campaigns have achieved critical competitive objectives in the following strategically significant categories:

- Disrupt Russian foreign influence operations in cyberspace targeting U.S. and western elections;
- Disrupt or degrade Russian and PRC economic espionage operations;
- Deter, disrupt, or degrade Russian (and Iranian) cut-out and proxy cyber operations targeting U.S. critical infrastructure;

- Identify and publicly attribute cyberattack malware by the so-called MuddyWater Group to Iranian Intelligence Services (MOIS) actively used to siphon data from government and telecom firms across the Middle East, publishing the code it used to alert improved cyber defense.[64]

The open question is how best to extend/expand the legal, ethical, and effective reach of U.S. military cyber campaigns and operations during times of competition and confrontation. As it was when General Keith Alexander testified before Congress in 2010, there remains much uncharted territory in the world of cyber policy, law, and doctrine.[65] But the historical record of military participation in strategic competition and the recent successes of USCYBERCOM campaigns and operations safeguarding vital American relative power in a peacetime environment both validate the legitimacy of greater military cyber participation in cyber campaigns – at least for a period of time.

The 'dual hat' USCYBERCOM-NSA command relationship already appears optimized to assure the agile and responsive interface between cyber-intelligence and cyber-operations against strategic rivals below the threshold of armed conflict.[66] The proper orientation and appropriate resourcing of USCYBERCOM to scale for these critical cyber campaigns requires greater American policy maker attention. To be successful at the appropriate scale, expanded national investment in cyber national mission teams and a more detailed legislative agenda establishing the legal and bureaucratic authorities for military-led, cyber persistence activities is necessary.[67]

Retaining the USCYBERCOM-NSA Dual Hat

The USCYBERCOM-NSA tight coupling and shared "dual hat" command structure establishes many vital interactions for successful strategic cyber-competition with America's Great Power adversaries.[68] Among these critical synergies are the three identified frequently by former USCYBERCOM Commander, General Paul Nakasone: "..speed, agility, and a unity of action between world class code-makers and code-breakers."[69] Unique among USG agencies and agency-teams, USCYBERCOM today alone can operate in cyberspace outside the U.S. against adversaries before they can do great harm inside the United States. USCYBERCOM can establish "persistent engagement" while "defending forward" in cyberspace with partners and allies that help attribute malicious actors, disrupt their activities before they strike, and impose costs on them that make it difficult to operate in space and time against strategically significant elements of national power.[70] The USCYBERCOM-NSA "dual hat" has stirred debate since USCYBERCOM was established in 2010, and numerous reviews and studies have been done about this peculiar relationship with an eye to separating them when appropriate. A 2023 report led by former Chairman of the Joint Staff, General Joseph Dunford, determined that retaining the "dual hat" for the foreseeable future was a net positive for national security.[71]

Retaining the "dual hat" aligns with geopolitical realities for cyberspace in this new era of multi-polar Great Power competition. Other key USG sectors need to build-out credible and responsible defensive, offensive, and enabling cyber tools to compete with rival state exploitation of cyberspace for decisive strategic advantage. But today, the dynamics of an intensifying multi-state Great Power Competition warn against under-utilizing the well-developed "hunt forward" and "persistent engagement" capabilities now found almost uniquely in the USCYBERCOM-NSA nexus. Managed in accordance with liberal and democratic values, the use of USCYBERCOM event-tested cyber ***hunt forward*** teams and ***persistent engagement*** strategies must be enabled and resourced for some reasonable transition period – likely through the end of the 2020s – if the U.S. is to stem the erosion of its relative power in critical areas before they compound into negative strategic impact.[72]

Expanding (Temporarily) Cyber Mission Force (CMF) Teams for Vital Strategic Competition

USCYBERCOM's 2018 vision argues that, at least for a period of time, U.S. whole of government capabilities and processes remain insufficient and destined to keep the U.S. in a reactive mode after costly intrusions or attacks occur into America's cyber critical infrastructure, and that DoD is the leader (at least for now) in building the operational expertise and capacity to meet critical cyberspace threats and stop cyber aggression before it can be used by our rivals to secure strategic advantage.[73] This analysis remains accurate in 2024, yet more capacity is needed to provide options and capabilities to conduct strategically significant cyber competition throughout times of peace and up to the brink of actual armed conflict.[74]

The USCYBERCOM-NSA nexus remains the right locus for expanding capacity for strategically significant cyber competition.[75] But this expansion needs be prudent, constrained, and properly resourced and authorized by Congress and the White House.

