INSTITUTE FOR DEFENSE ANALYSES

Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition

Michael P. Fischerkeller

November 2018

Approved for public release; distribution is unlimited.

IDA Non-Standard
NS D-9282

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

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task C5107, "Arriving at the Limits and Boundary Conditions of Cyberspace's Agreed Competition," for IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgment

I would like to acknowledge and express gratitude for the thoughtful review of and comments on this manuscript by Dr. Richard Harknett and Chris Pavlak.

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

Copyright Notice

© 2018 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

Persistent Engagement and Tacit Bargaining:

A Strategic Framework for Norms Development in Cyberspace's *Agreed Competition*

Michael P. Fischerkeller – Institute for Defense Analyses

Abstract

Interactions in the strategic competitive space below the threshold of armed conflict in the cyberspace strategic environment represent an *agreed competition*, a structure and dynamic characterized by actors seeking to gain strategic advantage through cyber campaigns/operations. This strategic competitive space is still maturing, however, and the potential exists for differing perspectives, ambiguity, or uncertainty over specific types of "acceptable" campaigns/operations short of armed conflict that could lead to unintended or non-deliberate escalation out of *agreed competition*. It is imperative, then, that a strategic process be identified through which states, without escalating to armed conflict, can arrive at understandings of acceptable behavior, expressed in this article as boundary conditions of *agreed competition* but more routinely called *cyber norms*. Thomas Schelling invested considerable time studying this same conceptual problem, and this article applies his scholarship on informal agreements and tacit bargaining to the cyberspace strategic environment and *agreed competition.* It is concluded that the process of tacit bargaining is well-suited for the challenge of developing cyber norms in *agreed competition* – a *strategy of persistent engagement* supports that process – but additional U.S. policy guidance is needed to both facilitate its implementation and increase the likelihood of its success.

Background

U.S. strategic guidance states that a consequence of the cyberspace strategic environment is a new strategic competition, one characterized primarily by states seeking to alter the international balance of power by cumulating strategic advantage through persistent cyber campaigns/operations below the threshold of armed conflict.[1] Such campaigns/operations are designed to target adversaries' sources of national power with the intent to degrade, usurp, or circumvent the same. In February 2018, United States Cyber Command (USCYBERCOM) published its *Command Vision* and argued that a new strategic approach – *persistent engagement* – was required to enable the United States to compete effectively in this new strategic competitive space. More recently, this was reiterated as strategic guidance in the 2018

[1] 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; and *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority* (United States Cyber Command, 2018). *Summary: Department of Defense Cyber Strategy* (Department of Defense, 2018), p. 2.

Department of Defense Cyber Strategy.[2] In an exploration of the potential impact this strategy could have on cyberspace interaction dynamics and escalation, it has been reasoned that this strategic contest below the threshold of armed conflict was well-described as an *agreed competition*, a concept derived from Herman Kahn's *agreed battle* and similarly rooted in factors relating to particular levels of escalation. Kahn 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 conscious quid pro quo arrangement."[3] He further notes that states can come to recognize through interactions "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."[4]

There are two aspects to ensuring the integrity of an *agreed competition*.[5] The first is to maintain enough stability in the international balance of power so that no competitor feels compelled or tempted to escalate out of *agreed competition* into armed conflict. Within the context of long-term *agreed competition*, the need or temptation to escalate to armed conflict could manifest if an enduring and significant imbalance of persistent engagement outcomes emerged, leading to a relative shift in power between adversaries or a relative decline of a state across the global distribution of power. Indeed, it has been argued that such extended or enduring imbalances are a necessary condition for instability.[6] Under such a condition, the declining state might see no other option but to escalate out of *agreed competition* and use armed attack-equivalent operations to reverse its decline.[7] This suggests that, operationally, restraint is structurally encouraged when a particular state gains sustained advantage so as not to create incentives for adversaries to challenge the integrity of an *agreed competition*.

The second aspect, and the emphasis of this article, is for competitors to arrive at understandings of and agreements on focal points and boundary conditions of *agreed competition*, more routinely referred to as cyber norms. In this article, a focal point is defined as a determining differentia – a feature, factor, or convention – around which attention/interest converges in *agreed competition* and a boundary condition is the range of acceptable/unacceptable behaviors about which actors have converged for a focal point. Or,

---

[2] *Command Vision for U.S. Cyber Command, op. cit.* and *Summary: Department of Defense Cyber Strategy, op. cit.*

[3] Herman Kahn, (with a new introduction by Thomas C. Schelling), *On Escalation: Metaphors and Scenarios (Routledge: London, 2017)*, fn 4, p. 3. Kahn attributes this term to Max Singer.

