Deterrence is Not a Credible Strategy for Cyberspace

May 18, 2017

By Michael P. Fischerkeller and Richard J. Harknett

Michael P. Fischerkeller is a research staff member in the Information, Technology and Systems Division at the Institute for Defense Analyses, where he has spent nearly 20 years supporting the Office of the Secretary of Defense, Joint Chiefs of Staff, and Combatant and Multi-National Force commanders. **Richard J. Harknett** is US-UK Fulbright Professor of Cyber Studies at Oxford University, UK, and former Scholar-in-Residence, US Cyber Command and National Security Agency in 2016. He serves as Department Head of Political Science at the University of Cincinnati. The views expressed here are the authors alone.

Abstract: *U.S. national cybersecurity strategy, to be effective must align with the structural features and operational characteristics of the domain. Yet, this article contends that the current U.S. strategy of deterrence, coupled with the establishment of norms in cyberspace, does not satisfy this requirement. Alternatively, a strategy of cyber persistence is proposed, one that is enabled rather than crippled by the uniqueness of cyberspace. In an environment of constant contact, a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behavior and sustaining and advancing U.S. national interests.*

In 2010, the U.S. Defense Deputy Secretary William J. Lynn wrote an article outlining a new strategy for a new operating domain—a strategy for cyberspace.[1] Consistent with most U.S. defense policy over the past 20 years, the strategy was grounded in a deterrence framework and, consequently, the domain was considered one of restraint and reaction.[2] Yet, the cyber aggression we have witnessed in, through, and from cyberspace since that article was written calls into question the appropriateness of this strategic approach.[3]

[1] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Sept./Oct. 2010.
[2] The deterrence policy for cyberspace that informed this strategy is described in detail in a 2015 White House Report on Cyber Deterrence Policy (to Congress), http://1yxsm73j7aop3quc9y5ifaw3-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf
[3] The phrase "in, through and from" is indicative of the unique operational character of cyberspace and refers, respectively, to operations that originate in and result in effects in cyberspace; operations that originate outside of cyberspace, leverage cyberspace (via transit), and result in effects outside of cyberspace; and operations that originate in cyberspace and result in effects outside of cyberspace.

doi: 10.1016/j.orbis.2017.05.003

This essay makes two central arguments: first, within cyberspace the protection or advancement of national interests cannot rest on deterrence as the central strategy. Rather, the United States needs a strategy that capitalizes on the unique characteristics of the domain—a strategy of cyber persistence. And second, if the United States is to shape the development of international cyberspace norms, it can do so only through active cyber operations that begin to shape the parameters of acceptable behavior. U.S. national security, advancement of interests, and the development of international norms require persistent cyber engagement, not operational restraint, in an environment of constant activity. Counterintuitively perhaps, a doctrine of active mitigation may be less escalatory than one of restraint.

The Uniqueness of Cyberspace

The cyberspace operational domain is defined as a global domain within the information environment comprising the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[4] Thus, some experts argue that cyberspace is human-constructed and malleable. Moreover, the scope of this constantly shifting space is distinctive—state and non-state actors' abilities to modify other operational domains cannot occur on the scale we are witnessing in cyberspace. Strategy must recognize that there is a qualitative difference between the capacity to modify terrain and the ability to create it whole cloth.

The uniqueness of cyberspace is also reflected in the low cost of entry to this domain. Various actors can affect relative national power to operate in cyberspace that are orders of magnitude higher than the narrow club of great powers that operate with consequence in the land, air, maritime and space operational domains. Moreover, there is currently no internationally agreed upon concept of cyberspace sovereignty. This fact suggests a corollary—international relations (and nature) abhor vacuums. Consequently, cyber security strategy should assume that states and other significant actors continually are seeking to exert their influence in cyberspace through cyber operations, activities, and actions (OAAs). In addition, it is a domain in which all other operational domains and national instruments of power are enabled (if not dependent). And, given cyberspace's interconnected nature, operations always involve contact, whether it is recognized or not. Furthermore, operations in cyberspace are unique because operators can manage attribution and design operations to generate a range of damage—reversible, temporary, or significant that is, nonetheless, short of internationally agreed upon definitions of use of force and armed attack.

