INSTITUTE FOR DEFENSE ANALYSES

Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation

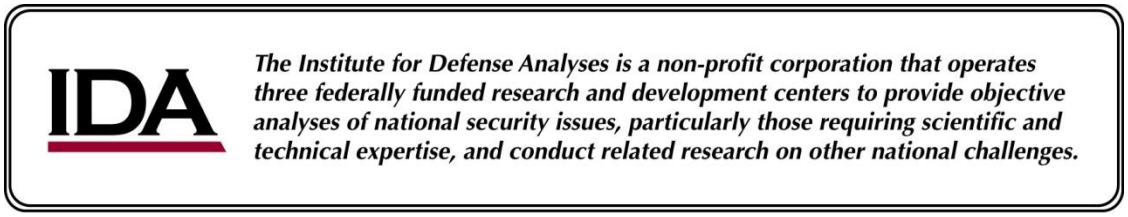
Michael P. Fischerkeller
Institute for Defense Analyses

Richard J. Harknett
University of Cincinnati

May 2018

IDA Non-Standard
NS D-9076

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882



About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under, Central Research Project C5191, "Offense-Defense and Cyberspace." 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.

Acknowledgments
Gen (ret'd) Larry Welch

For more information:

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Persistent Engagement, *Agreed Competition*, Cyberspace Interaction Dynamics and Escalation

Michael P. Fischerkeller – Institute for Defense Analyses
Richard J. Harknett – University of Cincinnati

Introduction

A significant concern among policymakers and academics discussing cyber operations is a fear of escalation should states adopt a more proactive posture in cyberspace.[1] Past policy statements and international security scholarship tend to focus narrowly on the escalation dynamics resulting from cyberattacks, or the threat thereof, that might cause physical damage or loss of life. This limited focus on *potential and episodic* cyber-enabled crises or war scenarios excludes an equally, if not more important, strategic space—*actual and continuous* strategic competition in cyberspace that does not reach the level of armed conflict. In 2018, U.S. strategic guidance found in the *National Security Strategy of the United States of America* shifted to emphasize the significance of this competitive space, and United States Cyber Command (USCYBERCOM) prescribed a strategic approach of *persistent engagement* to contest and counter the ability of adversaries to gain strategic advantage without engaging in armed attack. This article considers this shift in U.S guidance documents and analyzes the potential interaction dynamics in a cyber strategic environment structured by interconnectedness-constant contact-persistent engagement. In so doing, it introduces a distinction between interaction and escalation dynamics, one based on a 21st century adaptation of Herman Kahn's *On Escalation*. This article concludes that fears are not warranted that persistent engagement in cyberspace will result in spiraling or uncontrollable escalation.

This article is structured as follows. To set the context under which interaction dynamics will be considered, the first section summarizes the view of a competitive environment described in the White House and U.S. Department of Defense (DoD) 2017 and 2018 strategic guidance. This is followed by a description of the strategic approach of *persistent engagement*, both its theoretical and conceptual foundations and its

[1] See, for example, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities.* Committee on Armed Services, U.S. House of Representatives, March 1 2017, https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf; Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki (2015) "Cyber House Rules: On War, Retaliation and Escalation," *Survival* (2015), 57:1, 81–104; David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* (2014), 56:4, 7–22; Jason Healy, "Triggering the New Forever War in Cyberspace," *The Cipher Brief* (April 1, 2018), https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace.

operational prescription as provided by USCYBERCOM. Next is a review of the core security studies literature on escalation dynamics—in general and specific to cyberspace. The current strategic environment is then considered in light of this scholarship, generating a set of propositions regarding the impact of persistent engagement on cyberspace interaction dynamics. The stability of these operational dynamics is then discussed, followed by a brief consideration of shifting away from the traditional "ladder" metaphor for understanding cyberspace interaction dynamics.

Strategic Environment

The *2018 National Security Strategy of the United States of America* (NSS) and its complement, the *National Defense Strategy* (NDS), stand in marked contrast to their predecessors in their declarations that adversaries are executing strategic campaigns short of armed attack to secure and advance national interests. Indeed, both documents assert that the central challenge to U.S. security and prosperity is the re-emergence of a long-term, *strategic* competition with revisionist and rogue regimes and actors that have become skilled at operating below the threshold of armed conflict—challenging the United States, its allies, and partners with deniable hostile actions that seek to undermine faith and confidence in democratic institutions and the global economic system.[2]

Cyberspace and its derivative cyber operations, in particular, have been identified as offering state and non-state adversaries the ability to wage strategic campaigns against American political, economic, and security interests without ever physically crossing U.S. borders.[3] This view is presented most comprehensively in the 2018 *Command Vision for U.S. Cyber Command*, in which adversaries are described as continuously operating against the United States below the threshold of armed conflict—demonstrating the resolve, technical capability, and persistence to undertake strategic cyberspace campaigns to weaken U.S. democratic institutions and gain economic, diplomatic, and military advantages.[4,5] What is of critical importance to note from these documents is the assessment that these operations short of armed conflict can have cumulative impact at the strategic level—these operations can degrade or damage sources of American national power. Analytically, if this assessment is correct, it is not simply the United

---

[2] See *National Security Strategy of the United States of America* (The White House, December 2017), p. 3 and 31, respectively, and *Summary of The 2018 National Defense Strategy of The United States of America* (Department of Defense, 2018), p. 2.

[3] *National Security Strategy*, op. cit., p. 12.

[4] *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority* (United States Cyber Command, 2018), p. 3.

[5] Concern has been expressed regarding "the *persistence* exhibited by adversaries attempting to penetrate critical infrastructure and the systems that control these services." See, *Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, Before the Senate Committee on Armed Services*, (May 9, 2017). https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf

States that can be affected by such operations, but in practice, all state actors reliant on cyberspace for the development and projection of national power. It is in response to this challenge that USCYBERCOM has prescribed the strategic approach of *persistent engagement.*

Persistent Engagement

From a security studies perspective, cyberspace may be best understood as a technically enabled operational domain with distinct features that shape particular behaviors by state actors, businesses, and even individuals. Interconnectedness is the oft-cited, but rarely embraced in strategic thinking, core structural feature. If one accepts interconnectedness as such, then fundamental international relations concepts for understanding or explaining actor behaviors come into question, such as sovereignty and territoriality, because the core condition that follows from interconnectedness is constant contact, a term referenced by USCYBERCOM to describe the cyberspace operating environment.[6,7] This condition, when coupled with the nature and substance of cyberspace—a vulnerable and resilient technological system that is a global warehouse of and gateway to troves of sensitive strategic information—encourages persistent opportunism to access and leverage those sensitive data while simultaneously requiring states to continuously seek to secure those data and data flows from others.[8] The combination of interconnectedness and constant contact with cyberspace's ever-changing character both in "terrain" and in the capacity for maneuver across that terrain further encourages operational persistence/engagement in order to secure and leverage critical data and data flows. When these factors are considered in sum, in operational reality, operational persistence/engagement becomes a strategic imperative for states seeking to secure and advance their interests in, through, and from cyberspace.