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

[5] This same argument was made within the context of limited war by Thomas Schelling and Morton Halperin. See Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control* (Elsevier Science Ltd: Amsterdam, 1985 (Reprint, first published in 1975)), p. 30.

[6] For a more complete discussion of this aspect, see Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation* (Institute for Defense Analyses, 2018).

[7] Relative power loss can also occur outside the *agreed competition* and cause states to consider escalation out of *agreed competition* as a response. One might consider the use of code against Iranian centrifuges as such an example.

stated more simply, together they represent mutual understandings of acceptable/unacceptable behavior in *agreed competition* (or, even more simply, cyber norms).[8]

Although it has been proposed that the superordinate focal point and boundary condition of *agreed competition* appears to be a prohibition against crossing the threshold of armed conflict,[9] the overall strategic competitive space is still maturing and, consequently, the potential exists for some states to seek to legitimize significantly disruptive cyber actions/operations short of armed conflict-equivalence.[10] Moreover, even for states continuing to operationally explore this competitive space with benign objectives, differing perspectives, ambiguity, or uncertainty over specific types of "acceptable" campaigns/operations introduce avenues for unintended or non-deliberate escalation out of *agreed competition*. Such eruptions could potentially destabilize the overall strategic environment as states struggle to identify and communicate a new superordinate focal point and boundary condition in time to check the escalation of conflict.[11] To address these concerns, there is a need for a strategic process through which adversaries, without escalating to armed conflict, can increase clarity and reduce uncertainty regarding understandings of acceptable/unacceptable behavior in *agreed competition* – this is the primary motivation for and objective of this article. Kahn argues that states can come to recognize what are and are not acceptable behaviors but does not offer insights into how such understandings actually come about. Thomas Schelling, however, explores this issue in depth in his scholarship on informal agreements and tacit bargaining. We argue that his work supports a compelling case for adopting a strategic process of tacit bargaining to support the development of cyber norms that could bring further stability to *agreed competition*.

The first section of this article argues that, although much of the Schelling's seminal scholarship is from 50 or more years ago, it is, nonetheless, quite relevant for consideration in the cyberspace strategic environment and *agreed competition*. This is followed by a section reviewing two foci of Schelling's research addressing processes by which states can arrive at mutual understandings of acceptable/unacceptable behaviors – informal agreements and tacit bargaining – in spite of strategic features and factors that may inhibit traditional, formal approaches to so doing. This review highlights that adversaries can, in fact, come to understandings of and agreements on acceptable/unacceptable behaviors in such challenging

---

[8] Schelling describes a focal point as "a clue for coordinating behavior, some point for each actor's expectation of what the others expect him to be expected to do." Described as such, a focal point for Schelling could be a determining differentia, a range of behavior, or a combination of both around which actors converge (through interest and/or behavior). Further, in his application of the concept to arms control and limited war, he often uses the terms *limit* and *focal point* synonymously. It is Schelling's logic in the application of these terms that this article finds valuable, rather than the terms themselves. This article finds it analytically useful to formally deconstruct focal point to consistently keep separate the notions of a determining differentia (focal point) and ranges of behavior (boundary conditions). Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press: Cambridge, MA, 1960), p. 57.

[9] This serves an example of a focal point based on a convention.

[10] See, Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation, op. cit.*, and James A. Lewis, *Rethinking Cyber Security: Strategy, Mass Effects, and States* (Center for Strategic and International Studies, January 2018), specifically, Chapter 4, "Cyber Operations and Interstate Conflict," and Chapter 5, "Political and Strategic Constraints on Cyber Attack".

[11] Thomas C. Schelling, *The Strategy of Conflict, op. cit.*, p. 77.

environments, and it supports an argument that tacit bargaining is a strategic process well-aligned with the cyber strategic environment and *agreed competition*. The next section addresses a practical challenge of adopting this strategic process by introducing what considerations adversaries must take into account to increase their likelihood of contributing positively to the collaborative tacit process of arriving at understandings on what are acceptable/unacceptable behaviors in *agreed competition.* This is followed by an evaluation of how well the United States is presently postured to support a process of tacit bargaining process toward that end. The evaluation is approached from two vectors: first, determining if the U.S. has in place a strategic approach to cyberspace that supports this process, and second, determining if it has established any policy guidance that supports the same. The final section offers exemplars of focal points and boundary conditions and other factors for U.S. policymakers to consider as they strive to increase clarity and reduce uncertainty with adversaries regarding the boundary conditions of acceptable/unacceptable behavior in *agreed competition*.