These characteristics should be appreciated in developing a strategy for cyberspace. Unfortunately, most of these characteristics are not considered when applying to cyberspace the strategic approach that has dominated U.S. policy—deterrence.

[4] "Cyberspace Operations," Joint Publication 3-12(R), Department of Defense, Feb. 5, 2013.

One of These Things is Not Like the Other

Once the U.S. government recognized cyberspace as a domain, it needed to consider a framework to suggest norms of behavior for operating within it. The operational norms associated with the air, land, and maritime domains are derived fundamentally from the centuries-old concept of Westphalian sovereignty. This concept included respect for the principle of non-intervention and territorial integrity that marked the end of the Thirty Years' War.[5] Although specifics regarding these norms have evolved,[6] the basic principle is still widely accepted by state actors in the international system and is codified in the United Nations Charter article 2(4). Namely, "all members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state." Consistent with this language, it is assumed that norms of responsible behavior should default to a pattern of operational restraint.

The United States and its allies have advocated that the principle of relative operational restraint should anchor the efforts to develop and codify cyberspace norms. Unfortunately, many actors find that more aggressive cyber OAAs are advancing their interests. While these actors might be considered "unlike-minded,"[7] the sheer number and the effectiveness of their aggressive cyber OAAs suggest that many effective actors are rejecting the default to restraint.[8] Because norms first emerge through behaviors, and then mature through international discourse, the fact that there is disagreement about what constitutes acceptable behavior suggests that global norms are unlikely to be adopted in the near term. Global cyberspace norms of responsible behavior cannot take root if the universe of "like-minded" states is a small proportion of salient cyber actors.

A strategic approach to developing norms in cyberspace, based primarily on diplomacy, fails to consider the unique characteristics of cyberspace. For example, it is a global domain for which the low costs of entry allow a vast population of like-minded *and* unlike-minded actors to participate at various levels of agency. Therefore, any cyberspace policy should assume the continuous presence of actors who will operate in, through, and from cyberspace in order to exert influence. Analyses of behaviors in cyberspace over the past decade reveal that state and non-state actors have understood and leveraged the value of cyberspace and cyber OAAs to support their interests. Undoubtedly, these actors have recognized that when the time comes for international discourse regarding codification, those who operationally dominate the domain will be in the strongest position to argue for norms supporting their positions. While cyber OAAs vary significantly, it is

[5] The space domain is widely accepted as a global commons rather than a domain that is subject to the principles of sovereignty.

[6] For example, the width of territorial waters shifted from 3 to 12 miles over a period of two centuries.

[7] See "International Strategy for Cyberspace," The White House, May 2011, p. 9, for the strategy's specification of working with "like-minded" states to develop norms.

[8] See, "Cyber Strategy," Department of Defense, 2015, p. 6.

important to think through three categories discussed in academic analysis and policy circles—sabotage, espionage, and subversion.[9]

Sabotage is a deliberate attempt to weaken or destroy an economic or military system. Cyberspace examples of attributed and non-attributed sabotage include: Iranian cyber OAAs that targeted the U.S. financial sector; Russian cyber OAAs that targeted the Ukrainian power grid and pre-positioned BlackEnergy malware on other critical infrastructure; North Korean cyber OAAs that targeted Sony Pictures Entertainment; the employment of Stuxnet to degrade or destroy Iranian uranium enrichment centrifuges; the Wiper virus that permanently deleted data from Iranian oil ministry computers; and the code-based degradation or destruction of thousands of Saudi Aramco computer systems.

Espionage is defined as a deliberate attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information. Cyberspace examples include reported activities of the intrusion into—and subsequent exfiltration from—a U.S. contractor of thousands of files regarding the F-35 Joint Strike Fighter and the December 2014 data breach at the United States Office of Personnel Management.

Subversion is defined as a deliberate attempt to undermine the authority, integrity, and constitution of established authority or order. Cyberspace examples include: Russian cyber OAAs targeting Georgian government websites in 2008 and the coupling of cyber espionage against Democratic National Committee systems in 2016 with the subsequent exposure of data gathered from those operations and a similar case in the French presidential election of 2017.