This theoretical and conceptual argument for operational persistence/engagement is consistent with nearly a decade of domain and operational observations by USCYBERCOM. For example, in reference to the ever-changing character of cyberspace the *Command Vision* notes that cyberspace is where new vulnerabilities and opportunities continually arise as new terrain emerges; no target remains static; no offensive or defensive capability remains indefinitely effective; no advantage is permanent; and well-defended cyber terrain is attainable but continually at risk. And

---

[6] See Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* (Summer 2017), 61:3, pp. 381–393.

[7] *Command Vision, op. cit.*, p. 4.

[8] For a discussion of the nature, character, and substance of cyberspace and its implications for cyberspace strategy, see Michael Fischerkeller. *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*, (Institute for Defense Analyses: Alexandria, VA 2018).

adversary offensive activities are also said to persist because opportunity costs are low, and accesses, platforms, and payloads can remain useful for extended periods.[9,10]

To operate effectively in this dynamic environment, USCYBERCOM prescribes that the United States increase resiliency, defend forward as close as possible to the origin of adversary activity, and contest cyberspace actors to generate continuous tactical, operational, and strategic advantage.[11] They argue that a strategic approach of *persistent engagement*—described operationally as the combination of seamless resiliency, forward defending, contesting, and countering—will compel many U.S adversaries to shift resources to defense and reduce attacks. Moreover, *persistent engagement* is expected to allow for greater freedom of maneuver to impose tactical friction and strategic costs on U.S. adversaries pursuing more dangerous activities before they impair U.S. national power. This effort seeks to render the majority of adversary cyber and cyber-enabled activity inconsequential.

The *Command Vision* is absent any discussion of potential escalation risks from a strategic approach of *persistent engagement*.[12] This is a notable omission because the document does include a section on risks and risk mitigation.[13] Given that continuous engagement is intended to create uncertainty and cause friction, two factors often associated with increased risk of escalation, those predisposed to escalation concerns likely view this approach with alarm. Whether or not they should is the key question moving forward and the focus of this article's framework.

Background on Escalation Dynamics

It is not contentious to say that modern thinking regarding escalation dynamics was introduced in the seminal work of Herman Kahn, in which he defined escalation as "an

---

[9] *Command Vision*, *op. cit*., p. 4.

[10] Michael Fischerkeller, *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*, op. cit., p. 15, fn 58. Fischerkeller refers to low barrier to entry as an operational *incentive* for operational persistence vice a strategic imperative.

[11] USCYBERCOM argues that superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how they would operate—maneuvering seamlessly between defense and offense across the interconnected battlespace; where they would operate—globally, as close as possible to adversaries and their operations; when they would operate—continuously, shaping the battlespace; and why they operate—to create operational advantage for the United States while denying the same to U.S. adversaries. See, *Command Vision, op. cit.*, p. 5.

[12] Herbert S. Lin and Max Smeets in "What Is Absent from the U.S. Cyber Command 'Vision,'" *Lawfare*, (May 3, 2018), https://lawfareblog.com/what-absent-us-cyber-command-vision.

[13] The two risks highlighted are the impact of continuous engagement on high-demand low-density cyber forces and a diplomatic risk associated with claims that the United States is "militarizing" cyberspace.

increase in the level of conflict in international crisis situations."[14] Starting with the assumption of some sort of limited conflict or *agreed battle,* Kahn proposed three "ways" in which a would-be escalator could increase, or threaten to increase, his efforts: "increasing intensity," "widening the area," and "compounding."[15] *Intensity* was described as a function of doing more of what one is already doing—using more equipment, using new equipment, or attacking new targets such as logistics or a more "intensive increase" such as switching to nuclear weapons or attacks on cities.[16] *Widening the area* was described as increasing the geographical scope of the conflict. And *compounding* was described as extending the conflict to include allies or clients. Kahn's escalation ladder was developed with a focus on deliberate escalation in *potential, episodic* conflicts, giving primary attention to the threat or reality of force or coercion as a factor in negotiation.[17] Stated differently, in order to explore potential escalation dynamics from the launching point of a limited conflict, Kahn assumed that pursuit of any of these three ways would be viewed as escalatory.

Kahn argues that there are two basic classes of strategies that each side can use when engaged in limited conflict or *agreed battle*. One class makes use of the factors relating to particular levels of escalation in order to gain an advantage. The other uses the risks or threat of escalation or eruption from the *agreed battle*.[18] The latter, he notes, refers to the class of deterrence strategies.

Given its foundational and enduring value, it is not surprising to find Kahn's influence in more recent scholarship on escalation dynamics that focuses on nuclear, as well as non-nuclear-capable states in *potential, episodic* confrontations that involve or might come to involve the use of military force.[19] Morgan et alia expand on Kahn's focus of deliberate escalation to include other mechanisms—inadvertent as well as accidental escalation. Similar to Kahn's description, *deliberate* escalation is understood as being carried out with specific purposes in mind. For example, a party may deliberately escalate a conflict to gain advantage, to preempt, to avoid defeat, to signal an adversary about its own intentions and motivations, or to penalize an adversary for some previous action.[20] *Inadvertent* escalation is described as when one party deliberately takes actions that it does not believe are escalatory but which are interpreted as escalatory by another party to

---

[14] Herman Kahn (with a new introduction by Thomas C. Schelling), *On Escalation: Metaphors and Scenarios* (Routledge: London, 2017), p. 3.

[15] Ibid, pp. 4–6.

[16] Ibid, p.4.

[17] Ibid, p. 15.

[18] Ibid, p. 7.

[19] Forrest E. Morgan, Karl P. Mueller, Evan S. Madeiros, Kevin L. Pollpeter, Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008).

[20] Ibid, p. 20.

the conflict.[21] Such misinterpretation may occur because of incomplete information, lack of shared reference frames, or one party's thresholds or "lines in the sand" of which other parties are not aware. Finally, *accidental* escalation is described as when some operational action has direct effects that are unintended by those who ordered them, for example, a weapon may go astray to hit the wrong target, rules of engagement are sometimes unclear, a unit may take unauthorized actions, or a high-level command decision may not be received properly by all relevant units.[22]

Morgan et alia also assigned Kahn's "ways" of escalating to dimensions, where the *vertical* dimension was associated with "increasing intensity" and a *horizontal* dimension associated with "widening the area." They further equated the combination of *horizontal* and *vertical* with Kahn's "way" of *compounding*.[23] And they introduced a *political* dimension to escalation, which was described as when states adopt more extreme or unlimited objectives in crises/conflicts or, alternatively, pursue measures such as relaxing behavioral constraints that protect civilians.[24] Like Kahn's work, the study also proposes that the class of deterrence strategies is best suited for managing an enemy's propensity for deliberate escalation—discouraging an enemy from deliberately escalating a conflict by convincing that enemy that the costs of such actions will outweigh the benefits that may be accrued through escalation.[25] Within that class of strategies, they further argue that the key to managing risks of inadvertent escalation lies in clarifying thresholds—on all sides of a conflict.[26] And finally, they propose that the key to mitigating accidental escalation lies in an effective command and control strategy.[27]

Cyberspace Escalation Dynamics

Herbert Lin was an early adopter/adapter of the Morgan et alia framework to cyberspace by referencing it to aid in answering how the initial stages of conflict in cyberspace might evolve or escalate and what might be done to prevent or deter such escalation.[28] Lin also focused on how *potential, episodic* cyber conflict at any given level might be de-escalated or terminated (and what might be done to facilitate de-escalation or termination) and how cyber conflict might escalate into kinetic conflict (and what might

---

[21] Ibid, p. 23.