The Relevance of Schelling's Scholarship

The Strategic Environment, Then and Now

In 1960, Thomas Schelling recognized that even in environments of uncertainty concerning new military technology and deep mutual distrust, states nonetheless have a common interest in avoiding the kind of false alarm, panic, misunderstanding, or loss of control that may lead to unintended or non-deliberate escalation.[12] They also have a common interest in not getting drawn or provoked or panicked into war by the actions of other parties (whether a party intends that result or not).[13] And they may have an interest in saving some resources by not doing things that tend to cancel out. Importantly, these common interests do not depend on trust or good faith. "In fact," he argues, "it seems likely that unless thoroughgoing distrust can be acknowledged on all sides, it may be hard to reach any real understanding on the subject."[14] Similarly, "The intellectual clarity required to recognize the nature of the common interest may be incompatible with the pretense that all parties trust each other, or that there is any sequence of activities in the short run by which any side could demonstrate its good faith to the other."[15] These strategic realities motivated Schelling to consider an alternative process (to explicit bargaining) by which strategic stability between states could be arrived at or sustained in such an environment, leading him to introduce and develop the distinction between tacit and explicit bargaining.[16]

While obviously not referring to the cyberspace strategic environment in his work, the applicability of his arguments seems clear, as all of his arguments regarding military technology

[12] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *Daedalus* 89:4 (Fall 1960), pp. 892–914.

[13] This has been referred to as "catalytic" escalation in cyberspace. See Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* (Fall 2012), pp. 46–70.

[14] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *op. cit*., pp. 894–895.

[15] Ibid.

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

have been presented as challenges posed by the cyberspace strategic environment. Cyberspace has compressed the time available to make decisions, induced concerns that an armed conflict either could be or would be limited in scope, and has greatly reduced any actor's confidence that it can predict the capabilities any adversary had or would have in the future.[17] Indeed, cyberspace's unique structural feature of interconnectedness and the condition of constant contact that is its consequence significantly exacerbates each and every one of these challenges.[18] In addition, it is not a stretch to argue the significant distrust Schelling discussed in characterizing the U.S.-Soviet relationship is present today in bi-lateral or multi-lateral relations between the United States and Russia, China, Iran, and the Democratic People's Republic of Korea (DPRK), to name a few of the acknowledged advanced persistent threats (APTs) challenging the United States in, through, and from cyberspace.[19] Finally, it is equally defensible to argue that the mutual or common interests Schelling highlights are also present today in the cyberspace strategic environment. Thus, though published at the dawn of the digital age, Schelling's scholarship on informal agreements and tacit bargaining, motivated by the strategic environment of that time, is strikingly relevant to today's cyber strategic environment and *agreed competition*.

An Imperative for Collaboration, Then and Now

Schelling concluded that the dangerous technological and distrustful international political environment of the 1950s made imperative the pursuit of collaboration with adversaries (and potential adversaries) to reduce the likelihood of armed conflict and ensure strategic stability.[20] He noted further it was an area worth exploring because contemporary military policies and prospects could not promise security. Scholars and policymakers have expressed similar skepticism of the comprehensive effectiveness of what, until very recently, has been the

---

[17] See, for example, Defense Science Board, Resilient *Military Systems and the Advanced Cyber Threat, Task Force Report* (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January 2013); David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* (2014), 56:4, 7–22; James N. Miller, Jr. and Richard Fontaine, *A New Era in U.S.-Russian Strategic Stability* (Center for New American Security, 2017), pp. 16-18, and Defense Science Board, *Cyber Deterrence, Task Force Report* (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2017).

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

[19] Danial R. Coats, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community* (13 February 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[20] Schelling and Halperin noted that "… a situation in which the incentives on both sides to initiate war are outweighed by the disincentives is described as 'stable' when political events (internal or external to the countries involved), technological change, accidents, false alarms, misunderstandings, crises, limited wars, or changes in the intelligence available to both sides, are unlikely to disturb the incentives sufficiently to make mutual deterrence fail", Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control*, *op. cit*., p. 50. As deterrence is not descriptive of the strategic dynamic of *agreed competition*, for this article, the definition is modified to read "… a situation in which the incentives on both sides to initiate war are outweighed by the disincentives is described as 'stable' when … [factors] … are unlikely to disturb the incentives sufficiently *to encourage an actor to escalate out of agreed competition into armed conflict*."

dominant security approach to the cyberspace strategic environment and *agreed competition*, one largely founded on a strategy of deterrence and the process of explicit bargaining.[21] Today, just as it was in the 1960s, it is imperative that an alternative or complementary strategic approach and supporting process facilitating collaboration be pursued to reduce the likelihood of states escalating out of *agreed competition* into armed conflict.