Trend analyses and forecasts of these types of behaviors all tell the same story—their numbers are increasing and are expected to continue to do so, as will the sophistication of the cyber OAAs that support them.[10] Consequently, state and non-state actors seeking to establish responsible norms of behavior while simultaneously committing to doctrines of relative operational restraint have and will continue to accumulate a strategic deficit in cyberspace relative to "unlike-minded" actors. While replacing a doctrine of operational restraint with operational persistence is a necessary action for reducing this strategic deficit, it would not be a sufficient action. There is a more profound problem—the current strategy for cyberspace.

When air, land, and maritime operational domain restraint was normalized through international agreements, states were not so naïve as to expect that all actors would abide by such norms *in perpetuity*. And so, states developed new or leveraged existing capabilities to further deter actors from violating the status quo. The United

[9] The relationship between these three categories and cyberspace / cyber OOAs is detailed in Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies,* 35:1, 2012, pp. 5-32, http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf

[10] See, for example, *Emerging Cyber Threats Report 2016*, The Institute for Information Security and Privacy (Georgia Institute of Technology, 2015); Lee Rainie, Janna Anderson, and Jennifer Connolly, "Cyber Attacks Likely to Increase," http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase; and Jake Kambic, Kristine. Aurthor, Will Ellis, Tyler Jensen, Kyle Johansen, Brian Lee, Samuel Liles, "Crude Faux: An Analysis of Cyber Conflict in Oil and Gas Industries," Purdue University, 2013, https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf.

States adopted a similar strategic approach with the advent of cyberspace because it did not expect all state and non-state actors to embrace a call to establish responsible norms in cyberspace. In such cases, U.S. strategy under the Obama administration called for deterrence by denial and, should that fail, deterrence by cost imposition to punish the more egregious instigators.[11] Unfortunately, given the domain's unique characteristics, deterrence is not a credible strategy for cyberspace.

A Strategic Mismatch

The international environment is dynamic—all significant actors at all times are seeking, short of armed conflict, to shape it to support sustaining or advancing their interests. In Department of Defense (DoD) parlance, shaping OAAs broadly includes, but is not limited to, day-to-day research and development, capabilities development, force structure development, employment, sustainment, security relationships, and legal agreements. Shaping OAAs manifests in a global posture. In 2014 the U.S. Defense Deputy Secretary Robert Work described global posture as the deliberate apportionment and global positioning of forward-stationed and forward-deployed forces and the development of supporting global attack, global mobility and logistics, forcible entry, and command, control, communications, and intelligence forces that facilitate the rapid concentration of forces from all domains in time and space across transoceanic distances.[12]

U.S. global posture, in turn, is specifically and directly intended to generate strategic effects, including persuading a target not to consider a course of action (COA) that would threaten U.S. interests, persuading a target not to execute a COA that would threaten U.S. interests, and, persuading a target to consider and/or execute a COA that would support U.S. interests. Since the conclusion of World War II, shaping and global posture have continuously served as bedrocks that support various deterrence-based national strategies and doctrines.[13]

The well-understood strategic objective of deterrence is to influence an adversary's cost/benefit calculus so that it concludes that the costs of challenging the status quo outweigh the benefits. Further, it is a strategy based upon a threat of use of force with an operational objective of avoiding costly operational contact (i.e., the actual use of force). Challenges to the status quo can take many forms, of course, but the most obvious and oft-cited in studies of conventional deterrence success/failure are threats to (or incursions into) sovereign territory. As discussed earlier, the concept of state sovereignty and the explicit territorial boundaries associated with it facilitated the implementation of strategies of deterrence by allowing for the declaration of thresholds defined by internationally accepted land,

[11] "White House Report on Cyber Deterrence Policy."
[12] Deputy Secretary of Defense Robert Work, "A New Global Posture for a New Era," Council on Foreign Relations, Washington, D.C., Sept. 30, 2014, https://www.defense.gov/News/Speeches/Speech-View/Article/605614/a-new-global-posture-for-a-new-era/.
[13] For the most recent example, see, "The National Military Strategy of the United States of America," Joint Chiefs of Staff, June 2015.

air, and maritime boundaries that, if crossed, would lead to costly operational contact.[14] The current U.S. global posture supports this strategy through forward-deployed and pre-positioned capabilities near territorial thresholds in order to increase the credibility of a threat of use of force should they be crossed. However, with all due respect to the Deputy Secretary's comments, U.S. global posture does not extend to *all* domains. It is largely absent in cyberspace.