[22] Ibid, p. 26.

[23] This appears to have been an error, however, as Kahn described *compound* as expanding a conflict to include allies and others.

[24] Ibid, p. 18.

[25] Ibid, p. 22.

[26] Ibid, p. 24.

[27] Ibid, p. 27.

[28] Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* (Fall 2012), pp. 46–70.

be done to prevent kinetic escalation).[29] Lin's approach to responding to these questions was largely grounded in generating new sets of questions about and challenges associated with escalation dynamics in cyberspace. In support of his objective in writing the article, these serve as valuable checklists for national security planners/policymakers to reference in preparing for and managing a cyber-enabled crisis or conflict.[30]

Martin Libicki also adopted the Morgan *et alia* framework to explain escalation risk and dynamics in cyberspace, albeit with a stronger focus on potential risk.[31] Like Kahn and Morgan et alia, the context for his escalation discussion is *potential, episodic* conflicts (conflicts that involve or might come to involve military force)—once a crisis has blossomed into conflict, he states, crisis management becomes escalation management.[32] Stated differently, he focuses on the escalation risks associated with operational cyber war in which cyberattacks are carried out against targets that are considered legitimate war targets. Different types of targets are argued to carry different risks of escalation. Those outside a local conflict zone will carry one set of risks, civilian targets may carry another, dual-use yet another, and military and strategic targets another. Libicki argues that the relative severity of those risks will be a function of the value the adversary places on the targets.[33]

A similar argument is presented by Lawrence Cavaiola et alia in an article on escalation dynamics in a *potential, episodic* cyber-enabled war.[34] This effort blends Libicki's arguments into a succinct presentation, arguing that escalation could happen along three paths: horizontal, from military to civilian systems; vertical, from tactical to strategic military systems (perhaps affecting those that control nuclear weapons); and vertical, from limited civilian targeting to major civilian consequences.[35] Similar to other studies, the primary focus is on deliberate escalation, but the potential for inadvertent and accidental escalation is also explored by considering the many unique challenges that cyberspace and cyber operations pose, perhaps the most significant being uncertainty

---

[29] Lin also complemented the Morgan et alia framework by including another mechanism of escalation highlighted by Kahn—*catalytic*—which occurs when some third party succeeds in provoking two parties to engage in conflict (often referred to as "false flag" operations). Ibid, p. 46.

[30] Ibid, p. 56.

[31] Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012). Chapter 4, in particular, focuses on escalation risks and dynamics. Of note, he deviates a bit from Morgan et alia by describing *horizontal* escalation as the successive entry of the uninvolved into war on one or both sides. This descriptions aligns with Kahn's description of *compound* escalation.

[32] Ibid, p. 73.

[33] This point is also made by Michael Fischerkeller, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies," *Survival* (January 2017), 59:1, pp. 103–134.

[34] Lawrence J. Cavaiola *et alia*, "Cyber House Rules," op. cit.

[35] Ibid, p. 84.

associated with attribution and primary and/or potential secondary or tertiary operational effects.

In sum, Kahn's work certainly laid the conceptual foundations for thinking about "ways" in which would-be escalators could pursue escalation from a limited conflict. And several scholars have begun to think through what escalation dynamics may look like using similar ways in a cyber conflict. That said, there exists no "escalation ladder" equivalent nor, as will be discussed later, has there been a rich discussion of whether the "ladder" metaphor is even appropriate. The review also highlights that most of the cyberspace escalation scholarship adopted the same point of origin that Kahn did in his seminal work, i.e., deliberate escalation from a *potential, episodic* operational conflict or *agreed battle,* giving primary attention to the threat or reality of force or coercion as a factor in negotiation. And all also argued that the class of deterrence strategies was best for managing escalation from this starting point. Kahn's work clearly provides a solid foundation from which cyber escalation dynamics may be considered; however, it will be argued in the next section that existing scholarship would benefit from a closer examination of both cyberspace *interaction* and escalation dynamics, because it should not be assumed that the former, ipso facto, leads to the latter.[36]

Cyberspace *Interaction* Dynamics and Escalation in Today's Strategic Environment

The security studies community primarily has focused on *escalation* dynamics in cyberspace at the exclusion of interaction dynamics. Kahn, however, provides a basis for their consideration by mentioning a second class of strategies for managing escalation for *agreed battle,* a class that has all but been forgotten—*making use of the factors relating to particular levels of escalation in order to gain an advantage*.[37] Whereas deterrence strategies are well and commonly understood, this second class deserves further elaboration because it can play an important role in understanding cyberspace *interaction* as opposed to *escalation* dynamics. But first, the concept of *agreed battle* has to be considered in light of the current strategic environment because it will establish the strategic context for discussing this second class of strategies in the same.

According to Kahn, *agreed battle* is a concept rooted in factors relating to particular levels of escalation. It emphasizes that in an escalation situation in which both sides are accepting limitations, there is in effect an "agreement," whether or not it is explicit or even well understood. "Thus the term does not have any connotation of a completely shared understanding, an intention of containing indefinitely with the limitation, or even a

[36] This article argues that the distinction between interaction and escalation dynamics is critically important and not merely "distinctions without a difference." See, Herman Kahn, *On Escalation,* op. cit., p. xvi.

[37] Arguably, this class of strategies has been overshadowed in the last 70 years by strategies of deterrence, the class of strategies that was, and continues to be, the predominant focus of U.S. strategic thought and practice.

conscious quid pro quo arrangement."[38] Scholars who emphatically and urgently emphasize the importance of establishing cyberspace behavioral norms will see the construction of norms in this concept.[39] Others have argued, however, that de facto norms have already been established in cyberspace by states pursuing strategic cyber campaigns that generate effects short of armed attack.[40] In fact, the U.S. 2018 *NSS*, *NDS* and the *Command Vision* admit as much by stating that adversaries are continuously operating strategically against the United States short of armed conflict via strategic cyberspace campaigns to gain economic, diplomatic, and military advantages. What is important to note in Kahn's rendering is that the "agreed" part of the battle rests on *interactions* between adversaries, which despite being complex and nuanced can come to be understood and shared between actors. He notes that states can come to recognize "what the 'agreed battle' is and is not, what the legitimate and illegitimate moves are, and what are 'within the rules' and what are escalatory moves."[41]

Building upon Kahn's notion and applying it to current cyberspace campaigns and/or operations, this article argues that U.S. adversaries have, through their behaviors, established a strategic *agreed competition* in cyberspace at a level of interaction where operational effects fall below that equivalent to armed attack. After eight years of observing adversaries persistently operate in cyberspace, USCYBERCOM has argued that a strategic approach of *persistent engagement* is best suited for securing and advancing national interests in this *agreed competition*.[42] This, in effect, meets Kahn's definition of a class of strategy that makes use of the features of the particular *agreed battle*. The United States' adoption of such a strategic approach will introduce new interactions into the *agreed competition*.