As of early 2024, USCYBERCOM had just 133 Cyber Mission Force (CMF) teams with varying cyber-operational mission sets.[76] Only some of these are organized for the important ***hunt forward*** missions capable of assuring persistent engagement in partnership with U.S. international partners and allies. The number of CMF teams is programmed to grow to 147 by late 2024, but even at this expanded number, CMF teams could not undertake a vast array of missions required to contest single-event or stochastic ransomware, denial of service attacks, or espionage activities across the national economic, political, social and personal privacy dimensions of cyberspace.[77] Not all cyber-attacks against America and its allies are strategic in nature despite the understandable concerns felt by their victims.[78] Instead, the USG requires a more robust and durable capability to conduct persistent engagement and hunt forward missions aimed against the deliberate cyber campaigns undertaken by Great Power rivals China and Russia. The legitimate targets of these American cyber campaigns should include state-based cyber actors and state-affiliated ones credibly tied to these Great Power competitor state strategic cyber-campaigns.

Additional CMF teams should be resourced and USCYBERCOM-NSA given Congressional enabling authorities to develop and execute cyber campaign and counter-cyber campaign plans that pursue state and non-state actors credibly deemed culpable of conducting cyber campaigns directed by or coordinated with the PRC or Russia to achieve strategic cumulative effects against the U.S. or allies in the following vital areas of national power:

- Relative economic advantage through industrial espionage or via disruption and degradation of US productivity;
- Political confidence and social cohesion by manipulating the U.S. elections processes;
- Citizen confidence and trust in the U.S. government's ability to safeguard the privacy and personal security of citizens.

USCYBERCOM should be appropriately resourced for growth to 200 total CMF teams over the course of the 2025-2030 Future Years' Defense Program (FYDP 25-30). The NSA budget should be enhanced in parallel to build-out the support structure for these teams. This growth should allow for USCYBERCOM to generate forward presence by an additional 25-30 ***hunt forward*** teams at any given time with explicit focus on campaigns aimed at Russia and the PRC and in the three areas of national strategic competition.

Military-led cyber campaigns are a short-term necessity but not optimal for the long haul. As Great Power Competition continues to evolve, expedient and necessary use of military cyber capabilities to conduct persistent cyber engagement should be replaced with capabilities within the civilian governmental structure that is befitting of a 'new normal' of endemic competitive relations between the Great Powers.

Congress and the Executive should push the following government organizations to generate their own CMF-style ***hunt forward*** teams with appropriate funding and authorities to take the lead on cyber campaigns by the early 2030s: Department of Homeland Security (DHS), Department of State (DoS), Department of Justice (DoJ), Department of Commerce (DoC), and the FBI. The *Cyberspace Solarium Commission Report* of 2020 calls for expansion of the concept of "defend forward" across the government built on the concept originated in the Department of Defense but using all instruments of national power.[78] Empowering hunt forward teams in these agencies would enhance America's competitive ability to disrupt and defeat growing adversary cyber campaigns across an array of threat vectors. The U.S. *National Cybersecurity Strategy* of March 2023 also establishes this as a necessary part of the U.S. government's strategic objective to integrate federal cyber disruption activities, but it also notes that upgrading and properly organizing this will take time.[80] So for now, USCYBERCOM-NSA cyber persistence and disruptive capabilities are the best we have. The longer-term process of federal integration should include provisions for a cross-leveling of individuals and resources from the new USCYBERCOM CMFs to the interagency team analogs with an aim of drawing back USCYBERCOM CMF teams to around 150 as the interagency brings some 50 or so teams into fully operational status during the 2030s.[81]