The absence of a posture in cyberspace may be because no concept of cyberspace sovereignty currently exists around which to define a posture. In other words, no territorial boundaries are recognized to reference as thresholds that should not be crossed. The absence of sovereignty in cyberspace puts into question the value of a strategy of deterrence, a strategy the effectiveness of which, in part, depends on the specification of such thresholds. An alternative, non-territorial-based cyberspace threshold has been discussed that, if crossed, would justify responses of armed attack, but that threshold is based on cyber OAAs that cause the damage equivalent to the *use of force*. Such damage is of a very different nature and not representative of the significant damage being caused by on-going espionage, sabotage, and subversion cyber OAAs and, consequently, does not shape this consequential adversarial behavior occurring regularly below the *use of force* threshold.

An additional weakness of a strategy of deterrence in cyberspace is revealed when aligning its operational objective against the character of operations in cyberspace. A strategy of deterrence seeks to avoid operational contact, whereas cyberspace participants are interconnected, and consequently, all operations in cyberspace *always* involve operational contact. Cyberspace is a perpetually contested space. Further, because cyberspace enables its operators to manage attribution, potential uncertainty regarding the source of an attack does not necessarily lead to obvious targets for punishment via cyber OAAs in support of deterrence by cost imposition. The tactical, operational, and strategic bases of deterrence do not align with the characteristics and dynamics of cyberspace.

Strategic frameworks must map to the realities of strategic environments; the reverse is not possible. Deterrence applied to cyberspace seeks the absence of unwanted activity in an environment of constant activity and, thus, is a comprehensive mismatch. This explains why the United States and other countries, relying on deterrence, are losing ground in this vital global space.

Consequences of Applying a Strategy of Deterrence in Cyberspace

The continuous increase in scale and sophistication of cyber OAAs is evidence of the weakness of a strategy of deterrence by denial in cyberspace.[15] There

[14] Patrick Franzese, "Sovereignty in Cyberspace: Can it Exist?" *Air Force Law Review*, 64: 2009, pp. 1–40.

[15] Perhaps more troubling is that the concept of deterrence by denial as described in the 2015 White House Report on Cyber Deterrence Policy is not consistent with its description in classic deterrence literature. Whereas the White House policy defines it as persuading adversaries that the United States can thwart malicious cyber activity through hardening and resiliency, classic deterrence literature defines it as threatening punishment in the form of cost

are also other, less visible, consequences from this mismatched strategy. When deterrence by denial fails, as it has repeatedly, the next recourse in current U.S. strategy is deterrence by cost imposition. There is no doubt that the United States has the capability to impose costs in, through, and from cyberspace, but there is a strategic liability in frequently resorting to that course of action as a response action, i.e., an accumulation of *incurred* costs. These costs can include, but are not limited to, potential exposure/compromise of a valuable Internet-Protocol (IP)-based, Human Intelligence (HUMINT) or Signals Intelligence (SIGINT) (counter)intelligence asset that enables covert Computer Network Exploitation (CNE) or the potential loss of the future effectiveness of a valuable cyber tactical action used today. Moreover, response-based, cost-imposition cyber OAAs diminish, if not make irrelevant, the potential for managing attribution, a unique attribute of cyber OAAs that has significant strategic value.

Successfully applying deterrence by cost imposition requires effective signaling. If an adversary is not aware of an attempt in cyberspace to communicate resolve to defend the status quo, a cost-imposition effort will fail. Effective signaling before imposing costs begins with the threat to respond.[16] In this dynamic, a motivated adversary will have significant incentive to take this knowledge and pro-actively seek to mitigate the promised cost imposition, thereby muting its potential effect. Effective signaling after imposing costs in cyberspace requires that the United States reveal its identity (attribution) in cyber OAAs, thereby taking out-of-play the strategic value provided to it through manageable attribution. In addition, cost imposition in cyberspace requires that an effect be visible. Once a vulnerability has been exploited and revealed through a visible effect, a well-resourced adversary promptly will mitigate or remediate associated risks and pursue a full forensic investigation to reveal the cyber OAAs behind exploitation. Consequently, the cyber OAAs used likely will lose their potential value for future employment. In addition, if the target of the exploitation had intelligence value, yet another cost will be incurred by its engagement.