Structural Incentives and Strategic Rationales Sustaining "Agreed Competition"

The earlier introduction to the theoretical and conceptual foundations supporting *persistent engagement* argued that the interconnectedness of cyberspace creates a structural condition of constant contact that, when coupled with cyberspace's nature, character, and substance, generates a strategic imperative for operational

---

[38] Herman Kahn, *On Escalation*, op. cit., fn 4, p. 3. Kahn attributes this term to Max Singer.

[39] For example, Lin, Libicki, Cavaiola et alia and many policymakers repeatedly call for the establishment of such norms in cyberspace to encourage "responsible" behavior, make appropriate a strategy of deterrence, and facilitate escalation management. Also see, *Department of Defense – Defense Science Board Task force on Cyber Deterrence* (Department of Defense: 2017).

[40] See, James A. Lewis, *Rethinking Cyber Security: Strategy, Mass Effects, and States* (Center for Strategic and International Studies, January 2018), Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace", op. cit.

[41] Herman Kahn, *On Escalation*, op. cit., xiii.

[42] See, *Command Vision*, op. cit., p.6., where *persistent engagement* is described as allowing the United States to compete more effectively below the level of armed conflict.

persistence/engagement. Presuming that states respond to this imperative, a robust strategic competition in cyberspace should be expected. However, that same condition and those same features also generate incentives for states to limit the impact of their cyber operational effects below the threshold of armed attack. Two incentives, in particular, that have been discussed elsewhere are that deliberate escalation to armed attack equivalence could result in a cyberspace war that would likely be of long duration, expensive, and result in few, if any, enduring strategic gains.[43] And crossing the armed attack threshold opens the door for states to legitimately bring to bear cross-domain, conventional, kinetic weapons based on an argument of self-defense as defined in the United Nations Charter's Article 51.[44] Regarding the latter, once a conflict has expanded into multiple domains, the pursuit of national interests involves very different risks, costs, and challenges. It would no longer be *agreed competition*, but conflict, and potentially war.

In addition to these structural incentives sustaining *agreed competition*, James Lewis has offered a thoughtful and comprehensive discussion of the political and strategic constraints states also face in deliberately escalating above the armed attack threshold.[45] He argues that, if you consider how great powers have historically made strategic decisions about entering into conflict, resorting to operations equivalent to armed attack in cyberspace is highly unlikely. The existential conflicts of the last century, conflicts that required mass mobilization, territorial invasion, and mass destruction (including critical infrastructure) to realize strategic ends are not present today.[46] There is no doubt that many states seek to challenge the existing international order, but these are not existential challenges to any state, and the constraints of cost and destruction induce caution in the ways and means those challengers adopt. And so, for example, destructive attacks on critical infrastructure are more likely to appear as too risky for U.S. adversaries, of limited benefit to their goals, and perhaps irrelevant in achieving the desired strategic outcome of undermining U.S. hegemony and building regional dominance without armed conflict with the United States.[47] This perspective is further supported empirically through an analysis of a decade of cyber disputes among rival states.[48]

---

[43] See, Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Strategic Studies Institute and U.S. Army War College Press: Carlisle, PA, 2013), pp. 45–48 and Michael Fischerkeller, *Offense, Defense, and the Irrelevance of Advantage*, op. cit., pp. 15–16.

[44] Michael Fischerkeller, *Offense, Defense, and the Irrelevance of Advantage*, op. cit.

[45] James A. Lewis, *Rethinking Cyber Security, op. cit.* See, specifically, Chapter 4, "Cyber Operations and Interstate Conflict," and Chapter 5, "Political and Strategic Constraints on Cyber Attack."

[46] Ibid, p. 27.

[47] Ibid, p. 28.

[48] See Chapter 4 in Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press: New York, NY, 2015).

One of the main impetuses to examining escalation control in the 1960s was the recognition among theorists and policymakers that fighting all out nuclear war overshot any advancement of national interest. So the question became how one might advance interests, despite that risk, without using nuclear weapons. It appears that a similar logic is taking (or has taken) hold in the strategic use of cyber means. That is, if cyber means are to have unique strategic value, it will come from operations short of armed attack equivalence that cumulatively enhance one's own power or degrade and destabilize others' sources of national power. It could be argued, therefore, that armed attack/war (traditionally involving measures of death and destruction) with cyber means actually overshoots the strategic utility of cyber operations. That would be "eruption," in Kahnian-speak, beyond the ceiling of *agreed competition*. And that outcome would be, for rational strategic cyber actors, a failure of strategy. And so there is a strategic rationale for seeking to gain advantage in, through, and from cyberspace short of armed attack. Actors might decide to engage in war, but the strategic purpose of the competitive interactions in *agreed competition* is so they do not have to.[49,50]

If one accepts the above arguments that there are structural incentives and strategic rationales from which *agreed competition* emerged and because of which it will sustain if/when the United States adopts a strategic approach of *persistent engagement*, an entirely new strategic space that has heretofore been unexplored for *interaction and escalation* dynamics is laid bare. What is offered in the next section, then, is the initial intellectual expedition into cyberspace *interaction dynamics* and escalation in this *agreed competition* space.

Agreed Competition – Competitive Interaction

To reiterate, when discussing *agreed battle*, Kahn argued one class of strategies uses the risks or direct threat of escalation beyond the *agreed battle* to gain advantage over an adversary. These ranged from red lines (declared deterrence) to riskier forms of

[49] It is interesting to ponder why much of security studies literature on cyberwar, cyber conflict, cyber deterrence, cyber crisis, and escalation has been focused on a narrow band of important, but least likely activity, while the *agreed competition* space has emerged rather unexamined.

[50] A note of caution for U.S. and western policymakers is warranted. It would be folly to think that U.S. adversaries won't attempt to dissuade the adoption of a strategic approach of *persistent engagement* by initially responding in ways that seek to fuel the flames of fear of escalation from *agreed competition*. With this expectation, it would behoove U.S. policymakers to keep in mind the important distinction recently offered by James Lewis between mass effects vice strategic effects. Mass effect cyber operations are intended to be visible and disconcerting but are not of strategic consequence and so their early appearance after the adoption of a more proactive cyberspace strategy should not be unexpected. Given that such events are strategically inconsequential, their effects would not likely cross the threshold of *agreed competition*; therefore, their occurrence should not dampen policymakers' resolve or confidence in pursuing a persistent strategy in cyberspace. See, James A. Lewis, *Rethinking Cyber Security, op. cit.*

brinkmanship as well as forms of Thomas Schelling's coercive bargaining.[51] In discussing *agreed battle*, Kahn also recognized a second class of strategies through which advantage could be gained by leveraging the unique features particular to a level of escalation. It has been argued in this article that in today's strategic environment what defines the "particular level of escalation" associated with *agreed competition* is effects equivalent to armed attack. As such, that level represents a de facto ceiling for effects in this competition. In efforts to gain advantage in this *agreed competition*, then, it can be expected that states will do so through *competitive interaction* below this ceiling, "making use" of it to gain advantage while avoiding escalation.

