JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–10
https://doi.org/10.1093/cybsec/tyad006
Research paper

Research paper

The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation

Erica D. Lonergan [1,*,‡] **and Jacquelyn Schneider** [2]

[1]Army Cyber Institute, United States Military Academy at West Point, 2101 New South Post Road, West Point, NY 10996, USA and [2]Hoover Institution, Stanford University, 434 Galvez Mall, Stanford University, Stanford, CA 94305, USA

*Corresponding author. 2101 New South Post Road, West Point, NY 10996, USA. E-mail: eborghard@gmail.com
‡The views expressed are personal and do not reflect the policy or position of any U.S. government organization or entity.

Received 16 August 2022; revised 25 January 2023; accepted 27 February 2023

Abstract

Cyberspace's role in military power is vociferously debated. But how do these ideas manifest in cyber strategy? In this article, we trace the development of ideas about military cyber power, with a focus on the USA. In particular, we use a decade of US defense cyber strategies as a lens to explore how ideas about the role of the military in promoting cyber norms, the feasibility of cyber deterrence, and the risks of escalation have morphed over time. In doing so, we identify sources of continuity and discontinuity. We then turn to the academic literature to evaluate those ideas and appraise US defense cyber strategies, identifying gaps and tensions. Finally, we leverage these insights to provide recommendations for future US defense cyber strategies.

Introduction

It has been an extraordinary decade for the US military in cyberspace. The USA developed strategies and doctrines for cyberspace; created a Cyber Command, Cyber Mission Force (CMF), service cyber commands, and led numerous task forces [1]. To build these organizations, the Department of Defense (DoD) had to make sense where there was none, cultivating beliefs about the ways cyberspace would influence conflict, escalation, and the balance of power [2]. These ideas were articulated in three defense cyber strategies, penned in 2011, 2015, and 2018. Their evolution reveals both ideational continuity and change. In this article, we explore how the defense cyberspace policymaking community has aimed to make sense of the cyberspace environment by articulating ideas about military cyber power [3, 4]. Specifically, we examine three concepts that have dominated US defense thinking about cyberspace: how norms shape cyber behavior; the feasibility of deterrence; and the risks of cyber escalation. In doing so, we take an inward-out approach: rather than applying scholarly theories to assess policymaking, we use the intellectual evolution of defense cyber strategies as a lens to evaluate how ideas have been contested and debated in practice. We then turn to academic literature to appraise US defense cyber strategies. We conclude by discussing implications for future US defense cyber strategies.

Evolution of ideas and US defense cyber strategy

Despite a focus on structural variables and rationalism within many discussions of strategy [5, 6], a large body of scholarly work finds that ideas play a central role in how decisionmakers build strategies and policies [7–10]. Especially when decisionmakers must make choices under uncertainty, ideas help build road maps for decisions, enable bureaucratic factions to come to agreement when there is no status quo equilibrium, and can, in the long term, create habits that lead to policy path dependencies [9, 11]. Ideas are, therefore, central to how defense establishments organize themselves for new threats and take advantage of new capabilities. Cyberspace, as an emerging domain that poses both threats and opportunities, is therefore an ideal case for the influence of ideas. So how did these ideas emerge, evolve, and define US defense cyber strategies?

Remarkably for a defense establishment often loathe to change or develop new ideas [11], US defense cyber strategy underwent two

© The Author(s) 2023. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial 1 License (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

significant transformations in a relatively short period of time. The first shift took place between the 2011 and 2015 cyber strategies, both promulgated during the same presidential administration. During this time, the Defense Department's approach moved from one of optimism about the Internet and democratic values to pessimism and fear. But while perceptions of threat changed between 2011 and 2015, the US approach to dealing with cyber threats—and in particular the military's role—remained remarkably stagnant. This was mainly because core ideas about escalation, norms, and deterrence in cyberspace remained the same throughout the Obama administration, turning into linchpin defense assumptions that became influential for future strategies.

However, the Obama administration's concern about escalation and the role of the DoD in securing an open and interoperable Internet shifted dramatically in 2018 during the Trump administration. Unlike the Obama administration, Trump administration senior leaders questioned assumptions about cyber escalation, norm propagation, and the effectiveness of deterrence. Shifts in these beliefs led to new roles for the DoD in cyberspace. Below, we examine the origin and nature of these ideas through the lens of three defense cyber strategies.

2011: A strategy of optimism and ambiguity

The Defense Department promulgated its first cyber strategy in July 2011, more than a year after the creation of Cyber Command, then a sub-unified combatant command under US Strategic Command [12]. The 2011 DoD cyber strategy came on the heels of the Obama administration's International Cyberspace Strategy, which expressed optimism about the implications of cyberspace and the Internet for human rights, democracy promotion, and economic opportunity. This view was reinforced by the Arab Spring and the perception that social media was a critical enabler of democratic forces [13]. Accordingly, the White House strategy defined its end state as a free, open, interoperable, reliable, and secure cyberspace—something it articulated as a universally perceived good. The primary means to achieve these ends were through non-military instruments of power, particularly diplomacy, international cooperation, and norms promotion, which were seen as equally if not more important than law enforcement and military capabilities. These ideas about cyberspace shaped how, over the next 5 years, the Obama administration defined the cyber roles and responsibilities of the Federal government's departments and agencies.

From a Defense Department perspective, the White House cyber strategy did not place a significant emphasis on the military as an instrument of power. It merely called for the DoD to "recognize and adapt to the military's increasing need for reliable and secure networks, build and enhance existing military alliances, and to expand cyberspace cooperation [13]." While the strategy did include deterrence concepts, it emphasized denial-based approaches such as improving cyber defense and resilience. When the strategy did reference punishment, it emphasized the importance of proportionality and sought to limit the application of military power as much as possible. The strategy promised the Defense Department would "exhaust all options before military force whenever we can; we will carefully weigh the costs and risks of action and of inaction; and will act in a way that reflects our values and strengthens our legitimacy and international support whenever possible [13]."

Accordingly, the DoD's first attempt at promulgating a cyber strategy in 2011 reflected the Obama administration's uncertainty and wariness about the role of the military in a domain seen largely as full of promise for governance and societies. As such, the first DoD cyber strategy served more as a declaration that cyberspace "mattered" for defense than an articulation of priorities, threats, or lines of effort. Specifically, the strategy identified five strategic initiatives: organize the Defense Department to "take full advantage of cyberspace's potential"; protect the DoD's networks and systems; partner with other elements in the Federal government and private sector; strengthen collective cybersecurity internationally with allies and partners; and build an effective workforce and enable innovation [14].

Notably absent from the first DoD cyber strategy was any meaningful discussion of the application of military power in and through cyberspace. The 2011 strategy did not explicitly name adversaries and was as much concerned with non-state actors and insider threats as any one particular nation-state. The strategy was also vague about how the US military intended to combat threats emanating from cyberspace, which reflected broader uncertainty about the role the military should play in cyberspace as well as the DoD's relationships with other federal agencies in combating cyber threats. Nevertheless, the document foreshadowed some continuity across US cyber strategies over the ensuing decade, including a clear prioritization of "protecting and respecting the principles of privacy and civil liberties, free expression, and innovation," while mitigating the vulnerabilities of the Defense Department's reliance on digital technologies [14].