CONCLUSIONS

America's once dominant geostrategic position has measurably diminished. Today we find ourselves in an evolving era of Great Power Competition. Also seriously under threat is America's longstanding dominance in cyberspace. Where American ascendance in cyber hardware, software, infrastructure design, and norms for appropriate use in a one-world cooperative framework once ruled supreme, today's cyber domain is characterized by increasing fragmentation, a drift into confrontational and coercive activities by one state against many others, and a preference by Russia and the PRC – America's Great Power rivals – to use cyberspace for aggressive campaigns that seek relative power gains against the U.S. and its allies in strategic competition.

Although it may be pursued among contemporary allies and partners, *a legal/law enforcement framework* for Great Power strategic competition in cyberspace is not sufficient in the face of durable cyber domain fragmentation. Instead, the U.S. must pursue a ***Relative Power Erosion Framework***, which requires use of all elements of U.S. national power. A ***Relative Power Erosion Framework*** for strategic competition in cyberspace aligns well with the new **cyber persistence theory**, and USCYBERCOM's ***persistent cyber engagement*** conducted by ***hunt forward*** military cyber teams.

A ***Relative Power Erosion Framewor***k featuring military cyber teams must be disciplined and focused on truly strategic cyber campaigns (and counter cyber campaigns) designed against Russian and Chinese cyber organizations and affiliated cyber actors conducting cyber campaigns aimed at one of three relative strategic gains:

- ***Relative economic advantage*** through espionage, disruption and degradation.
- Reduced ***domestic political cohesion, confidence and trust in the electoral system***; and
- Reduced faith and confidence in the U.S. being able to protect its citizens from coercive cyber campaigns that compromise ***privacy and personal security***.

A ***Relative Power Erosion Framework*** should feature USCYBERCOM CMF teams for a period of time limited to the end of the 2020s. By 2030, the U.S. should establish civilian interagency teams that operate as the military CMF teams operate today and thus take full control of persistent cyber engagements and hunt forward campaigns. The military-to-civilian transition for these peacetime cyber campaigns will help signal the necessary change in mindset by the entire U.S. government from one mistakenly assuming cyber cooperation to one properly structured for persistent and effective cyber competition.