Kahn's "ways" can be adapted to cyber operational realities to conceptualize what *competitive interaction* comprises. Two of his three "ways"—widening the geographic area and compounding by including allies or clients—are indicative of the types of behaviors to be expected in *competitive interaction* in cyberspace. Kahn's "widening the area" and "compounding" should, however, be re-interpreted in light of the nature, character, and substance of cyberspace. Traditional territorial-based definitions do not apply well to an operating domain in which territory and segmentation have little, if any, relevance. Employing cyber operations short of armed attack equivalence, states are able to secure their own and degrade, usurp, or circumvent others' national power (economic, diplomatic, military, and social cohesion) by targeting specific data, data flows or sectors/industries/populations that are the sources of that power. *Competitive interaction* in *agreed competition*, then, should be characterized as campaigns populated by cyber operations seeking, over time and over space, to generate cumulative strategic effects (i.e., to gain advantage) by targeting sources of national power through shifts and/or increases in scope, scale, and frequency (as a function of "count"). In this *agreed competition* within cyberspace, *widening* could be measured as an increase in the number of systems affected and *compounding* as the number of other actors whose systems are utilized or affected. The analytical utility of these two measures enables one to capture with greater clarity the characteristics of strategic cyber campaigns and operations. For example, *compounding* could occur in at least two ways: transiting through someone's system to gain access to someone else's or targeting a new system for effect.

It follows, then, that the class of strategies best suited for managing interaction dynamics in this *agreed competition* is that which counters or contests widening and compounding. The strategic approach of *persistent engagement* intends to do just that

[51] Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press: Cambridge, MA, 1960).

through operations that maneuver seamlessly between defense and offense *across* the interconnected cyber battlespace to compete more effectively outside of armed conflict.[52]

There is substantial, publicly reported evidence of specific U.S. adversaries engaging in cyberspace *competitive interaction* (as described in this manner) for the last several years, with different states doing so for different reasons to address their strategic interests.[53] China has directed a great deal of time and effort to targeting a range of industry and commercial enterprises in pursuit of general scientific, technical, and business information. Examples include exploitation of data on the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the MV-22 Osprey. This cyber campaign, directed at contractors and agencies residing within and external to U.S. borders (a combination of widening and compounding), will reduce costs and accelerate the development of foreign weapon systems, enable reverse-engineering and countermeasures development, and undermine U.S. military, technological, and commercial advantage.[54,55] China has also sought out more specific information through cross-sector/industry cyber operations targeting personally identifiable information (PII), possibly with the objectives of using these data to facilitate future "insider" cyber operations, assist in the recruitment of human intelligence assets, or identify and monitor persons of interest to the government (e.g., dissidents, foreign journalists, and/or others who may pose a threat to the Communist Party's image and legitimacy.)[56] Russia, through its campaign of cyber operations—including those used in Russia's war with Georgia in 2008 and those used to influence the Brexit referendum and the U.S. election in 2016—is pursuing a strategic campaign to undermine Western democracies and weaken the multilateral alliances that Russia sees opposing its future, including NATO

---

[52] See, *Command Vision*, *op. cit*., p. 6. The *Vision* also notes that in form and conduct, the competition in cyberspace is one over initiative, i.e., by sustaining initiative over time through operations that can cumulatively affect relative power, strategic advantage can be realized.

[53] For a chronological list of significant events, see *Center for Strategic and International Studies' Significant Cyber Events List*. https://csis-prod.s3.amazonaws.com/s3fs-public/180308_Significant_Cyber_Events_List.pdf?Szs5ZuZShJAIfgcUXRsvB5T8C76PJR0y

[54] The reference to "within" and "external" is intended to reinforce the notion that, through cyberspace, adversaries are able to secure their own and degrade, usurp, or circumvent others' sources of national power no matter where those sources are located. See, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Government Publishing Office, Washington, D.C.: November 2016), p. 299. https://www.uscc.gov/Annual_Reports/2016-annual-report-congress

[55] Statement *for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community, May 11, 2017*, p. 2. https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

[56] China is said to have been the source of 2015 cyber operations targeting the U.S. Office of Personnel Management and the health care firms Anthem, and Premera and Carefirst Blue Cross. See, *Krebs on Security: Catching Up on the OPM Breach*, https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/, and *Mandiant Consulting: M-Trends 2016* (February 2016).

and the European Union.[57] Finally, it has been concluded with confidence that North Korea, in efforts to mitigate the impact of international economic sanctions, has successfully subverted for significant monetary gain the Society for Worldwide Interbank Financial Telecommunication system (SWIFT).[58] Those funds likely contributed to North Korea's ability to finally cross the nuclear weapons threshold, consequently undermining U.S. military overmatch.

Figure 1 offers a brief summary of a few strategic cyber campaigns over a two-year period characterizing *competitive interaction* (through widening/compounding) and ascribes motivations for the same by advanced persistent threat (APT) groups, groups that are assessed as taking direction from a nation-state. The figure includes a 2014–2016 summary of a few strategically relevant industries, the scale of the threat sources, ascribed objectives for the operations, and malware families.[59] Note that the breadth of the reported industry threats and the objectives for the same cut across military, economic, and diplomatic sources of national power.

Industry	Attack Source	Objective	Malware Families (top three)
Aerospace & Defense	24 APT groups	Acquire intellectual property to advance domestically produced capabilities, develop countermeasures to degrade adversary military overmatch, and produce arms for sale on global market.	47% GhOstRAT 21% PcClient 13% ZXShell
Construction & Engineering	25 APT groups	Acquire intellectual property pertaining to technical innovations, expertise, and processes to develop and advance state-owned firms and to better position those firms for bids against and negotiations with foreign firms.	52% LEOUNCIA 20% LV (aka NJRAT) 13% GhOstRAT
Financial Services & Insurance	15 APT groups	Gain insight into company operations or information on potentially sensitive customers.	34% WITCHCOVEN 22% XtremeRAT 19% GhOstRAT
Government & International Organizations	9 APT groups	Gain an edge in negotiations and agreements.	49% GhOstRAT 30% ERACS 14% PHOTO

[57] Garrett M. Graff, "A Guide to Russia's High Tech Toolbox for Subverting US Democracy," *Wired*, (August 13, 2017). https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/

[58] Sean Lyngaas, "Symantec Traces Swift Banking Hacks to North Korea," *FCW* (May 31, 2016). https://fcw.com/articles/2016/05/31/swift-hack-dprk.aspx

[59] The comprehensiveness of public records of attacks and exploitations is a function of the willingness of targets to report them. Many targets, for various reasons, do not publicly disclose them nor is there a single source detailing the same. That said, general patterns of widening and compounding are still evident in analyses of events that have been reported. The trends data presented in this paragraph are based on industry research reports authored by FireEye Corporation and Mandiant, a FireEye company.

Industry	Attack Source	Objective	Malware Families (top three)
Health Care & Health Insurance	13 APT groups	Acquire PII to facilitate future "insider" cyber operations, assist in the recruitment of human intelligence assets, or identify and monitor persons of interest to the government.	49% WITCHCOVEN 32% XtremeRAT 11% ChinaChopper
Hi Tech & IT	20 APT groups	Acquire economic and technical information to support development of domestic companies through reducing R&D costs.	29% GhOstRAT 26% TAIDOOR 19% POISON IVY

Figure 1. Summary of 2014–2016 Cyber Threats to Industry

A second example of widening is the previously referenced example of Russia's use of cyberspace (through social media, specifically) to undermine the confidence of adversaries' populations and leaders in their democratic institutions and alliances, respectively.[60] Widening, in this campaign, was characterized by micro-targeting at scale within populations.