2015: A dose of cyber reality

Following the 2011 strategies, there was a significant increase in the magnitude, severity, and targets of cyber incidents affecting US national security and defense interests. Chinese cyber espionage and intellectual property theft skyrocketed, including a multi-year campaign conducted by APT10 (linked to China's Ministry of State Security) to steal data from over 100 000 US Navy personnel, the 2014 Cloud Hopper campaign, and the 2014 Office of Personnel Management breach [15]. Meanwhile, Iran executed a series of nuisance but concerning cyber operations, including penetrating a dam in upstate New York, conducting disruptive cyber attacks against the US financial sector in 2011–2013, and launching a destructive attack against Sands Casino in 2014 [16, 17]. All these efforts seemed to come to a head publicly with North Korea's 2014 attack against Sony Pictures [18]. Together, these incidents forced the Obama administration to publicly revise its early optimism about cyberspace. Compared to 2011, when the USA was arguably one of the most proficient and capable actors in cyberspace, by 2015, the cyber threat landscape was full of capable and willing cyber actors—many targeting the USA.

Nevertheless, the administration largely avoided turning to the military to address these growing threats. For the Obama administration, uncertainty had only increased in the 4 years since the 2011 strategies, leaving the administration even more concerned about escalation and determined to contain the role of military power in cyberspace [19, 20]. As former Secretary of Defense Chuck Hagel asserted in 2014, the Pentagon "will maintain an approach of restraint to any cyber operations outside the US Government networks. We are urging other nations to do the same [21]." A critical implication for the military was to focus on deterring cyber attacks by credibly conveying a military readiness to respond, rather than taking preemptive or preventive action. This would support the restraint norms the administration was leading through traditional diplomatic institutions, such as the United Nations' Group of Governmental Experts and other fora, such as the G7 and G20, the Organization for Security and Cooperation in Europe, and the Organization of American States [22].

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

The 2015 DoD cyber strategy, therefore, reflected tension between the Obama administration's appreciation of the growing cyber threat environment, on one hand, with a lingering circumspection about the military's ability to address those threats without risking escalation [23]. Unlike the 2011 strategy, the 2015 strategy explicitly identified priority adversaries: Russia, China, Iran, North Korea, and non-state actors. It also defined five strategic goals: build and maintain ready forces to conduct cyberspace operations; defend the DoD's information network, data, and missions; be prepared to defend the US homeland; build and maintain viable cyber options to control conflict and escalation; and develop alliances to deter threats and promote stability [24]. These goals reflected a strategy more focused on cyber threats than the optimistic vision enshrined in the 2011 strategy. To grapple with these threats, the 2015 strategy leaned heavily on a deterrence posture: holding the military's cyber force in reserve while ostensibly developing capabilities to retaliate. The Obama administration also implemented significant oversight and control over military cyber operations, including computer network exploitation. As former National Security Council advisor on cyberspace Michael Daniel recalled, "We have very clear rules in the physical world that we don't have in cyberspace yet." He noted that this, "lack of clarity is part of the problem…and why there's an argument for being careful about and having oversight over offensive cyber operations [25]."

2018: A more assertive approach

This period of relative restraint shifted to a decidedly more risk acceptant posture during the Trump administration. An important inflection point was Russia's cyber-enabled information operations in the 2016 US Presidential election, which prompted heated debates within the Obama administration about how aggressively to respond, including through cyber means. Media reports indicate that the administration considered, but rejected, offensive cyber operations in the summer of 2016 in part due to concerns about triggering further Russian aggression [26]. Reportedly, one of the more forceful cyber options the administration considered was to take down websites hosting leaked information, conduct disruptive cyber attacks against Russian media, and disrupt command and control infrastructure used by Russian intelligence organizations [27]. Instead, the response was limited to diplomatic, economic, and law enforcement measures.

This prompted a push from some elements in the private sector and Defense Department to question previous assumptions about escalation and call for a more forward-leaning strategy. Two critical documents reflected this evolution of ideas. First, US Cyber Command released its Command Vision, anchored in the concept of "persistent engagement," which argued that Cyber Command should persistently engage adversaries in cyberspace, rather than wait to respond to deter cyber attacks. The 2018 Command Vision called for achieving "cyber superiority" through "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver…to create operational advantage for us while denying the same to our adversaries [28]." Shortly thereafter, the DoD released an unclassified summary of the 2018 cyber strategy, which articulated a "defend forward" concept to counter cyber threats beyond US networks and before attacks occurred [29].

Both of these documents professed new ideas about cyber escalation and the role of military power in creating tacit norms of restraint. Whereas the Obama administration had responded to uncertainty with hedging strategies (focused on diplomatic norms) and deterrence strategies (focused on defense, resilience, and the credible threat of retaliation), these new documents asserted more certainty about the purportedly minimal risks of day-to-day cyber operations as well as the lack of escalation to violence. As Nina Kollars and Jacquelyn Schneider noted in their comparison of the two strategies:

> The 2015 strategy strove to "mitigate risk" and "control escalation." In comparison, the 2018 strategy takes a much more active and risk-acceptant tone, pledging to "assertively defend our interests." This is because the document views the main risk to US objectives not as the use of cyber operations but, rather, "inaction: [as] our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day [30]."

This was also an important time period of expansion and growth for the DoD. In 2018, US Cyber Command was elevated to a unified combatant command and the CMF reached full operational capability. This institutional maturation reportedly occurred alongside the delegation of authority below the Presidential level to conduct offensive cyber operations [31]. Subsequently, Cyber Command defined election defense as a priority mission and, together with the National Security Agency and other partners across the Federal government, formed the Russia Small Group to defend the 2018 and 2020 elections. Reportedly, these efforts included limited counter-cyber operations to disrupt groups like the Internet Research Agency from conducting election interference [32–34]. Additionally, Cyber Command partnered with allies, such as Estonia and Montenegro, through its "hunt forward" mission to proactively search for cyber threats in allied-controlled networks [35, 36]. It also leaned forward to support the private sector. It conducted "malware inoculation" through information sharing, including indicators of compromise, malware hashes, and other technical artefacts, in public venues such as VirusTotal [37]. Together with interagency partners, it formed two pilot "Pathfinder" programs to collaborate with the financial services and energy sectors [38]. These pilot programs involved joint training and analysis and information-sharing across classification levels. Finally, Cyber Command began to play a role in combating cybercrime, with leadership acknowledging in 2021 that Cyber Command had conducted operations to "impose costs" against ransomware groups, in conjunction with the UK [39]. Taken together, these efforts reflect a far more assertive and active role for the military in cyberspace—a significant evolution from the perspective envisioned a decade prior.