Expanding deterrence by cost imposition to include threats of law enforcement penalties, sanctions, and "name and shame" approaches—denoted as whole-of-government deterrence—should be recognized for what it is—the addition of weaker forms of punishment because robust costs cannot be credibly imposed. Adding to a menu of weak options does not make deterrence stronger; it only reveals its inherent incompatibility with the challenge of the domain.

---

imposition through denial or limitation of an adversary's objectives. This misunderstanding has crept into the discussion on cyber deterrence in policy circles conflating deterrence by denial with defense and implying that hardening and resiliency are de facto deterring, which they are not.

[16] For example, after the DPRK exploitation of Sony Pictures Entertainment, President Obama stated that the United States would "respond … at a place and time of our choosing," http://www.chicagotribune.com/news/nationworld/chi-president-obama-end-of-year-news-conference-20141219-story.html.

This discussion is not intended to rebut the effectiveness of a strategy of deterrence applied to and operationalized in the land, air, maritime, and space domains. These well-defined operational domains, the identities of those who operate in them, and their activities and intentions are more easily monitored and well-understood. These certainties support the appropriateness of an adversary-centric, threat-based strategy of deterrence to protect or advance U.S. interests in these domains. Conversely, the unique characteristics of cyberspace and cyber OAAs introduce and sustain many uncertainties. The domain is malleable with no agreed-upon boundaries; the breadth and identity of others operating in cyberspace are not well known; the activities and intentions of others can be difficult to attribute or discern, respectively; and the costs associated with cyber OAAs are highly contestable.[17] This high degree of uncertainty calls for a capabilities-based strategy for cyberspace rather than a threat-based strategy.[18] A capabilities-based strategy for cyberspace would focus less on who might threaten the United States or where it might be threatened, and more on what the United States wants to be able to do in cyberspace.

The notion of a domain-specific strategy may seem entirely novel, but it is only partially the case. The United States, after all, has a capability-specific strategy, i.e., nuclear weapons and its associated strategic nuclear deterrence strategy, and a multi-domain conventional deterrence strategy (air, land, maritime, and space). A single domain strategy applied to cyberspace may merely be a natural evolution in strategic thinking.

A Strategy of Cyber Persistence

To begin, the current strategic approach of seeking to establish norms of responsible behavior through diplomacy should continue to be pursued. What must be cast aside is the simultaneous directive of operational restraint that is supporting a strategy of deterrence. A strategy for cyberspace should be enabled, not crippled, by the unique characteristics of cyberspace and cyber OAAs. Such a strategy should consider the malleability of cyberspace, the absence of cyber sovereignty, continuous operations and contact, the strategic value of manageable attribution, and the operational versatility that is afforded through reversible damage and damage short of armed conflict. It should shape cyberspace ad infinitum to enable U.S. relative autonomy in cyberspace, which, in turn, would generate, if effective, non-specific and indirect effects to persuade adversaries to not consider or execute COAs that threaten U.S. interests in cyberspace and persuade allies to consider and/or execute COAs that support U.S. interests. Such a strategy would support the generation of cyber power. The cyberspace operational domain calls for a strategy of cyber persistence, a strategy based upon the use of cyber OAAs (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding

[17] Richard J. Harknett, "The Logic of Conventional Deterrence and the End of the Cold War," *Security Studies,* Autumn 1994, pp. 86-114

[18] Donald Rumsfeld, *Report of the Quadrennial Defense Review,* Sept. 2001*,* Department of Defense, Washington, D.C.

contact) continuous tactical, operational, and strategic advantage in cyberspace so that the United States could ultimately deliver direct effects in, through, and from cyberspace at a time and place of its choosing.