DISCLAIMER

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

NOTES

1. Thomas F Lynch III ed., *Strategic Assessment 2020: Into a New Era of Great Power Competition*, (2020). Washington, D.C.: National Defense University (NDU) Washington, D.C.: National Defense University (NDU) Press, https://ndupress.ndu.edu/Portals/68/Documents/Books/SA2020/Strategic-Assessment-2020.pdf/, 59-65; Ali Wyne, *America's Great Power Opportunity: Revitalizing U.S. Foreign Policy to Meet the Challenges of Strategic Competition*, (July 5, 2022). Boston, MA: Polity Press, 45-65.
2. "ICANN's Historical Relationship with the U.S. Government," ICANN.org, last accessed, September 30, 2024, https://www.icann.org/en/history/icann-usg; Lynch ed., *Strategic Assessment 2020*, 46-59.
3. Lynch ed., *Strategic Assessment 2020*, 46-59
4. Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, (2022). *China's Cyber Operations: A Rising Threat to American National Security*, New York: Margin Research LLC for DARPA, 8-37; Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, (2022), *Russia's Cyber Operations: A Rising Threat to American National Security*, New York: Margin Research LLC for DARPA, 1-18, 49-82.
5. Fletcher Schoen and Christopher J. Lamb, Deception, *Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, (2012). NDU-INSS Strategic Perspectives 11, Washington, D.C.: NDU-Press; Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
6. Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict, (2020). Washington, D.C.: Georgetown University Press; Justin Sherman, Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior*, (September 19, 2022). Washington, D.C.: Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.
7. Thomas F. Lynch, III, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," (July 25, 2024). *Joint Forces Quarterly*, Volume 114, 3rd Quarter, Washington, D.C.: NDU Press, https://digital-commons.ndu.edu/joint-force-quarterly/vol114/iss2/4/, 18; U.S. Department of Defense, *Summary – 2023 Cyber Strategy of the Department of Defense*, (September 2023). Washington, D.C:, https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/, 4-5.
8. Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
9. U.S. Department of Justice, *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*, (September 4, 2024). Washington, D.C., https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; Shanon Bond, "Microsoft says Russia's election interference efforts have pivoted to Harris and Walz," (September 17, 2024). *NPR.org*, https://www.npr.org/2024/09/17/nx-s1-5116267/russia-election-interference-harris-walz-microsoft.
10. Cybersecurity and Infrastructure Security Agency (CISA), "Alert AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," (last revised May 9, 2022). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a; Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
11. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community – 2024*, (February 2024). https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf, 12; Tiffany Hsu and Steven Lee Myers, "China's Advancing Efforts to Influence the U.S. Election Raise Alarms," (April 2, 2024). *The New York Times*, https://www.nytimes.com/2024/04/01/business/media/china-online-disinformation-us-election.html
12. Christopher Bing and Katie Paul, "US voters targeted by Chinese influence online, researchers say," (September 3, 2024). Reuters.com, https://www.reuters.com/world/us/us-voters-targeted-by-chinese-influence-online-researchers-say-2024-09-03/; Micah McCartney, "'Spamouflage': China Cyber Army Mimics Americans to Influence US Election," (September 3, 2024). *Newsweek.com*, https://www.newsweek.com/china-news-cyber-army-mimics-americans-influence-us-election-2024-1947901.
13. U.S. Department of Defense, *Summary – 2023 Cyber Strategy*, 4; Dave Aitel, et al., *China's Cyber Operations*, 8-37.
14. James A. Lewis, " How Much Have the Chinese Actually Taken?" (March 22, 2018). *CSIS.org*, https://www.csis.org/analysis/how-much-have-chinese-actually-taken.
15. James A. Lewis, "China's Economic Espionage: Why It Worked in the Past but It Won't in the Future,"(November 13, 2012). *Foreign Affairs*, https://www.foreignaffairs.com/articles/china/2012-11-13/chinas-economic-espionage.; Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices related to Technological Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (March 22, 2018). https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/june/section-301-investigation-fact-sheet.