As noted earlier in this article, it has now been recognized and accepted that a strategic approach of *persistent engagement* is better suited for protecting and advancing U.S. interests in *agreed competition* than is a strategy of deterrence.[22] This serves as evidence of a positive step in a corrective direction. There is another bedrock conceptual frame that needs reorientation, however, if U.S. national interests (and global interests for that matter) are to be attained. Across the past four U.S. administrations, the idea of *establishing* cyber norms as an essential element to stabilize cyberspace has become close to a dogma.[23] This perspective dominates the academic literature, as well.[24] The core idea is finding consensus among "like-minded" states about acceptable and unacceptable cyber behavior, articulating that standard, and then working to convince other states to abide by that "norm." Unfortunately, just as a strategy of deterrence is not aligned with the unique structural and operational characteristics comprising the cyber strategic competitive space, neither is this traditional process of explicit bargaining. If the United States is eventually to attain greater stability within cyberspace, it requires a policy better aligned to the behavioral realities within the environment.

As has been argued regarding deterrence, this is not a proposal to completely abandon traditional approaches, but rather a call for an aligned application of them to the strategic realities the United States is attempting to manage. So, it is important to note that the U.S. has achieved some progress through explicit bargaining on agreements of principles of "responsible" state

---

[21] See, for example, Michael Sulmeyer, "How the U.S. Can Play Cyber Offense: Deterrence Isn't Enough", *Foreign Affairs*, 22 March 2018, https://www.belfercenter.org/publication/how-us-can-play-cyber-offense-0, Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace", *op. cit.*, and *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 and *Summary: Department of Defense Cyber Strategy*, *op. cit.*

[22] *Command Vision for U.S. Cyber Command*, *op. cit*.. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace", *op. cit*., and Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*, *op. cit*., *Summary: Department of Defense Cyber Strategy*, *op. cit.*

[23] See, for example, *The National Strategy to Secure Cyberspace, 2003* (The White House: Washington, D.C., 2013), pp. 50-51, *International Strategy for Cyberspace, 2011* (The White House: Washington, D.C., 2011), p., 9, and *National Cyber Strategy of the United States of America, 2018* (The White House: Washington, D.C., 2018), p. 20.

[24] This perspective was recently reiterated by Michelle Flournoy and Michael Sulmeyer, "A Plan for Securing Cyberspace", *Foreign Affairs* (September/October 2018), https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet and Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain, *Strategic Studies Quarterly* (Fall 2018), https://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf.

behavior in cyberspace; however, it has only been in the strategic space of armed conflict.[25] The 2015 G20 Leader's Communique and 2017 G7 declaration on "responsible" behavior are notable successes.[26] However, such non-binding agreements are with like-minded states, and so, by definition, are not recognized as legitimate by U.S. adversaries. The 2013 and 2015 United Nations Group of Governmental Experts (UN GGE) on Information Security Reports represented initial international progress on recognizing appropriate bodies of law and suggesting voluntary norms, but progress stalled at the 2017 convention.[27] Indeed, after the 2017 meeting, the U.S. posited that the realization of cyber norms may not be achievable through a United Nations effort and that other approaches must be considered.[28]

To note the limited progress of this negotiation approach is not to discourage explicit bargaining efforts in pursuit of formal agreements on responsible behavior in the strategic space of armed conflict. However, the U.S. must be sober in assessing the likelihood of realization, effectiveness, and depth of potential reach. Regarding the former, U.S. adversaries have routinely rejected any substantive agreements on cyber norms. Regarding the latter two, consider, for example, the most significant explicit, bi-lateral diplomatic agreement to-date with China that reached into *agreed competition.* In 2015, Presidents Obama and Xi committed that neither country would conduct or knowingly support cyber-enabled theft of intellectual property for commercial gain.[29] Subsequent evidence, however, suggests that operatives based in China sustained cyber espionage campaigns exploiting the business secrets and intellectual property of American businesses, universities, and defense industries.[30] This explicit agreement failed not because of any deficit in U.S. diplomatic bargaining skills, rather, it failed (we will argue) because the bargaining process itself was not appropriate for the strategic competitive space to which it was applied.

The challenge faced by the United States and its allies and partners, then, is to identity an alternative or complementary strategic process through which it can develop a *modus vivendi* in *agreed competition* with those who either cannot or will not negotiate explicitly or, even if they

---

[25] This strategic space comprises any cyber operation generating an effect equivalent with a "use of force" or "armed attack" but not those cyber operations that generate effects in the strategic competitive space below the level of armed conflict.