Appraising defense cyber strategy

Each of these strategies advocates for different uses of the military, primarily through three beliefs: (1) how international norms are established; (2) the utility of deterrence in cyberspace; and (3) the escalation risks stemming from military cyber operations. What role do these ideas play in driving differences across these strategies? And what insight does cyber scholarship have in arbitrating these ideas? Below, we elaborate on these three questions, the results of which are summarized in Table 1.

Evaluating approaches to norms

Despite the prominence of norms across three defense cyber strategies, there are significant differences in how norms are understood within the three strategies. Obama-era strategies assumed that military action in cyberspace would erode cyber norms of restraint and therefore largely treated the DoD as a negative actor for norm propagation. This led to a focus on non-action, or deterrence, as the DoD's primary contribution to cyber norms. In contrast, the Trump administration was skeptical that diplomatic norms could change cyber behavior. Instead, it argued that focusing on military cyber power for

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

Table 1: Ideas about norms, deterrence, and escalation across three cyber strategies.

	2011 Strategy	2015 Strategy	2018 Strategy
Norms	Strong emphasis on international norms with a focus on democracy and human rights; DoD largely seen as a risk to stability norms	Additional emphasis placed on declaring DoD's restraint in operating consistent with international norms	DoD is seen as a norm entrepreneur in its own right, with norms established through military cyber operations; focus on a narrower set of norms
Deterrence	Deterrence is not clearly defined and is not a core concept	Deterrence is the anchoring concept; focus on denial and resilience; ambiguity about deterrence by punishment	Deterrence exists alongside if not underneath new strategic concepts, defend forward/persistent engagement
Escalation	Escalation is a significant concern; military cyber operations are seen as a source of risk	Escalation beliefs are consistent with the 2011 strategy	Escalation is not mentioned; military cyber operations can be contained below a threshold of conflict

deterrence would give rise to an implicit norm that would restrain US adversaries from cyber attacks by threatening a more persistent and engaged US military in cyberspace (as captured in the Cyber Command vision). However, both 2018 strategy documents stopped short of articulating the appropriate bounds of US military cyber action—an ambiguity that many argued inadvertently undermined the very international norms the US government sought to establish [40, 41]. All of these strategies, therefore, represent divergent ideas about how cyberspace norms are created and upheld. What does scholarship say about these assumptions?

It is helpful to begin with a baseline review of norms scholarship. Norms are "a collective expression for the proper behavior of actors with a given identity [42]." They rest on a shared sense of appropriateness [43]. Successful norms often follow a lifecycle [44]. Norm emergence, the first stage of the lifecycle, advents with norm entrepreneurs who shepherd the idea and attempt to convince others to adopt it. These norm entrepreneurs play a critical role in issue framing. Struggles over framing have long-term consequences because initial approaches tend to be sticky and difficult to dislodge. This can create a first-mover advantage in efforts to reframe norms or create new norms. Beyond framing, norm entrepreneurs often build organizational platforms from which they seek to promote and institutionalize norms [45]. Successful norm entrepreneurs create a "norm cascade" when the norm is adopted across a plurality of pertinent actors—a tipping or threshold point for norm adoption [45]. Some actors or states are so critical that a norm will not reach a tipping point without their endorsement [46]. Therefore, identifying these actors is essential for norms to develop through the full lifecycle. The most mature norms are finally internalized so that they are taken for granted as appropriate and natural behaviors.

While defense cyber strategies do not use the phrase "norm entrepreneur," debates within and across these strategies hinge on the unspoken assumption that the Defense Department is a type of norm entrepreneur. However, unresolved tensions about the role of military organizations in the norms lifecycle may have impeded US success as a cyber norm entrepreneur. On the one hand, some elements of the strategies conceptualized the DoD as a risk to cyber norms, particularly around stability and escalation. Others saw the DoD as a stakeholder in the reinforcement of norms, including non-military norms about Internet freedom and democratic values. A third view conceives of the DoD as tacitly creating norms through engaging with adversarial actors in cyberspace. These represent very different perspectives on how cyber norms emerge and spread—as well as their substantive content. Yet, they share a common conception of the military as an important player in that process.

Under the Obama administration, norms were propagated primarily through public strategy documents and speeches [47]. The DoD was expected to assist the propagation of these norms passively, principally by leading by example, "protecting and respecting the principles of privacy and civil liberties, free expression, and innovation [14]" and promising to "act in a way that reflects our values and strengthens our legitimacy [48]." The DoD conceptualized international norms as means to "increase stability and predictability of state conduct in cyberspace [48]." Through confidence-building measures and international norms promotion, the Department assessed that the USA would be able to "avoid escalation and misperception in cyberspace [48]." The DoD saw norms developing through formal processes grounded in international institutions and agreements [48]. It was therefore a secondary propagator of norms—mainly by upholding deterrence, which would create incentives for stability and openness.

DoD's role as a passive norm propagator continued into the 2015 strategy [24]. However, this strategy was more explicit in restraining the Defense Department to conform to the publicly disseminated norms. For instance, the strategy underscored that the department would "ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally [24]." Later in the document, the strategy further reiterated that the USA would "always conduct cyber operations under a doctrine of restraint….As in other domains of operations, in cyberspace, the Defense Department will always act in a way that reflects enduring US values, including support for the rule of law, as well as respect and protection of the freedom of expression and privacy, the free flow of information, commerce, and ideas [24]."

In contrast, the 2018 strategy presented a fundamentally different theory of how norms develop, propagate, and influence behavior. It repositioned the DoD's role in norm propagation from passive to active and introduced the DoD as a norm entrepreneur in its own right [29]. In particular, it tasked the Defense Department to lead two norms: "prohibitions against damaging civilian critical infrastructure during peacetime" and not "allowing national territory to be used for intentionally wrongful cyber activity [29]." This reflected a narrower, national security-focused approach to the DoD's conception of cyber norms, rather than a broader view encompassing democracy and human rights.

Additionally, the 2018 strategy and the 2018 Command Vision articulated a different theory for how the Defense Department could promote international norms. While previous focus was on mainstream diplomacy, the 2018 documents posited that states could "persistently engage" with each other in cyberspace, exchanging tit for tat responses without escalating to the level of "armed conflict" and, as part of this process, establish norms. In other words, norms were something that emerged endogenously and were clarified through military cyber operations. From Cyber Command's per-

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

spective, it was "[t]hrough persistent action and competing more effectively below the level of armed conflict, [that] we can…clarify the distinction between acceptable and unacceptable behavior [28]." As Michael Fischerkeller and Richard Harknett elaborated, the concept of persistent engagement relied on establishing acceptable forms of "agreed competition" between states in the cyber domain through the conduct of cyber operations, rather than through arriving at formal agreements. The central premise was that, through a process of "tacit bargaining" by way of grappling with one another in and through cyberspace, the USA and its adversaries could find consensus about acceptable behavior and develop an understanding of an "agreed battle" in which adversaries "can come to tacit understandings of constraints on their actions through repeated interactions [49, 50]." What followed from this logic was that what actors observed about each other's cyber conduct would constitute shared understandings about acceptable behavior—effectively, cyber norms—even though states may not formally agree to them or write them down.