NOTES

16. Federal Bureau of Investigation, *Executive Summary – China: The Risk to Corporate America*, (2019). Washington, D.C., https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf.
17. Dave Aitel, et. al., *China's Cyber Operations; Office of the United States Trade Representative, Findings of the Investigation into China's Acts, Policies, and Practices related to Technological Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (March 22, 2018). https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
18. Nick Beecroft, "The West Should Not Be Complacent about China's Cyber Capabilities," (July 6, 2021). Washington, D.C.: Carnegie Endowment for International Peace, https://carnegieendowment.org/2021/07/06/west-should-not-be-complacent-about-china-s-cyber-capabilities-pub-84884.
19. Eric Tucker, "FBI, US Agencies Look beyond Indictments in Cybercrime Fight," (January 18, 2022). *US News and World Report*, https://www.usnews.com/news/politics/articles/2022-01-18/fbi-us-agencies-look-beyond-indictments-in-cybercrime-fight.
20. Karen A. Rasle and William R. Thompson, *The Great Powers and Global Struggle*, 1490-1990, (1994). Lexington, KY: *University of Kentucky Press*, 73-97 and 157-72; Thomas F. Lynch III, "Cyberspace: Great Power Competition in a Fragmenting Domain," (2024). Orbis 68, Issue 4, https://doi.org/10.1016/j.orbis.2024.09.007, 607-623
21. Clint Watts, "Five Generations of Online Manipulation: The Evolution of Advanced Persistent Manipulators," (March 11, 2019). *Foreign Policy Research Institute – National Security Program E-note*, https://www.fpri.org/article/2019/03/five-generations-of-online-manipulation-the-evolution-of-advanced-persistent-manipulators/. Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
22. Council on Foreign Relations, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, (June 2022). New York, NY: Council on Foreign Relations [CFR], Independent Task Force Report No. 80, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace; Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
23. James A. Lewis, "Sustaining Progress in International Negotiations on Cybersecurity," (July 25, 2017). The Center for Strategic and International Studies (CSIS), https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity; Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
24. Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed.*, (2017). Cambridge: Cambridge University Press; The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual*, (last accessed September 30, 2024). Tallinn, Estonia, https://ccdcoe.org/research/tallinn-manual/.
25. In December 2023, the U.S. and ten European allies and strategic partners endorsed the Tallinn Manual as a 'Mechanism' to coordinate civilian cyber assistance to Ukraine in its struggle with Russia. The arrangement indicated the globally constrained, but sub-group viable potential for legal norms and procedures in cyber space during an era of accelerating domain fragmentation. See, U.S. Department of State, *Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine* (December 20, 2023). Washington, D.C., https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/.
26. Mieke Eoyang and Chimene Keitner, "CyberCrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity," (February 2, 2021). *Journal of National Security, Law and Policy*, https://jnslp.com/2021/02/02/cybercrime-vs-cyberwar-paradigms-for-addressing-malicious-cyber-activity/, 327; Gary D. Brown, "Spying and Fighting in Cyberspace," (2016). *Journal of National Security Law & Policy*, https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf.
27. Eric Tucker, "FBI, US Agencies Look beyond Indictments in Cybercrime Fight," (January 18, 2022). *APNews.com*, https://apnews.com/article/technology-indictments-crime-europe-hacking-8e97ebd22a64a28bfc4ea83c123ee1dc; University of Baltimore Law Review Staff, "Indictments Don't Deter Cyberattacks, So Why Does the U.S. Keep Using Them? An Analysis in Response to the U.S.'s Recent Indictment of Six Russian Hackers," (February 26, 2021), Baltimore, MD: *University of Baltimore Law Review*, https://ubaltlawreview.com/2021/02/26/indictments-dont-deter-cyberattacks-so-why-does-the-u-s-keep-using-them-an-analysis-in-response-to-the-u-s-s-recent-indictment-of-six-russian-hackers/.
28. Justin Sherman, "Russia's largest hacking conference reflects isolated cyber ecosystem," (January 12, 2023). *Brookings.com*, https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.
29. Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, (May 19, 2022). Oxford: Oxford University, https://academic.oup.com/book/41918.