The conceptual framework of *agreed competition* with interaction dynamics of widening and compounding more accurately describes the cyber operational space of the past two decades. It also can serve as an analytical frame for examining the dynamics that could lead via escalation to conflict and war.

Cyber-enabled Conflict – Deliberate Intensification and Escalation

It is from the point of origin of cyber-enabled crises or war that most cyberspace escalation dynamics scholarship has been written. In this context and as related to the contents of this article, this point is realized when an actor has deliberately escalated from *agreed competition* by threatening to or generating cyber operational effects that are equivalent to armed attack. Escalation, then, is defined as an increase from the level of *agreed competition* to conflict (which would be inclusive of Kahn's definition of an increase in the level of conflict in international relations in crisis situations).[61] In this framework, the mechanism for escalation is *intensification*. Just as Kahn's "ways" of widening and compounding can be adapted to cyberspace, so, too, can his third "way"—intensification. Intensification within cyberspace is characterized by campaigns and/or operations that include increases in frequency (as a function of count over time), duration, damage, and visibility of effects. Intensification may also include expanding cyber operations to other operating domains. Intensification is a necessary condition for escalation, and when the "way" employed causes physical damage, intensification results in an escalatory breakdown of the *agreed competition* space as described in this article. In

[60] Garrett M. Graff, "A Guide to Russia's High Tech Toolbox for Subverting US Democracy," op. cit.

[61] This is a modification of Kahn's definition of escalation to include escalation from *agreed competition*.

what may appear counter-intuitive to conventional wisdom, the more *competitive interaction* occurs within the *agreed competition* space, the more clarity will emerge on the demarcations of illegitimate or legitimate cyber operations and what are outside or within the "rules" of *agreed competition* and thus, may or may not lead to escalation.[62] To help ground the concept of intensification in actual events, a few examples follow.

Intensification through increases in the frequency of effects (through widening and compounding) is found in the Russian campaign targeting Estonia in 2007. On the night of April 26, 2007, Estonian government websites were subject to DoS and DDoS effects. The perpetrator launched 1,000 assaults that day, increasing that number to 2,000 per hour on second day. On May 9, the day marking the peak of the assault, the perpetrator was injecting an average of 4 million packets of data per second. The assaults came in waves, were delivered from up to 85,000 systems, and continued for a 23-day period.[63]

Intensification through physical damage, a breach of the ceiling associated with *agreed competition* and, thereby escalatory, can be illustrated through three cases. In 2008, the Baku–Tbilisi–Ceyhan pipeline near the eastern Turkish city of Erzincan suffered significant damage resulting from a massive explosion. The cyber operation believed to have led to the explosion shut down alarms, cut off communications and super-pressurized the crude oil in the line.[64] In 2010 the deployment of "Stuxnet" caused highly publicized damage to the Natanz Fuel Enrichment Plant.[65] And, in 2014, a report issued by Germany's Federal Office for Information Security revealed that an unnamed steel mill in Germany had suffered "massive," though unspecified, damage when its control systems were manipulated and disrupted to such a degree that a blast furnace could not be properly shut down.[66]

---

[62] There need not be any necessary symmetry to the "rules" nor does *agreed competition* require initial concurrence on what is legitimate or acceptable. There are cyber actions/operations short of war that some states may seek to legitimize/delegitimize, and differing perspectives or initial ambiguity over specific types of operations introduce a potential for intensification short of escalation. "Rules" and conventions, however, will develop over the course of interactions through interactive learning and other forms of signaling, i.e., diplomatic communications. Herman Kahn, *On Escalation*, op. cit., pp. 260–263.

[63] Rebecca Grant, *Victory in Cyberspace*. (Air Force Association Special Report: Washington D.C., October 2007), pp. 5–7.

[64] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg Technology*, 10 December 2014, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blastopened-new-cyberwar

[65] For a comprehensive analysis of "Stuxnet," see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, Crown Publishers, 2014).

[66] The perpetrator infiltrated the corporate network using a spear-phishing attack. Once a foothold was established in one system, the company's networks were explored, resulting in the eventual compromise of a multitude of systems, including industrial components on the production network. See Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, 1 August 2015. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

In the escalation dynamics scholarship referenced in this article, the strategic recommendation for managing deliberate escalation, in cyberspace as well as other domains, is the class of deterrence strategies. But what if such a strategy fails and an adversary deliberately intensifies, to use this article's term, in cyberspace? How can such an action be managed in cyberspace through cyber operations within *agreed competition* and beyond it? The cases cited above hint that managing such intensification and escalation is possible, since in none of the referenced cases does one find extended spirals of increasing intensification or escalation. Rather, what occurred was dissipation or a move back into the *agreed competition* space, respectively, followed by a recommencing of competitive interactions of widening and compounding.

Cyber-enabled Conflict – Managing Deliberate Intensification and Escalation

To begin, let us quickly and briefly set aside the notion that escalation dominance in cyberspace is a viable strategic option. It is not, because dominance is not sustainable in cyberspace given the fluidly contested, and congested nature of the domain. Importantly, there is a distinction, however, between the condition of dominance and the possibility of contested superiority that might be sustained for some period of time. This position has support from both a theoretical/conceptual perspective and an operational one, with the latter stated in USCYBERCOM's *Command Vision*.[67] If cyberspace escalation dominance (or a threat thereof) is not sustainable, what management alternatives remain? The answer lies in the unique characteristics of cyberspace and cyber operations. Note that the discussion that follows applies equally well for managing *inadvertent* as well as *accidental* intensification and escalation in cyber-enabled conflict.

To reiterate, intensification within cyberspace is characterized by campaigns and/or operations that include increases in frequency (as a function of count over time), duration, damage, and visibility of effects. If an adversary chose to escalate from *agreed competition* in cyberspace, i.e., generated effects that caused physical damage, and the target state chose to respond with operations in cyberspace that also caused physical damage, significant escalation should not be assumed. One way to limit the potential for an undesired escalatory spiral to such a response would be to ensure that excessive damage through widening or compounding to unintended targets (collateral damage) was highly unlikely. Bellovin et alia argue that, contrary to conventional wisdom, such

[67] See Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," op. cit., p. 68, Michael Fischerkeller, *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*, op. cit., and *Command Vision*, op. cit., p. 6, where it is argued that cyber escalation dominance is not sustainable and superiority is always at risk. There are those who, nonetheless, refer to cyberspace escalation dominance as a viable strategy. See, Lawrence J. Cavaiola et alia, "Cyber House Rules," op. cit., p. 99.

precise targeting and discrimination are possible (and that we have already witnessed them) and that cyber operations can also be designed to reduce proliferation risks.[68]

An alternative (or complementary) targeting strategy would be to select targets whose destruction, damage, or degradation was visible to only a select audience whereas an alternative *design* strategy could be to allow for damage that is reversible and effects whose frequency and duration could be continuously and actively managed. All three of these operational options could serve to reduce the risk of further deliberate or inadvertent/accidental intensification or escalation.[69] Each will be discussed, in turn.