Unanswered questions about the military and cyber norms

There were logical inconsistencies across all of these approaches. For example, Obama administration strategies focused on developing an Internet based on freedom and democratic values. The 2011 and 2015 strategies were concerned the Defense Department could undermine or threaten these norms. Therefore, the administration took pains to reiterate offensive cyber restraint and to build processes that signaled to adversaries (and allies) deliberation and proportionality in US cyber operations [51]. However, there was ambiguity in this restraint that may have undermined norm development. For instance, was the USA restraining itself in cyberspace because it was a responsible actor or because it did not have the capability (or will) to punish adversaries? Did the centralization of authority for military cyber operations represent a deliberate, rational policy choice or bureaucratic necessity?

On the other hand, the Trump administration's cyber strategy argued that military cyber operations reinforced, rather than undermined, cyber norms. It proposed that by defending forward and persistently engaging, the USA could solidify norms that scoped and delimited an "agreed" cyber battle. However, the administration's relative silence on norms that emphasized freedom and democratic values in cyberspace as well as its abdication of leadership within formal international bodies in favor of tacit norms built by the US military seemed to ignore a competing norm being propagated by US adversaries: the spread of non-democratic approaches to information technology [52]. Further, the focus on tacit efforts to create boundaries of agreed cyber battle did not provide clarity on mitigating the risks of cyber operations being misperceived, and contributed to perceptions of cyber hypocrisy, eroding US credibility as a norm entrepreneur [53]. In other words, it was unclear the words of the US government (the formal norms it publicly agreed to), matched its deeds in cyberspace [54].`

The ideational power of cyber deterrence

A second foundational idea for US defense cyber strategy is the role of deterrence. Public narratives suggested a significant shift from purely deterrence-based perspectives in 2011 and 2015 to one in 2018 that was skeptical of or even rejected deterrence. However, in reality, the strategies reveal a more complicated relationship with deterrence [55]. This echoed similar debates in academic circles about the feasibility of cyber deterrence and the applicability of deterrence by denial and punishment to cyberspace [56–63].

The 2011 defense cyber strategy hardly touched on deterrence concepts. The term "deterrence" appeared only a few times throughout the document and was used to refer to two distinct issues, neither of which was at the core of the overall strategy. The first, insider threats, bears little resemblance to what scholars understand as deterrence theory in an international relations context [14]. The second was about "collective deterrence" in the context of international cooperation and partnerships (though it provided few details about how exactly collective deterrence would be implemented [14]). Most importantly, deterrence did not function as an essential, overarching concept to guide the strategy. Instead, it was a small part of other lines of effort.

By 2015, however, deterrence became the crux of US defense cyber strategy. The strategy argued that the DoD "seeks to deter attacks and defend the United States against any adversary that seeks to harm US national interests during times of peace, crisis, or conflict [24]." Later, it specified the targets and aims of deterrence: "to deter key state and non-state actors from conducting cyberattacks against US interests [24]." Moreover, the strategy clearly linked the development of cyber capabilities and the conduct of cyber operations to deterrence [24]. A whole section of the strategy was devoted to deterrence through response, denial, and resilience [24].

What is most interesting is what is left unsaid: while the strategy did not preclude the use of military power to respond to cyber attacks, it refrained from employing the term of art, "deterrence by punishment" and avoided similar language often found in other defense strategies, such as "cost-imposition." This is a notable absence given that deterrence strategies are often associated with the logic of punishment [64]. Instead, the strategy devoted considerable energy to emphasizing the non-military response options at the US government's disposal, such as attribution, diplomacy, law enforcement, and economic sanctions—even for those cyber attacks that may "present a significant threat to US national security [24]." The omission of an explicit discussion about how military force fits into a cyber deterrence strategy is highly unusual for a defense strategy that, by its very nature, is focused on the military instrument of power.

While the 2018 strategy did represent a significant shift in the Defense Department's emphasis on cyber deterrence, there was more continuity than is typically depicted. The 2018 strategy did not reject deterrence outright. Indeed, it asserted the DoD will, "deter aggression, including cyber attacks that constitute a use of force" and, "preempt, defeat, or deter malicious cyber activity targeting US critical infrastructure [29]." A key difference, however, is that deterrence did not hold the central position in the 2018 strategy that it enjoyed in the 2015 strategy. Rather, deterrence was one strategic concept that existed alongside (and somewhat in tension with) other concepts, especially the Defense Department's new notion of "defend forward." Rather than simply being prepared to respond in the event of a cyber attack, the military would now be operating beyond its own networks to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict [29]."

While Cyber Command's 2018 command vision was a "vision statement," not technically a strategy document, it articulated how the command intended to implement the 2018 DoD strategy. The command vision obliquely referred to deterrence, noting that it would "deter aggression" and "contribute to national strategic deterrence [28]." However, the central figure of the vision was "persistent engagement," which was presented as an alternative to deterrence [65]. The command vision represented a "repudiation of the previous 7 years of cyberspace strategy [66]" and was a more strident rejection of cyber deterrence in a way that far exceeded the 2018 DoD strategy. Writing prior to the release of the command vision, "Deterrence is

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

Not a Credible Strategy for Cyberspace," Fischerkeller and Harknett previewed these ideas, arguing that, "within cyberspace, the protection or advancement of national interests cannot rest on deterrence as the central strategy"; instead, the authors advocated, "a strategy of cyber persistence [59, 67]." Offering a more nuanced approach, Emily Goldman and Michael Warner, civilian cyber experts at US Cyber Command, wrote in 2021 that deterrence and persistence concepts, while theoretically distinct, could exist simultaneously at different thresholds. In their view, deterrence had been effective at preventing decisive cyber attacks above the level of conflict while cyber persistence, which is, "designed for the conditions of the cyber strategic competitive space short of armed conflict," could work through "persistently disrupting" adversary cyber campaigns [68].

The tension between persistent engagement and deterrence was also manifest in public statements by senior military leaders. For instance, in a 2019 interview with *Joint Force Quarterly*, General Paul Nakasone, Commander of US Cyber Command, was asked about how Cyber Command could deter adversaries. He answered without any reference to deterrence and instead called for the USA to "*persistently engage* with that adversary…[and] impose cumulative costs [69]." Indeed, Nakasone did not mention deterrence once throughout the interview. Deterrence was similarly overlooked in Nakasone's 2020 *Foreign Affairs* article, coauthored with his then-advisor, Michael Sulmeyer [70]. And speaking in November 2021 at the Aspen Security Forum, Nakasone argued that deterrence "is a model that does not comport to cyberspace [71]."