NOTES

30. Emily O. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn," (Winter 2022), *Cyber Defense Review* Vol. 7, No. 1, 113-120, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/CDR_V7N1_WINTER_2022_Special_Edition_r7.pdf; Jacqueline C. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," (May 10, 2019); *Lawfare*, https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy.
31. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
32. Cyberspace Solarium Commission, *Cyberspace Solarium Commission*, (March 2020). Report, Washington, D.C.: Senator Angus King and Representative Mike Gallagher, Co-chairmen, https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/; Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn," Page?
33. Martin Libicki, *Cyberdeterrence and Cyberwar,* (2009). Santa Monica: RAND Corporation, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf,
34. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," (June 23, 2017). Orbis Vol. 61, No. 3, Fall 2017, https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/, 381-393.
35. Richard L. Harknett and Joseph S. Nye Jr., "Is Deterrence Possible in Cyberspace?," (November 1, 2017) *International Security*, Vol. 42, No. 2, https://doi.org/10.1162/ISEC_c_00290, 199
36. Joseph Nye Jr., "Deterrence and Dissuasion in Cyberspace," (January 1, 2017). *International Security*, Vol 41, No. 3, Fall 2017, https://doi.org/10.1162/ISEC_a_00266, 44-71; Harknett and Nye, "Is Deterrence Possible in Cyberspace?," 199.
37. Jacquelyn C. Schneider, Emily O. Goldman, and Michael Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, (2020). Newport, RI: U.S. Naval War College – Newport Papers #45, https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.
38. Emily O. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
39. Chris Inglis, "Cybersecurity Cooperation," (May 11, 2022), Remarks at The Lowy Institute, Sydney Australia. Locationhttps://www.lowyinstitute.org/publications/regional-cybersecurity-cooperation-evolving-geopolitical-landscape.
40. Schneider, Goldman, and Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, 40-41; Max Smeets and Herb Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence and Defend Forward," (November 28, 2018). *Lawfare*, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward; Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
41. James A. Lewis, "Private Actors Roles in International Cybersecurity Agreements – Unlearned Lessons," (Winter 2022). *The Cyber Defense Review* ,Vol. 6, No. 1, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/04_Lewis_CDR_V7N1_WINTER_2022.pdf?ver=l865DxcB5fL5jJxwk7n9eg%3d%3d, 34-39.
42. Fischerkellers, Goldman, and Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, page?
43. Thomas L. Lynch III, "Cyberspace: Great Power Competition in a Fragmenting Domain," (September 2024). *Orbis* Volume 68, Issue 4, https://www.sciencedirect.com/science/article/abs/pii/S0030438724000516, 620-621.
44. Paul Nakasone, "A Cyber Force for Persistent Operations," (2019). *Joint Forces Quarterly* Vol. 92, No. 1, 10-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf; Smeets and Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence and Defend Forward.";" Lynch, "Cyberspace: Great Power Competition in a Fragmenting Domain," 621.
45. Paul Nakasone, "A Cyber Force for Persistent Operations;" Paul Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, U.S. Cyber Command before the 117th Congress," (April 5, 2022). https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/. Lynch, "Cyberspace: Great Power Competition in a Fragmenting Domain," 621.
46. U.S. Department of Defense, *Fact Sheet: 2022 National Defense Strategy,* (March 2022). https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF, 2.
47. Michael P. Fischerkeller, "What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?", (May 3, 2022). *Lawfare,* https://www.lawfareblog.com/what-does-2022-nds-fact-sheet-imply-forthcoming-cyber-strategy.
48. *Cyberspace Solarium Commission (CSC) Report*, 1-7.
49. *Cyberspace Solarium Commission (CSC) Report*, 26-30.
50. U.S. Department of Defense, *Fact Sheet: 2022 National Defense Strategy,* 2.