Suggesting persistent operations in cyberspace may raise concerns to readers. And so, before diving more deeply into the strategy of cyber persistence, it would be constructive to consider further why operational restraint has thus far dominated U.S. policy in cyberspace. Doing so may assuage several concerns of those who fear the specter of persistent operations in cyberspace.

U.S. policymakers during the Obama administration appear to have been concerned that cyber OAAs could potentially lead to unintended damage and uncontrollable escalation, which, in turn, reinforced a policy of operational restraint.[19] A close examination of the unique technical nature of the cyberspace operational environment, however, reveals that, if anything, the potential exists for more management, not less when engaged in cyber OAAs.

Escalation can be defined as "an increase in the intensity or scope of action in a competition that crosses thresholds considered significant by one or more of the participants."[20] Acts of sabotage have been studied and well documented in international relations historical scholarship. Such acts are described as being inherently technical in nature and systems-oriented. As most economic and military systems are now cyberspace-enabled, if not cyberspace-dependent, many targets (physical systems) are potentially at risk of sabotage in cyberspace. Historical scholarship also informs us that the effects from sabotage operations have been primarily tactical, and only rarely operational or strategic. There is little reason to conclude that the same is not true of sabotage operations in cyberspace, especially if one considers the unique characteristics of cyberspace and cyber OAAs. There is no doubt that the technical basis of cyberspace creates an inherent condition of vulnerability, but it is critical to remember that its design was meant to provide systemic resiliency, as well. It is not an oxymoron to consider cyberspace a vulnerable-resilient system. Thus, for example, cyberspace makes possible distributed denial of service (DDOS) operations, but it also facilitates recovery from them. The question, then, is only whether one has the capacity to sustain the disruption or whether the network resiliency will emerge relatively swiftly or not. The fluidity of this space that makes the DDOS operation possible also makes the recovery possible.

The duration, scope, and intensity of cyber OAAs and their resultant technical damage (e.g., deny, degrade, disrupt, destroy) can be managed by taking into account an adversary's abilities to reconstitute functionality lost by target

[19] For an analysis of how senior leaders apply extreme caution in the use of cyber OAAs in wargames, see Jacquelyn Schneider, *Cyber and Crisis Escalation: Insights from Wargaming* (Newport, RI: U.S. Naval War College, 2017).

[20] Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Rand: Project Air Force, 2008), http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.sum.pdf

engagement. For example, cyber tactical action-target pairings can be designed to deliver damage that is slight (no reconstitution action required by adversary), moderate (action includes transferring functionality to redundant or suboptimal systems), or significant (action includes terminating systems and losing all functionality). Additionally, pairings can be designed to generate low-visibility damage, thereby limiting the scope of the intended effect. Finally, pairings can be designed to enable reversible damage so that escalation thresholds can be crossed over and withdrawn back to, at will.

Such cyber OAAs offer another advantage that other domain-capabilities pairings do not, i.e., tactical effects can be intentionally managed to generate strategic effects. For example, extending the duration of a tactical effect intentionally could generate a cumulative strategic effect over time. And, given that cyberspace is defined as consisting of interconnected physical systems, a pairing designed to have a tactical effect can be directed at multiple like targets, thereby intentionally generating a cumulative strategic effect over space. For example, disrupting a single regional power station through Industrial Control Systems (ICS) exploitation would have a localized, tactical effect, whereas disrupting simultaneously several multi-regional power stations would have a broader, strategic effect. These are manageable political-military options.

Subversion is primarily social in nature, and many potential targets (humans) are accessible in cyberspace via social and other media. Consequently, engaging in subversive activity has become far easier. Moreover, the persistent-contact character of cyberspace facilitates message saturation. But, accessibility and persistent contact do not lead obviously to the conclusion that subversion operations in cyberspace are inherently escalatory.

In fact, other characteristics of cyberspace and cyber OAAs serve to self-limit the potential for subversion effects to escalate independently into the realm of actual politics, to successful insurgency, and ultimately to governance. For example, the potential for non-attribution has lowered the risks of participating in subversion efforts. Yet, it has also lowered the risks of a state stopping such activity, i.e., there is no "public face" around which followers can coalesce in order to have more significant impact. Consider, for example, the very active *Anonymous* group whose members abide by few rules, but do agree not to disclose one's identity and not talk about the group. Many other groups similarly take advantage of the potential for plausible deniability that is afforded by manageable attribution.