Lingering cyber deterrence issues

While the debate within the cyber community about deterrence continues to churn, the broader concept remains the anchoring principle for defense strategy writ large. Indeed, the Biden administration doubled down on deterrence. It placed "integrated deterrence" (which it defines as, "developing and combining our strengths to maximum effect, by working seamlessly across warfighting domains, theaters, the spectrum of conflict, other instruments of US national power, and our unmatched network of Alliances and partnerships") at the center of its new National Defense Strategy (NDS) [72, 73], of which cyberspace is a key component [31, 74]. The problem is that the Defense Department has not yet expressed a clear and consistent vision for the role of deterrence in cyber strategies—let alone the role of cyberspace in broader deterrence strategies [75]. In particular, there are three areas where the DoD's ideas about cyber deterrence remain underspecified: the relationship between defend forward/persistent engagement and deterrence; the thresholds at and conditions under which cyber deterrence operates; and how the DoD communicates these approaches.

In April 2022 Congressional testimony, Nakasone—taking cues from the new NDS—testified that integrated deterrence was a top priority for Cyber Command. To square the circle between defend forward/persistent engagement and deterrence, Nakasone noted that, "supporting the national priority of Integrated Deterrence means preparing for crisis and conflict while campaigning in competition across the full spectrum of cyber operations [34]." This seemed to imply a status quo in which defend forward exists in parallel with deterrence, with the former encompassing cyber operations in "competition" and the latter entailing cyber operations to support crisis management, kinetic conflict, and full spectrum deterrence above the level of armed conflict.

While these approaches may (in theory) amicably exist in tandem, they suggest divergent implications for how the Defense Department should posture its forces, including the type, targeting, and scale of offensive cyber operations that the DoD should plan and conduct. For instance, deterrence requires gaining access to strategic targets and holding them at risk. Defend forward and persistent engagement, in contrast, largely involve conducting counter-cyber operations to disrupt adversary offensive cyber capabilities, shape the strategic environment, and glean information to share with partners to thwart ongoing or impending adversary malicious activity—all while keeping these operations below the level of conflict. The types of cyber operations suggested by defend forward/persistent engagement are, therefore, more tactical than the decisive, strategic employment of cyber power—precisely because the intent is to contain interactions below the level of war.

Deterring cyber attacks also suffers from the ambiguity between deterrence and persistent engagement because academic research suggests that deterring malicious cyber behavior writ large is both unrealistic and counterproductive [76]. One alternative, following the intent of the 2018 strategy, could be to focus on deterring specific actions or effects, such as disruptive or destructive cyber attacks against critical infrastructure and key functions. This would require reconciling the logical inconsistency between what the DoD thinks is unacceptable in cyberspace (and therefore aims to deter), and what the US views as its own cyber boundaries. Specifically, the USA has sought to deter adversaries from conducting cyber attacks against the homeland, going so far in the 2018 Nuclear Posture Review as to imply that the USA could respond to cyber attacks with nuclear retaliation [77]. However, it does not hold its own actions to the same threshold. In fact, an implication of the 2018 strategy is that most cyber attacks are below a threshold of armed conflict. This, in turn, justifies US conduct of cyber actions prior to conflict without anticipating retaliation. This ambiguity in language suggests that the USA might have different interpretations about what it believes it could do in cyberspace versus what its adversaries should do [78]. This tension has been brought into stark relief during the Ukraine conflict, where the USA has issued public statements warning against Russian retaliation against the West through cyber attacks—even implying that such actions could constitute justification for invoking Article 5, the collective defense clause of the NATO alliance [79]. At the same time, in response to comments by Nakasone at a May 2022 NATO conference in Estonia that the USA had conducted offensive cyber operations in support of Ukraine, the White House press secretary commented that these operations do not constitute a direct military attack against Russia [80, 81].

This analytical slippage also has secondary effects on deterrence credibility as it calls into question whether the USA is really willing to inflict punishment (up to nuclear weapons) in response to cyber attacks. This is compounded by the expansive way in which the USA has defined what it deems as "off limits" cyber targets for adversaries. If everything is important, then nothing is important. Absent an understanding of what the USA cares about in cyberspace, ambiguous cyber deterrence has been unable to stem the increasingly prolific and sophisticated wave of cyber operations against the USA.

How dangerous is cyberspace? Competing ideas on escalation

A third unresolved issue in US defense cyber strategies is the extent to which cyberspace is a dangerous domain prone to escalation and, by extension, the risks associated with a more assertive operational posture. As described above, the Obama administration's defense strategies were grounded in an explicit concern about the escalatory implications of offensive cyber operations. This led the administration to articulate a restraint-based approach and limit the conditions under which military cyber power would be employed. In stark con-

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

trast, the 2018 strategy documents do not even mention the concept of escalation—an omission that speaks volumes [82, 83, 34]. Additionally, proponents of persistent engagement, such as Fischerkeller and Harknett, argued that military cyber forces could conduct offensive operations without incurring undue risks of escalation [84]. Fischerkeller and Harknett's claims parallel the argument by Goldman that persistent engagement is not an escalatory approach but, rather, represents a response to adversary malicious cyber activity. Moreover, Goldman describes the approach as "assertive and proactive," rather than, "aggressive or offensive," and notes that, "[w]e have demonstrated that we can preclude and disrupt cyber aggression without escalating to armed conflict [85]."

But while Cyber Command argued cyber operations were not escalatory, official comments about US cyber strategy sometimes seemed to imply that US escalation was intentional. Then National Security Advisor John Bolton warned that "[w]e're now going to do a lot of things offensively and I think our adversaries need to know this [86, 87]." Similarly, Nakasone testified "[n]o longer are we going to be on the sidelines [88]." These comments contributed to speculation about how "offensive" defend forward was in practice, including reports from mainstream news venues that suggested the USA was placing malware exploits in Russian critical infrastructure or that the military had been given a blank check to operate in cyberspace [89, 90]. Faced with ambiguity about how far "forward" the USA was "defending," some critics were worried that these new strategic concepts could inadvertently lead to retaliation, potentially violent [91]. The DoD's new approach also caused some consternation among some US allies, which held different perspectives on the definition of sovereignty in cyberspace and voiced concerns about the extent to which US cyber forces could be maneuvering in and through their networks [92].

Unresolved escalation concerns

Academic research on escalation increasingly suggests the Obama administration's escalation concerns may have been overblown. Through statistical analysis, case studies, experimental surveys, and wargames, researchers have consistently found little empirical support to the idea that cyberspace is *highly* escalatory. Instead, cyber actions are typically met with proportionate, tit-for-tat responses, either in cyberspace or through non-military instruments of power [93]. Moreover, in more than 4 years since defend forward debuted, there is little evidence the strategy led to escalation. In the current Ukraine–Russia conflict, cyber operations have notably not contributed to escalation. In fact, Erica Lonergan and Shawn Lonergan suggest cyber operations may help defuse crises by giving states an additional, non-violent means of signaling [94]. Similarly, Benjamin Jensen and Brandon Valeriano argue that "[C]ountries have different ways of responding to crises when cyber options are available [95]."