NOTES

51. Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," (Fall 2020). *Texas National Security Review* Vol. 3, No. 4, https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/; Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," (January/February 2022). *Foreign Affairs* Vol. 101, No. 1: 10-21, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning; Max Sweets, "The Strategic Promise of Offensive Cyber Operations," (Fall 2018). *Strategic Studies Quarterly,* Vol. 12, No. 3: 105, https://www.airuniversity.af.edu/; *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, (June 2022). New York, NY: Council on Foreign Relations [CFR], Independent Task Force Report No. 80.
52. Florian J. Egloff and James Shires, "The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence," (October 12, 2021). *European Journal of International Security*, 1-20, https://www.cambridge.org/core/journals/european-journal-of-international-security/article/better-angels-of-our-digital-nature-offensive-cyber-capabilities-and-state-violence/B225F961FD2212E34FDB0B267A1CB5E6
53. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
54. Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace*, (2023). Oxford: Oxford University Press, 2023), Chapters 1 and 6; J.E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyber Attacks on Iran," (June 22, 2019). *New York Times*, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; R. Chesney, "The Legal Context for CYBERCOM's Reported Operations Against Iran," June 24, 2019. *Lawfare.com*, https://www.lawfareblog.com/legal-context-cybercoms-reported-operations-against-iran; Erica D. Bohrghard, "What a US Operation Against Russian Trolls Predicts About Escalation in Cyberspace," (March 22, 2019). *War on the Rocks*, https://warontherocks.com/2019/03/what-a-u-s-operation-against-russian-trolls-predicts-about-escalation-in-cyberspace/.
55. Michael Warner, "A Brief History of Cyber Conflict," (2020). In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner. Newport, RI: U.S. Naval War College – Newport papers #45, 2020, 20.
56. Chris Demchak, "When Irregular Becomes Everywhere: The Cybered Fight in Unwanted Places," (July 13, 2022). *Modern War Institute*, https://mwi.usma.edu/when-irregular-becomes-everywhere-the-cybered-fight-in-unwanted-places/
57. The Cyber National Mission Force, *Before the Invasion: Hunt Forward Operations in Ukraine*, (November 28, 2022). Washington, D.C: USCYBERCOM, https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf; Anastasia Obis, "Cyber Command Finishes its First 'Hunt Forward' Operation in Latin America," (June 30, 2023). *GovCIO.com*, https://governmentciomedia.com/cyber-command-finishes-its-first-hunt-forward-operation-latin-america.
58. U.S. Department of Defense, *Summary – 2023 Cyber Strategy of the Department of Defense*, 6-7; David E. Sanger and Mark Mazzetti, "US had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," (February 16, 2016). *The New York Times*, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html; Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," (October 16, 2019). *Reuters*, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK; Michael Martelle, ed., *USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY*, (January 21, 2020). Washington, DC: GWU National Security Archive, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony; Florian J. Egloff, "Public Attribution of Cyber Intrusions," (Winer 2020). *Journal of Cybersecurity* Vol. 6, No. 1, https://doi.org/10.1093/cybsec/tyaa012, 1-12; Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," (March 10, 2021). *Journal of Strategic Studies*, Vol 36, No 3, 1–32. https://doi.org/10.1080/01402390.2021.1895117.
59. Paul Nakasone, "A Cyber Force for Persistent Operations;" Paul Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," (August 25, 2020). *Foreign Affairs*, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
60. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority, A Command Visions for US Cyber Command*, (April 2018). Washington, D.C.; https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, 1-3.