Traditional propaganda operations sought to replace a target audience's reality with a coherent alternative reality—a new truth. Creating a new truth is more difficult in cyberspace because of the multitude of actors and counter-information disseminators. Rather than seek to replace truth, an alternative approach is to use the disaggregated nature of cyberspace to flood so many counter-narratives that no one knows what to believe. These counter-narrative operations can only escalate into politics and beyond if the target population's trust in state institutions is low to begin with, which is a broader political issue, not a cyber-generated issue. While political action, thus, must be directed toward reestablishing political trust, those subjected to subversive cyber OAAs must have active counter-subversive cyber OAAs in place that both deal with subversive content and remove the technical capacity being used

for subversion. Rather than sit back and allow cyber platforms to be used for subversion covertly, one must be prepared to call out subversive actors publicly and regularly so that the public can discern the intent behind the information flows they are experiencing. Again, an active engagement in counter-subversion is not a strategy of escalation but rather one of mitigation, and it will require persistent engagement in the information space to achieve that mitigation.

Fears of unintended damage and uncontrollable escalation have not taken into account sufficiently the unique characteristics of cyberspace and cyber OAAs, which, arguably are far better than any other domain-capabilities pair, at enabling the United States to manage well the prospects of both. This perspective does not dismiss a healthy concern of fear of escalation. Rather, it is to suggest that the fear is no more salient for cyberspace and cyber OAAs than it is for any other military capability or national instrument of power that is brought to bear in support of national strategy.

The vulnerable–resilient nature of cyberspace means that we will see cyber aggressive acts, but it also means that the system can facilitate responses to such actions and strike a mitigation balance. What does guarantee that such aggressive cyber OAAs will have large-scale effects is if one does nothing to mitigate them and allows them to go unfettered. A strategic goal of cyber persistence is to remove the escalatory potential from adversarial action.

Operationalizing a Strategy of Cyber Persistence

A strategy of cyber persistence would accept and embrace that the absence of sovereignty as well as constant contact are structural and operational characteristics of the cyberspace domain and would support posturing globally and persistently. It would leverage the malleability of cyberspace by routinely employing domain expansion/contraction practices to frustrate efforts at exploitation.[21] In addition, cyber OAAs that dynamically shift attack surfaces, such as "moving target defense," could be employed to further frustrate the plans of would-be exploiters.[22]

Given the extraordinary volume of cyberspace interactions, a strategy of cyber persistence would require developing and implementing automated courses of action. Intrusion Detection Systems, for example, have reached a high level of sophistication, a consequence of which can be an unmanageably high number of alerts to which to respond.[23] Upon identifying a bad actor by IP, URL or any other security control, an automated solution could not only block the activity and send an

[21] One defensive measure, for example, is to mislead attackers through such tactics as the creation of honeypots, honeynets, or honeytokens in cyberspace (created physically or virtually). Spencer R. Calder, "A Case for Deception in the Defense," *Military Cyber Affairs,* 2:1, Article -4, 2016, http://scholarcommons.usf.edu/mca/vol2/iss1/4/, and https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9.
[22] "Moving Target Defense," https://www.dhs.gov/science-and-technology/csd-mtd.
[23] Thomas Toth and Christopher Kruegel, "Evaluating the impact of automated intrusion response mechanisms," 18th Annual Computer Security Applications Conference Proceedings, 2002, pp. 301–310, https://www/eeexplore.ieee.org/document/1176302/.

alert, but also isolate the affected system from the network, image the system for forensics, rebuild it to a known trusted state and bring it back online.[24] In addition, an automated solution could disrupt or degrade the source of the offending action, leveraging the unique capability of cyber OAAs to deliver temporary or reversible damage short of that associated with use of force and armed attack. While care will have to be directed to the decision-making models that use automation, those who can introduce it as a facet of effective persistence will gain significant security advantages.