Finally, there is the question of how cyber operations could increase the risk of inadvertent nuclear conflict [96]. For example, if during a crisis or conflict, a target state discerns a cyber intrusion or attack, it may take measures to raise nuclear alerts, disperse nuclear forces, pre-delegate launch authorities, or otherwise take measures to increase nuclear readiness in a way that creates greater opportunities for nuclear escalation, even if not intentional [97, 98]. Alternatively, different perspectives across military and civilian leaders on the utility of cyber operations for signaling purposes during nuclear crises may inadvertently increase instability [99]. Additionally, the "entanglement" of nuclear and non-nuclear capabilities for command and control, communications, intelligence, and surveillance and their vulnerability to cyber attack could create novel escalation risks [100].

Next steps for defense cyber strategy

Overall, the Defense Department has made significant strides throughout the past decade to organize around, prepare for, and combat cyber threats. But continuing to press ahead without rectifying some of the core issues endemic to past strategies risks, at best, strategic ineffectiveness or myopia and, at worst, failure. Below, we propose several steps for defense cyber strategy to address these gaps.

Lingering ambiguity about the extent of DoD's offensive cyber operations impacts the credibility of both norm promotion and deterrence. The DoD should be clear about what it views as appropriate behavior in cyberspace—both for itself and its adversaries [78]. This may mean narrowing the scope of the norms that the USA will prioritize for "enforcement" as well as restricting its own cyber operations. Additionally, future cyber strategies should decrease strategic ambiguity about what cyber attacks warrant a violent response from the USA. To date, the USA has not resorted to violence in response to cyber attacks, despite threatening up to nuclear response. Instead, the USA should focus on strategic deterrence of only the most significant cyber attacks. This is a high bar, but the USA may be able to credibly threaten cross-domain punishment for truly strategic cyber attacks: those that create significant effects against civilian populations, national security, the economy, or that threaten a state's nuclear command and control. At this level, which is only reserved for the most dangerous cyber operations, the USA could credibly threaten its vast and lethal military force and therefore shore up deterrence. At the same time, the USA should declare these cyber attacks off limits for itself. The adoption of a no-first-use cyber strategic attack policy, especially one buttressed by credible threats of retaliation across military options, could help signal credible US restraint and scope appropriate "status quo" cyber activity, thus shoring up both a strategic threshold of restraint and a lower threshold of status quo cyber activity that occurs without violent retaliation [78].

Future defense cyber strategies should also adopt clearer statements about what types of activities fall under the banner of defend forward. Ideally, defend forward would be scoped to include only counter-cyber operations against cyber adversaries, and not include civilian infrastructure. While defend forward may include offensive cyber activity, a clearer articulation what defend forward is targeting (and what it is not) would communicate assurance that the USA would not target civilian infrastructure preemptively.

Beyond clarifying the ideas discussed in prior strategies, future strategies should focus less on deterrence and norms and instead think more broadly about resilience, which features in the 2022 NDS (though its logic is not comprehensively articulated). A resilience approach assumes cyber defenses may occasionally fail and therefore frames strategic success as being able to anticipate, prepare for, withstand, recover, and learn from disruptive events [101]. Resilience requires not only investing in networks and technologies that are more technically resilient, but also in cultivating data users that are more resilient. For the DoD, this involves building networks that gracefully degrade and campaigns that can be executed in a denied or contested environment. To do this requires information sharing, collaboration with the private sector, investments in commercial technology, and Federal investment in research and development in cybersecurity.

Additionally, while this analysis has focused on the US defense cyber strategy, there are also implications beyond the USA. In many ways, the USA is unique in its promulgation of multiple defense cyber strategies—not to mention the maturity of its military cyber capabilities and organizations. However, other mature cyber powers, such as the UK, have increasingly adopted strategic approaches similar to the USA—which is not surprising given the concerted effort by US

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

policymakers to cultivate common understandings among allies and partners [102]. Therefore, as other states continue to develop military cyber capabilities and draw lessons from the USA's experience, they should be careful to learn from both the positive and more problematic elements of the past decade of US defense cyber strategy.

Author contributions

Erica Lonergan (Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Writing - original draft, Writing - review & editing), and Jacquelyn Schneider (Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Writing - original draft, Writing - review & editing).

References

1. Schneider J, Goldman E, Warner M. *Ten Years In: Implementing Strategic Approaches to Cyberspace*. Newport, RI: Newport Papers, 2020.
2. Branch J. What's in a name? Metaphors and cybersecurity. *Int Organ* 2021;**75**:39–70.
3. Haas PM. *Epistemic Communities, Constructivism, and International Environmental Politics*. New York, NY: Routledge, 2015.
4. Valeriano B, Jensen B. *Building a national cyber strategy: the process and implications of the cyberspace solarium commission report*. In: 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2021.
5. Walt S. US grand strategy after the cold war: can realism explain it? Should realism guide it? *Int Relat* 2018;**32**:3–22.
6. Gaddis JL. *On Grand Strategy*. New York, NY: Penguin, 2019.
7. Dueck C. Realism, culture and grand strategy: explaining America's peculiar path to world power. *Secur Stud* 2005;**14**:195–231.
8. Rosecrance RN, Stein AA. *The Domestic Bases of Grand Strategy*. Ithaca, NY: Cornell University Press, 1993.
9. Goldstein J, Koehane R (ed). *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*. Ithaca, NY: Cornell University Press, 1993.
10. Reich S, Domrowski P. *The End of Grand Strategy: US Maritime Operations in the Twenty-First Century*. Ithaca, NY: Cornell University Press, 2018.
11. Porter P. Why America's grand strategy has not changed: power, habit, and the US foreign policy establishment. *Int Secur* 2018;**42**:9–46.
12. U.S. Cyber Command. *Our history*. https://www.cybercom.mil/About/History/ (6 March 2023, last accessed).
13. *International Strategy for Cyberspace: prosperity, security, and openness in a networked world*. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (6 March 2023, last accessed).
14. *Department of Defense strategy for operating in cyberspace*. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (6 March 2023, last accessed).
15. *For a discussion of notable cyber threats and incidents, see United States of America Cyberspace Solarium Commission*. https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf (6 March 2023, last accessed).
16. Volz D, Finkle J. *U.S. indicts Iranians for hacking dozens of banks, New York dam. Reuters*. https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF (6 March 2023, last accessed).
17. Brandom R. *Iran hacked the Sands Hotel earlier this year, causing over $40 million in damage. Bloomberg Businessweek*. https://www.theverge.com/2014/12/11/7376249/iran-hacked-sands-hotel-in-february-cyberwar-adelson-israel (6 March 2023, last accessed).
18. The U.S. Department of Justice. *North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions*. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (6 March 2023, last accessed).
19. Kaminska M. Restraint under conditions of uncertainty: why the United States tolerates cyberattacks. *J Cybersecur* 2012;**7**:1–15.
20. Macdonald J, Schneider J. Presidential risk orientation and force employment decisions: the case of unmanned weaponry. *J Conflict Resolut* 2017;**61**:511–36.
21. Alexander D. *Hagel, ahead of China trip, urges military restraint in cyberspace. Reuters*. https://www.reuters.com/article/uk-usa-defense-cybersecurity/hagel-ahead-of-china-trip-urges-military-restraint-in-cyberspace-idUKBREA2R1YN20140331 (6 March 2023, last accessed).
22. *For a comprehensive review of international cyber norms, see Cyber Norms Index and Timeline. Carnegie Endowment for International Peace*. https://carnegieendowment.org/publications/interactive/cybernorms (6 March 2023, last accessed).
23. Assuming reporting about the U.S. role in the Stuxnet cyber attacks is accurate, this reflects an unresolved tension between the Obama administration's view that, on the one hand, covert offensive cyber operations to sabotage adversary critical infrastructure is acceptable, while on the other hand, the application of military power in and through cyberspace is dangerous and escalatory.
24. *The DOD Cyber Strategy*. https://www.hsdl.org/c/view?docid=764848 (6 March 2023, last accessed).
25. Smalley S. *Biden administration is studying whether to scale back Trump-era cyber authorities at DoD. Cyberscoop*. https://www.cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/ (6 March 2023, last accessed).
26. Miller G, Nakashima E, Entous A. *Obama's secret struggle to punish Russia for Putin's election assault. The Washington Post*. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/ (6 March 2023, last accessed).
27. Isikoff M, Corn D. *"Stand down": How the Obama team blew the response to Russian meddling. HuffPost*. https://www.huffpost.com/entry/stand-down-how-the-obama-team-blew-the-response-to-russian-meddling_n_5aa29a97e4b086698a9d1112 (6 March 2023, last accessed).
28. Achieve and maintain cyberspace superiority: command vision for US Cyber Command. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf (6 March 2023, last accessed).
29. Summary: Department of Defense Cyber Strategy 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (6 March 2023, last accessed).
30. Kollars N, Schneider J. *Defending Forward: the 2018 Cyber Strategy is here. War on the Rocks*. https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ (6 March 2023, last accessed).
31. Lonergan E, Schneider J. *Cyber challenges for the new National Defense Strategy. War on the Rocks*. https://warontherocks.com/2021/12/cyber-challenges-for-the-new-national-defense-strategy/ (6 March 2023, last accessed).
32. Nakashima E. *U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. The Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (6 March 2023, last accessed).
33. Vavra S. *NSA's Russian cyberthreat task force is now permanent. CyberScoop*. https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/ (6 March 2023, last accessed).
34. *Posture statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the 117th Congress*, Senate Committee on Armed Services. https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf (6 March 2023, last accessed).
35. U.S. Cyber Command. *Hunt Forward Estonia: Estonia, US strengthen partnership in cyber domain with joint operation*. https:

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

//www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/ (6 March 2023, last accessed).
36. U.S. Cyber Command. *US, Montenegro work together to defend against malicious cyber actors*. https://www.cybercom.mil/Media/News/News-Display/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/ (6 March 2023, last accessed).
37. U.S. Cyber Command. *U.S. Cyber Command's malware inoculation: linking offense and defense in cyberspace*. https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace#:~:text=Malware%20inoculation%20reduces%20the%20attack,simply%20through%20sharing%20useful%20information (6 March 2023, last accessed).
38. Vergun D. *Cyber strategy protects critical U.S. infrastructure*. https://www.defense.gov/News/News-Stories/Article/Article/1954009/cyber-strategy-protects-critical-us-infrastructure/ (6 March 2023, last accessed).
39. Barnes JE. *U.S. military has acted against ransomware groups, General acknowledges*. *The New York Times*. https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html (6 March 2023, last accessed). Although it is important to note that this took place during the Biden administration.
40. Healey J. The implications of persistent (and permanent) engagement in cyberspace. *J Cybersecur* 2019;**5**:1–15.
41. Rovner J. *More aggressive and less ambitious: Cyber Command's evolving approach*. *War on the Rocks*. https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/ (6 March 2023, last accessed).
42. Katzenstein PJ (ed). *The Culture of National Security: Norms and Identity in World Politics*. New York, NY: Columbia University Press, 1996.
43. Finnemore M. *Cybersecurity and the concept of norms*. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870 (6 March 2023, last accessed).
44. Of course, not all norms complete the lifecycle, but some norms and norm entrepreneurs are more likely to succeed. Research has found that the norms that are most likely to be adopted are those that display the following three characteristics: specificity (clarify a definition); durability (length of time the norms have been in effect); and concordance (extent of acceptance).
45. Finnemore M, Sikkink K. International norm dynamics and political change. *Int Organ* 1998;**52**:887–917.
46. Legro JW. Which norms matter? Revisiting the "failure" of internationalism. *Int Organ* 1997;**51**:31–63.
47. Kerry J. *An open and secure Internet: we must have both*. *U.S. Department of State*. https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm (6 March 2023, last accessed). These norms, which represent US beliefs, were developed to influence international norms which are perhaps best codified by the agreements generated by the United Nation's group of general experts on cyberspace. Some of these norms, for example a norm of restraint against critical infrastructure, are aligning more closely with UN GGE shared agreements but may not have become so prominent or upheld to be considered universally accepted.
48. Department of Defense Cyberspace. *Policy report: a report to Congress pursuant to the National Defense Authorization Act for fiscal year 2011, Section 934*. https://irp.fas.org/eprint/dod-cyber.pdf (6 March 2023, last accessed).
49. Fischerkeller MP, Harknett RJ. *What is agreed competition in cyberspace? Lawfare*. https://www.lawfareblog.com/what-agreed-competition-cyberspace#:~:text=Agreed%20competition%20is%20a%20unique,space%20short%20of%20armed%20conflict (6 March 2023, last accessed).
50. Fischerkeller MP, Harknett RJ. *Persistent engagement and tacit bargaining: a path toward constructing norms in cyberspace*. *Lawfare*. https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace (6 March 2023, last accessed).
51. Goldsmith J, Wu T. Who controls the Internet? Illusions of a Borderless World. New York, NY: Oxford University Press, 2006, 238.
52. This is often referred to as "digital authoritarianism." See, for example, Dragu T, Lupu Y. Digital Authoritarianism and the future of human rights. *Int Organ* 2021;**75**:991–1017.
53. Finnemore M, Hollis DB. Constructing norms for global cybersecurity. *Am J Int Law* 2016;**110**:425–79.
54. Group of Governmental Experts on advancing responsible state behavior in cyberspace in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf (6 March 2023, last accessed).
55. This is the case even for how Cyber Command frames its vision. See, for example, Nakasone, PM. A cyber force for persistence operations. *Joint Force Q* 2019;**92**:10–14. Nakasone describes how Cyber Command is, "Shifting from a response outlook to a persistence force that defends forward," and reiterates that, "We have shifted away from the earlier emphasis on holding targets 'at risk' for operations at a time and place of our choosing."
56. Libicki M. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
57. Rattray G. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press, 2001.
58. Nye Jr. JS. Deterrence and dissuasion in cyberspace. *Int Secur* 2017;**41**:44–71.
59. Fischerkeller MP, Harknett RJ. Deterrence is not a credible strategy for cyberspace. *Orbis* 2017;**61**:381–93.
60. Brantley AF. The cyber deterrence problem. In: *10th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2018.
61. Schneider JG. Deterrence in and through cyberspace. In: Gartzke E, Lindsay JR (ed). *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York, NY: Oxford University Press, 2019, 384.
62. Denning DE. Rethinking the cyber domain and deterrence. *Joint Force Q* 2015;**77**:8–15.
63. Borghard ED, Lonergan SW. Deterrence by denial in cyberspace. *J Strateg Stud* 2021. doi:10.1080/01402390.2021.1944856.
64. Art RJ. To what ends military power? *Int Secur* 1980;**4**:3–35.
65. Nakasone PM, Sulmeyer M. *How to compete in cyberspace: Cyber Command's new approach*. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity (6 March 2023, last accessed).
66. Schneider JG. *Persistent engagement: foundation, evolution and evaluation of a strategy*. *Lawfare*. https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (6 March 2023, last accessed).
67. Fischerkeller M. *The fait accompli and persistent engagement in cyberspace*. *War on the Rocks*. https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/ (6 March 2023, last accessed).
68. Goldman EO, Warner M. The military instrument in cyber strategy. *SAIS Rev Int Aff* 2021;**41**:56.
69. Nakasone PM. An interview with Paul M. Nakasone. *Joint Force Q* 2019;**92**:5.
70. *Preparing the next phase of US cyber strategy*. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/preparing-the-next-phase-of-us-cyber-strategy/ (6 March 2023, last accessed).
71. Williams BD. *Nakasone: cold war-style deterrence "does not comport to cyberspace"*. *Breaking Defense*. https://breakingdefense.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/ (6 March 2023, last accessed).
72. U.S. Department of Defense. *Fact sheet: 2022 National Defense Strategy*. https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF(6 March 2023, last accessed).
73. U.S. Department of Defense. *2022 National Defense strategy of the United States of America*. https://media.defense.gov/2022/Oct/27/2003