NOTES

61. Fischerkeller and Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," 381-393.
62. Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," (July 26, 2018). *Lawfare*, https://www.lawfaremedia.org/article/law-military-cyber-operations-and-new-ndaa.
63. Fischerkeller, "What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?"
64. Sean Lyngaas, "U.S. Military Links Prolific Hacking Group to Iranian Intelligence." (January 12, 2022). *CNN.com*, https://edition.cnn.com/2022/01/12/politics/iran-cyber-command-hacking-muddywater/index.html.
65. Robert Chesney and Max Smeet, "Intervention: Exploring Cyber Conflict and Competition," (October 20, 2020). *War on the Rocks*, https://warontherocks.com/2020/10/the-dynamics-of-cyber-conflict-and-competition/
66. Jim Garamone, "Cyber Command, NSA Successes Point Way to Future," (March 8, 2023). *Defense.gov*, https://www.defense.gov/News/News-Stories/Article/Article/3322765/cyber-command-nsa-successes-point-way-to-future/; National Security Agency, "How NSA, U.S. Cyber Command are defending midterm elections: One team, one fight," (August 25, 2022). NSA.gov, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight/.
67. Lizbeth Perez, "CYBERCOM Working 25 'Hunt-Forward' Missions This Year," (September 5, 2024). *MeriTalk.com*, https://cdn.meritalk.com/articles/cybercom-working-25-hunt-forward-missions-this-year/; Chauncey Goss, "DoD's FY24 Cyber Budget," (April 17, 2023). *Federal Budget IQ.com* https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/
68. Chris Demchak, "Five Reasons Not to Split Cyber Command from the NSA Any Time Soon – If Ever," (March 5, 2021). *War on the Rocks,* https://warontherocks.com/2021/03/five-reasons-not-to-split-cyber-command-from-the-nsa-any-time-soon-if-ever/.
69. Paul Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, US Cyber Command before the 117th Congress."
70. Ellen Nakashima and Tim Starks, "NSA, Cyber Command should continue to share a leader, a key review suggests," (December 22, 2022). *The Washington Post*, https://www.washingtonpost.com/politics/2022/12/22/nsa-cyber-command-should-continue-share-leader-key-review-suggests/.
71. Nakashima and Starks, "NSA, Cyber Command should continue to share a leader, a key review suggests."
72. Anna Scherbina, "How much do US businesses lose due to malicious cyber activity?" (May 3, 2024). *The Hill.com*, https://thehill.com/opinion/cybersecurity/4641199-cyberattack-businesses-money-loss-malicious-cybersecurity/; Anna Ribeiro, "FBI warns of increased cyber threats to expanding US renewable energy sector," (July 2, 2024). *IndustrialCyber.com*, https://industrialcyber.co/threats-attacks/fbi-warns-of-increased-cyber-threats-to-expanding-us-renewable-energy-sector/; Michael J. Mazarr, Tim Sweijs and Daniel Tapia, *The Sources of Renewed National Dynamism – RAND Report -RRA2611-3*, (April 30, 2024). https://www.rand.org/pubs/research_reports/RRA2611-3.html.
73. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority, A Command Visions for US Cyber Command*, 4-5.
74. Jaclyn Kerr and Alexander Campbell, *Workshop Summary: Strategic Competition in Cyberspace: Challenges and Implications*, (July 10, 2019). Livermore, California: Center for Global Strategic Research, Lawrence Livermore National Laboratory, https://cisac.fsi.stanford.edu/publication/strategic-competition-cyberspace-challenges-and-implications.
75. Demchak, "Five Reasons Not to Split Cyber Command from the NSA Any Time Soon – If Ever."
76. Congressional Research Service, *FY2023 NDAA: Cyber Personnel Policies*, (March 6, 2023). Washington, D.C.: CRS Report R47270, https://crsreports.congress.gov/product/pdf/R/R47270, 1-3; Mark Pomerleau, "US Cyber Command releases first full budget," (March 13, 2023). *Defense Scoop*, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.
77. Pomerleau, "US Cyber Command releases first full budget."
78. Alan Suderman, "Global War on Ransomware? Hurdles Hinder the US Response," (June 5, 2021). *Associated Press*, https://apnews.com/article/europe-hacking-health-coronavirus-pandemic-technology-5d69e46750abd3b40fc9adf395869c7d.; Erica Lonergan and Mark Montgomery, "What Is the Future of Cyber Deterrence?" (2021). *SAIS Review of International Affairs* Vol. 41, No. 2, 61-73, https://muse.jhu.edu/article/852327.
79. *Cyberspace Solarium Commission (CSC) Report*, 28-29.
80. The White House, *National Cybersecurity Strategy*, (March 2023). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 14-15.

NOTES

81. As of mid-2024, the U.S. Government is advancing slowly toward more robust, interagency-wide, coordinated cyber

operations. The USCYBERCOM-NSA Integrated Joint Cyber Center, launched in 2018, is a productive node for agency-wide collaboration on cyber defense. Non-DOD, government agency cyber persistence and hunt forward operations are inching forward. The Cybersecurity and Infrastructure Security Agency (CISA) established and exercised Red Team "hunt" operations in support of national defense in depth during 2023 and 2024, but its capabilities are nascent. The FBI has special Cyber Action Team (CAT) of approximately 65 members to deploy across the globe in response to malicious cyber activity threatening U.S. public safety, national security or economic security. This is an incident reaction team not yet a hunt forward one. See, Mark Pomerleau, "Five years in, a look at how Cybercom and NSA's Integrated Cyber Center improved coordination of operations," (May 31, 2023). *DefenseScoop.com*, https://defensescoop.com/2023/05/31/five-years-in-a-look-at-how-cybercom-and-nsas-integrated-cyber-center-improved-coordination-of-operations/; Cybersecurity and Infrastructure Securaity Agency, "CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth," (July 11, 2024). CISA.gov, Cybersecurity Advisory, Alert Code: AA24-193A, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-193a; Federal Bureau of Investigation, "Meet the Cyber Action Team," (July 23, 2024). *FBI.com*, https://www.fbi.gov/news/stories/meet-the-cyber-action-team.