In certain scenarios, covert cyber operations designed to generate well-directed effects that only leadership are able to detect would send a message of resolve but may also create an environment more conducive to de-intensification and non-escalation, as leadership might be more inclined toward resolution when considerations of public awareness and any associated protestations need not figure in their deliberations.[70] Libicki discusses this aspect of visibility by offering a distinction between making the adversary look powerless versus making the United States look powerful, where the former focuses on making a challenger aware (quietly) of its vulnerabilities and the latter focuses on demonstrating (loudly) U.S. power.[71]

A common, current example of cyber operations that could be designed to allow for reversible damage are those targeting electrical grids. Such operations could be designed to target Industrial Control Systems (ICS) or, specifically, Supervisory Control and Data Acquisition systems (SCADA) and, in essence, hold those systems hostage, and, by extension, the functions those systems support. In such scenarios, states could negotiate demands that must be met in order for system functionality to be restored, or alternatively, face permanent systems damage.[72]

---

[68] Steven M. Bellevin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* (March 2017), 3:1, pp. 59–68.

[69] See, Michael Fischerkeller, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies," op. cit. pp. 120–121 and Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," op. cit., pp. 390–393.

[70] Such considerations in conflict resolution or bargaining scholarship are often referred to as "two-level games." See, for example, Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* (Summer 1988), 42:3, pp. 427–60.

[71] An action could also be selected that serves both objectives simultaneously. See Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica, CA: RAND National Defense Research Institute, 2013).

[72] Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," *Wired* (September 6, 2017); ICF International (US Dept. of Energy Report), *Electric Grid Security and Resiliency: Establishing a Baseline for Adversarial Threats* (June 2016). Note that this either/or proposition cannot be offered via kinetic solutions.

Finally, cyber operations can be designed to be continuously and actively managed, thereby allowing for a constant metering of their effects. This would allow for responsive tuning, for example, of the frequency (count over time) and the duration of effects as a function of adversary behavior. Such active command and control of cyber operations could allow for agile management of cyberspace intensification dynamics as uncertainties regarding adversary intentions, objectives, and capabilities become clearer over time.[73]

Agreed Competition – Inadvertent and Accidental Intensification and Escalation

Recall that *inadvertent* escalation was described as when one party deliberately takes actions that it does not believe are escalatory but which are interpreted as escalatory by another party to the conflict and *accidental* escalation is when some operational action has direct effects that are unintended. In this section, *inadvertent* and *accidental* are considered as modifiers for both intensification and escalation. Regarding the former, misinterpretation may occur because of incomplete information, lack of shared reference frames, or one party's thresholds of which other parties are not aware. When considered in the context of *agreed competition,* cyber operational effects from widening or compounding could inadvertently or accidentally lead to intensification or escalation; however, the existing political context would in large part determine the degree to which the operations were viewed as consequential. In a period of severe crisis between adversaries, for example, inadvertent and/or accidental effects from cyber operations could subsequently lead more likely, in response, to deliberate intensification or escalation by the targeted state. In the previous section, however, several unique characteristics of cyberspace and cyber operations were highlighted that an affected state could leverage to respond in a measured manner and potentially de-intensify or de-escalate the situation. So it is not contradictory to note that while states will increasingly experiment with strategically salient cyber campaigns and operations, they will likely do so risk-informed as they have done over the past decade, in part to manage the potential for inadvertent and accidental effects while the *agreed competition* in this space remains relatively immature. In essence, one can expect the structural incentives and strategic rationales cited previously to compete short of armed attack to affect choices in an environment of unclear operations and encourage care.[74]

---

[73] Note that this reference to command and control differs from that discussed by Morgan et alia and Libicki. Whereas the concern here is with command and control of a specific cyber operation to actively manage escalation dynamics, their references are to the command and control of forces, writ large, to manage against unauthorized cyber operations. Forrest E. Morgan et alia, *Dangerous Thresholds*, op. cit., p. 26 and Martin C. Libicki, *Crisis and Escalation in Cyberspace,* op. cit., pp. 114–119.

[74] Libicki discusses the use of narrative, rather than signaling to manage escalatory dynamics. Such an approach would align with our notion of strategic rationales for why escalation dynamics could be muted. Martin C. Libicki, *Crisis and Escalation in Cyberspace,* op. cit., Chapter 3.

Stability of Agreed Competition

Just as it is critical to distinguish interaction from escalation in cyberspace, it holds logically that engagement should not be defined in and of itself as instability. A question that requires significant study beyond this article is under what conditions could *competitive interaction* involving widening and compounding lead to deliberate intensification and, thus, the destabilization of *agreed competition* short of armed conflict?

States contesting the current international order within the strategic context of *agreed competition* are pursuing strategic cyber campaigns with the objective of generating cumulative degrading effects against adversaries and/or cumulative enhancing effects for themselves. When states seek to gain advantage in, through, and from cyberspace, the dominant dynamic in *agreed competition* is *competitive interaction*. Within the context of long-term *agreed competition*, however, the incentive for intensification could emerge if there were present an enduring and significant imbalance of *persistent engagement* between adversaries leading to a relative shift in power between them or a relative decline of a state across the global distribution of power. This article posits that within the strategic contest of *agreed competition*, such extended or enduring imbalances of competitive outcomes leading to relative power shifts are a necessary condition for instability. Under such a condition, the declining state might see no other option but to break out of the *agreed competition* and use armed attack equivalent operations to reverse the situation. Thus, a sustained loss of relative power would undermine the stability of *agreed competition* short of war. The structural imperative for *persistent engagement*, therefore, produces dynamics toward an equilibrium of stability, since the main objective of this strategic approach is to prevent widening and compounding that can lead to relative power loss. Instability would be a consequence of ineffective or non-existent persistent engagement.[75] Operationally, restraint is structurally encouraged *only when* a particular state gains sustained advantage so as not to create incentives for adversaries to challenge the integrity of the *agreed competition*.

Interaction and Escalation Metaphors for Cyberspace

Kahn noted that metaphors can be useful but have their limitations and took that perspective of his own metaphor of a ladder. But the escalation ladder took hold and one rarely can mention escalation without thinking about rungs. The arguments presented in this article suggest that a ladder is not well suited as a metaphor for building a model of potential cyberspace interaction dynamics and escalation. There are two reasons for this

[75] Relative power loss can occur outside the agreed competition of cyber operations short of armed attack and also cause states to consider intensification or escalation through cyber means as an option. One might consider the use of code against Iranian centrifuges as such an example.

conclusion. First, it has been offered that today's strategic environment is considered to be a long-term, strategic competition in which states will pursue their national interests short of war. The *agreed competition* in cyberspace, in particular, is, similarly, characterized by operations that generate effects short of armed conflict equivalence. In this strategic space, *competitive interaction* will be the predominant cyberspace dynamic as states seek to gain advantage. This dynamic is more analogous to grappling, because grappling most often refers to competitions in which competitors seek to gain advantage through constant engagement that is short of violence.