In some instances of cyber operations (e.g., DDOS), the high volume of interactions is a function of the perpetrator's use of botnets. Microsoft revealed a technique that continuously "listens" to sound patterns of infected computers to collect clues on the botnet's command centers. Their efforts supported identifying key servers that subsequently were seized by law enforcement authorities in support of a criminal investigation. This type of cyber operation could be applied continuously and globally to identify botnet-enabling servers against which automated course of action could be directed to disrupt or degrade the functionality of those servers.[25]

While prevalent in the private sector financial industry, automated courses of action are not consistent with the current U.S. strategic approach of operational restraint in cyberspace. Consequently, a change in current authorities would be required to allow for them to support a new strategy of cyber persistence, including, but perhaps not limited to, Presidential Policy Directive 41, which establishes principles that govern the federal government's activities in cyber incident response.

In early 2017, U.S. Cyber Command planning projected 133 Cyber Mission Force teams would be operational by 2018.[26] A strategy of cyber persistence may require a rebalancing of the teams within that total, perhaps weighting them more in favor of National Mission Teams (which currently number 13), whose responsibilities are to defend the United States and its interests against cyberattacks of significant consequence.

All of the above are but a few of the considerations that would follow from a decision to implement a strategy of cyber persistence. The strategy would generate

[24] "Cyber Security for Financial Services," White Paper, https://www.symantec.com/content/en/us/enterprise/white_papers/cybersecurity-whitepaper-financial-wp-21352892.pdf.

[25] "Hear that botnet? Microsoft listens to infected computers to help fight cybercrime," https://blogs.microsoft.com/.../hear-that-botnet-microsoft-listens-to-infected-computer-cybercrime/#sm.000k6h3bi1dw4effzh72kry9zb0sg, "Microsoft assists law enforcement to help disrupt Dorkbot botnets," https://blogs.technet.microsoft.com/mmpc/2015/12/02/microsoft-assists-law-enforcement-to-help-disrupt-dorkbot-botnets/. and "Microsoft: We've taken down the botnets. Europol: Would Sir like a kill switch, too?" https://www.theregister.co.uk/2016/01/19/microsoft_botnets_kill_switch/.

[26] "The Department of Defense Cyber Strategy Fact Sheet," https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.

cyber power which, in turn, would support autonomy in cyberspace. By accruing that benefit, the United States could take advantage of the fact that cyberspace is a domain by and through which all other operational domains and national instruments of power are enabled—diplomatic, information, military, economic, financial, intelligence, and law enforcement—and develop a comprehensive strategy for the use of cyberspace that would address how cyberspace and cyber OAAs can be leveraged to support or be supported by those instruments to sustain or advance U.S. national interests.

Conclusion

The U.S. strategic approach to cyberspace is failing against cyber threats. It is also failing to take advantage of the security opportunities that flow from the uniqueness of cyberspace and cyber OAAs. Developing international norms for responsible behavior in cyberspace is an appropriate goal, but not an achievable one when accompanied by a policy of operational restraint. Relying upon a strategy of deterrence in cyberspace to create specific and direct behavioral effects until norms are established reflects deterrence strategic inertia—the inappropriate application of which is at the core of an ever-increasing U.S. strategic deficit in cyberspace. The character of cyberspace and cyber OAAs is unlike that of any other operational domain and its associated capabilities and does not align with the requirements of a strategy of deterrence. That uniqueness demands a unique strategy, a capabilities-based strategy of cyber persistence that is less adversary-centric and more focused on what the United States wants to be able to do in, through, and from cyberspace.

Disclaimer: The views and opinions expressed in this paper and or its images are those of the authors alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DoD), U.S. Cyber Command (USCYBERCOM), or any agency of the U.S Government. Any appearance of DoD visual information for reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission or broadcast. Additionally, comments made by others regarding this paper does not expressly or impliedly indicate DoD endorsement, sanction, or support of those views. Further, any information or material placed online, including advice or opinions, are the views and responsibility of those making the comments and do not reflect the views of the DoD, U.S. Government or its third party service providers. By submitting a comment for publication or posting, you agree that the DoD, U.S. Government and its third party service providers are not responsible, and shall have no liability to you, with respect to any information or materials posted by others, including defamatory, offensive, or illicit material, even material that violates this agreement or is otherwise illegal.