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023

103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF (6 March 2023, last accessed).
74. Lopez CT. *Defense Secretary says "integrated deterrence" is cornerstone of U.S. defense*. *DoD News*. https://www.defense.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/ (6 March 2023, last accessed).
75. Lonergan E, Montgomery M. What is the future of cyber deterrence. *SAIS Rev Int Aff* 2021;**41**:61–73.
76. Valeriano B, Jensen B, Maness RC. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York, NY: Oxford University Press, 2018.
77. Nuclear posture review. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF (6 March 2023, last accessed).
78. Schneider J. A strategic cyber no-first-use policy? Addressing the U.S. cyber strategy problem. *Washington Q* 2020;**43**:159–75.
79. Lonergan ED, Moller SB. *NATO's credibility is on the line with its cyber defense pledge. That's a bad idea*. *Politico*. https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829 (6 March 2023, last accessed).
80. Martin A. *US military hackers conducting offensive operations in support of Ukraine, says Head of Cyber Command*. *Sky News*. https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (6 March 2023, last accessed).
81. Hunnicutt T, Holland S. *White House: cyber activity not against Russia policy*. *Reuters*. https://www.reuters.com/world/white-house-cyber-activity-not-against-russia-policy-2022-06-01/ (6 March 2023, last accessed).
82. Pomerleau M. *Here's how Cyber Command is using "defend forward"*. *C4ISRNET*. https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/ (6 March 2023, last accessed).
83. Smalley S. *Nakasone says Cyber Command did nine "hunt forward" ops last year, including Ukraine*. *CyberScoop*. https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/ (6 March 2023, last accessed).
84. Fischerkeller MP, Harknett RJ. Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *Cyber Defense Rev* 2019;**273**:267–287.
85. Goldman EO. Paradigm change requires persistence—a difficult lesson to learn. *Cyber Defense Rev* 2020;**4**:115–6.
86. Liptak K. *John Bolton: US is going on the offensive against cyberattacks*. *CNN*. https://www.cnn.com/2018/09/20/politics/us-cybersecurity-strategy-offense-john-bolton/index.html (6 March 2023, last accessed).
87. Lyngaas S. *White House announces federal cyber strategy, vows to go on offensive*. *CyberScoop*. https://www.cyberscoop.com/white-house-cyber-strategy-john-bolton-announcement/ (6 March 2023, last accessed).
88. Dilanian K. *Under Trump, U.S. military ramps up cyber offensive against other countries*. *NBC News*. https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281 (6 March 2023, last accessed).
89. Sanger DE, Perlroth N. *U.S. escalates online attacks on Russia's power grid*. *The New York Times*. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?module=inline (6 March 2023, last accessed).
90. Nakashima E. *Trump gives the military more latitude to use offensive cyber tools against adversaries*. *The Washington Post*. https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html (6 March 2023, last accessed).
91. Healey J, Jervis R. The escalation inversion and other oddities of situational cyber stability. *Texas Natl Secur Rev* 2020;**3**:30–53.
92. Smeets M. U.S. cyber strategy of persistent engagement and defend forward: implications for the alliance and intelligence collection. *Intell Natl Sec* 2020;**35**:444–53.
93. Lonergan ED. *The cyber-escalation fallacy: what the war in Ukraine reveals about state-based hacking*. *Foreign Affairs*. https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy. https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971 (6 March 2023, last accessed).
94. Lonergan ED, Lonergan SW. Cyber operations, accommodative signaling, and the de-escalation of international crises. *Secur Stud* 2022;**31**:32–64.
95. *What do we know about cyber escalation*. *Atlantic Council*. https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf (6 March 2023, last accessed).
96. Lin H. *Cyber Threats and Nuclear Weapons*. Stanford, CA: Stanford University Press, 2021.
97. Schneider J. *The biggest risk in ukraine? How Russian hacking could threaten nuclear stability*. *Foreign Affairs*. https://www.foreignaffairs.com/articles/ukraine/2022-03-07/biggest-cyber-risk-ukraine (6 March 2023, last accessed).
98. Schneider J, Schechter B, Shaffer R. Hacking nuclear stability. *Int Organ Forthcoming*. 2017;**3**:43–4.
99. Lonergan E, Yarhi-Milo K. *Cyber signaling and nuclear deterrence: implications for the Ukraine crisis*. *War on the Rocks*. https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/ (6 March 2023, last accessed).
100. Acton JM. Escalation through entanglement: how the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. *Int Secur* 2018;**43**:56–99.
101. Borghard ED. *A grand strategy based on resilience*. *War on the Rocks*. https://warontherocks.com/2021/01/a-grand-strategy-based-on-resilience/ (6 March 2023, last accessed).
102. *See, for example, National Cyber Strategy 2022*. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#:~:text=The%20new%20National%20Cyber%20Strategy,promote%20our%20interests%20in%20cyberspace (6 March 2023, last accessed).

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988 by guest on 21 September 2023