Second, should a state deliberately choose intensification and challenge the integrity of *agreed competition*, cyberspace intensification dynamics and escalation are unlikely to be as straightforward as an ascending ladder. Libicki offers a modification of the ladder metaphor by arguing that escalation in cyberwar—particularly cyber against cyber—is likely to be jerky rather than smooth. What may look like a carefully calibrated ladder could, in practice, end up as a hodgepodge of sticky and bouncy rungs, where sticky rungs are those from which one cannot rise and bouncy rungs are those from which one rises much farther than anticipated.[76] This has some salience given the lack of states' experiences in cyber-enabled conflict and the uncertainty that is a consequence of the same. However, awareness of that uncertainty demands a consideration of how best it can be managed. It was argued in the previous sections that cyberspace and cyber operations offer opportunities for managing intensification and escalation risks associated with those uncertainties. Operations that intensify or escalate but are designed to allow for the metering of effects and/or reversible damage, for example, take account of the uncertainty the target state may have regarding another's intentions and, therefore, facilitate de-intensification or de-escalation.[77] But the notion of rungs still implies a linearity biased toward intensification that we have not witnessed to date in the widening and compounding interaction dynamics of cyber operations and campaigns.

Grappling and effects management (through persistent engagement, for example) in *agreed competition* or beyond it may lead to "movements" up, down, and sideways. This *competitive interaction* may be best visualized and conceptualized as the Penrose Stairs, represented most famously in M.C. Escher's 1960 lithograph entitled *Ascending and Descending*. Experience over time might help clarify whether one is going up, down, or sideways, but cyber interactions may not be straightforward in any of those three directions consistently. As an interactive space populated by many actors with many

---

[76] Martin C. Libicki, *Crisis and Escalation in Cyberspace,* op cit., p. 120.

[77] While these types of operations share the same strategic objective of the massively destructive operations associated with the Russia's strategic concept of escalating to de-escalate, they do not share the same destructive result. See, Joshua Stowell, "The Problem with Russia's Nuclear Weapons Doctrine," *Global Security* (February 13, 2018). https://globalsecurityreview.com/nuclear-de-escalation-russias-deterrence-strategy/

interests, any single cyber operation will be interaction-specific. Penrose's stairs, rather than Kahn's ladder, is the better visualization of this competitive and dynamic space.

Conclusion

Several years ago U.S. adversaries waded cautiously but strategically into the strategic competitive space between war and peace, perhaps most fulsomely in cyberspace. Adversaries are now pursuing aggressive strategic campaigns in, through, and from cyberspace to gain strategic advantage in military, economic, and diplomatic arenas. As evidenced in recent U.S. strategic guidance, the United States has recognized that it must operate persistently in this space, as well, if it hopes to re-gain the upper hand on adversaries who have been reaping the benefits of their early strategic adaptation to cyberspace at the expense of U.S. national interests. Over the past eight years, USCYBERCOM has been both observing adversarial behavior and *learning* from it, resulting in the prescription of a new strategic approach to arrest adversary gains and secure and advance U.S. interests in cyberspace—*operational persistence/engagement.*

A recurrent concern among policymakers and security studies scholars is that any proactive posture in cyberspace taken by the United States will result in uncontrollable and quickly spiraling escalation. Classic and current escalation dynamics scholarship focuses almost entirely on this escalation dynamic, doing so from the same launching point of policymakers, i.e., a *potential, episodic* conflict (or threat thereof). This context is an extremely narrow focus, and the scholarship to date addressing it, while capable of informing the understanding of cyberspace escalation dynamics within that narrow context, still falls short by not taking into account the potential for targeting strategies that reduce the risk of escalation (target discrimination and/or visibility) and cyber operations design strategies that allow for reversible damage and active management of operational effects. Incorporating these considerations into the existing body of cyberspace escalation scholarship would mark only an incremental improvement in knowledge, however, because it ignores cyberspace *interaction* dynamics within the context of the current strategic environment—an *actual, on-going*, long-term strategic competition occurring below the armed attack threshold. Moreover, it doesn't consider the potential impact of the manner in which the *agreed competition* can be managed for advantage—a strategic approach of *persistent engagement*.

Herman Kahn's *On Escalation*, the veritable gift that keeps on giving, included a brief, albeit largely unexplored reference to a second class of strategies for managing escalation in *agreed battle* (what was adapted in this article for cyberspace to be *competition)*, i.e., strategies that would make use of the factors relating to particular levels of escalation in order to gain an advantage. U.S. strategic guidance identifies a "particular level of escalation" that characterizes the on-going long-term competition—the threshold of armed attack—and this article offers both country-specific and general

pattern analyses of adversary cyber operations that support that characterization. In the context of *agreed competition,* it was argued *competitive interaction* is the dominant dynamic that would occur as states seek to gain strategic advantage in this competition. It follows, then, that the class of strategies best suited for managing interaction dynamics in *agreed competition* would be that which counters or contests competitive interaction. As was noted, a strategic approach of *persistent engagement* is well-suited for securing and advancing national interests in this *agreed competition* and as such populates Kahn's second class.

The arguments and analysis offered in this article lead to a conclusion that sustained, robust competition should be expected (and is occurring) in cyberspace in an *agreed competition* and that *competitive interaction* is currently and will continue to be the dominant interaction dynamic *whether or not* the United States, in particular, adopts a strategic approach of *persistent engagement*. As stated previously, interaction, persistent or not, is not *ipso facto* escalation. In fact there are forms of persistent engagement, if pursued strategically, that could lead not only to operational de-escalation—reduced widening, compounding, and intensification—but over time clarify what can be regarded within the rules of an increasingly stabilizing *agreed competition.* Agreement to compete robustly short of armed conflict may be the grand strategic consequence of cyberspace—a different form of national security challenge of consequence that will require not just persistent engagement, but persistent study.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-05-18	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller, Richard J. Harknett	C5191
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-9076

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 4850 Mark Center Dr., Alexandria, VA 22311	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

A significant concern among policymakers and academics discussing cyber operations is a fear of escalation should states adopt a more proactive posture in cyberspace. Past policy statements and international security scholarship tend to focus narrowly on the escalation dynamics resulting from cyberattacks, or the threat thereof, that might cause physical damage or loss of life. This limited focus on *potential and episodic* cyber-enabled crises or war scenarios excludes an equally, if not more important, strategic space—*actual and continuous* strategic competition in cyberspace that does not reach the level of armed conflict. In 2018, U.S. strategic guidance found in the *National Security Strategy of the United States of America* shifted to emphasize the significance of this competitive space, and United States Cyber Command (USCYBERCOM) prescribed a strategic approach of *persistent engagement* to contest and counter the ability of adversaries to gain strategic advantage without engaging in armed attack. This article considers this shift in U.S guidance documents and analyzes the potential interaction dynamics in a cyber strategic environment structured by interconnectedness-constant contact-persistent engagement. In so doing, it introduces a distinction between interaction and escalation dynamics, one based on a 21st century adaptation of Herman Kahn's *On Escalation*. It is concluded that fears are not warranted that persistent engagement in cyberspace will result in spiraling or uncontrollable escalation.

15. SUBJECT TERMS

Cyberspace, strategy, escalation, agreed competition

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	23	19b. TELEPHONE NUMBER (Include Area Code)