[26] See, http://www.g20.utoronto.ca/2015/151116-communique.pdf and https://www.mofa.go.jp/files/000246367.pdf, respectively.

[27] See, http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html, and https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well, respectively.

[28] See, https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

[29] See, *FACT SHEET: President Xi Jinping's State Visit to the United States* (The White House, September 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[30] See, for example, *Foreign Economic Espionage in Cyberspace 2018* (National Counterintelligence and Security Center: Washington, D.C., 2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf and https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf

did, none would trust the others with respect to any agreement explicitly reached.[31] The United States has faced a similar challenge, however; one which motivated Schelling to explore the role of informal agreements and tacit bargaining in arms control and limited war. In the next section, his work in those areas is first reviewed and then considered within the context of the cyber strategic environment and *agreed competition*.

Informal Agreements and Tacit Bargaining

Arms Control

Schelling initiates his exploration into the concept of informal agreements by, perhaps counterintuitively, focusing on war itself rather than its prospect. He notes that "It is interesting that cooperation between potential enemies in reaching agreed limits and restraints in case of war may be less dependent on any 'outcome' of negotiations than simply on the negotiations themselves." And that "Negotiations may be too strong a word here, since the pertinent communications need not be formalized, institutionalized, or even recognized as negotiation." He concludes that in reaching shared expectations with an adversary about conduct in wartime, "it is the understanding that matters, not the instrument (if any) in which the understanding is expressed."[32] Schelling considers this insight an important clue to a process by which arms control may be reached and to the kinds of arms control that could be reached by that process. He argues that "Maybe arms control is destined to be something more informal than is suggested by the great diplomatic deployments in Geneva. Maybe limited measures of arms control can be arrived at by quite indirect and incomplete communication; maybe they will take the form of a proposal embodied in unilateral action (or abstention from action) which continues if matched by corresponding action on the other side and only for so long as it is. Maybe instead of arguing about what we should do, we will simply do it and dare the other side to do likewise, or do it and quietly suggest that we would like to keep it up, but only if they find it in their interest to do something comparable."[33]

In support of this perspective, Schelling offers examples of tacit, informal arms understandings between the United States and the Soviet Union, concluding that, in general, it appeared such understandings concerned what the United States did with its weapons more than what it possessed. For example, there seemed to have been some understandings about traffic rules for patrolling bombers; there were certain lines the United States stayed on "this side" of, lines the Soviets presumably could recognize and the crossing of which they could probably monitor to some extent. This was a restraint that the United States unilaterally observed in the interest of reducing misunderstandings and alarms. Schelling claimed (to the best of his knowledge) that the traffic rules "were communicated, not explicitly, but simply by behaving in accordance with them (perhaps conspicuously in accordance with them) and possibly by having

[31] Thomas C. Schelling, "Bargaining, Communication and Limited War", *Negotiation and Conflict Management Research* (2008), 1:2, pp. 198-217

[32] Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control*, *op. cit.*, p. 23.

[33] Ibid.

chosen the dividing lines in such a way that their significance is recognizable."[34] In addition, the United States and Soviet Union both abstained from harassing actions on each other's strategic forces: They did not jam each other's military communications, put at risk each other's populations with fallout from weapons tests, or wage surreptitious peacetime undersea wars of attrition.[35] Strategic and operational maneuver, not explicit bargaining through diplomatic exchange, was the dominant form of communication that led to these understandings.

Limited War

Schelling applies the same reasoning to the context of limited war by arguing that "In fact, all of the tacitly agreed limits that do apply, or may apply, in limited war can be construed as a kind of informal arms control tacitly arrived at."[36] And, he notes, that although agreements on limits are difficult to reach – not only because of the uncertainties and the acute divergence of interests but because negotiation is severely inhibited both during war and in crises – such agreements nonetheless have occurred.[37] Most of those agreed limits, he claims, have historically been arbitrary, conventional, and purely matters of tradition and precedent – and thus uncertain and insecure. Nobody was even nominally committed to honor them, *and yet they were honored*. Thus, he concludes, they demonstrated it is possible for adversaries to arrive tacitly, or by indirect communication through strategic maneuver, at an understanding about some rules and about how to interpret intentions through the way one operates and deploys his resources. Tacit bargaining, then – bargaining in which communication is absent or impossible – assumes significant importance in connection with limited war, or, for that matter, "with limited competition, jurisdictional maneuvers, jockeying in a traffic jam, or getting along with a neighbor that one does not speak to."[38]

Perhaps Schelling's most important conclusion in this regard is that "the limits that can be observed in limited war are a powerful demonstration that sheer self-interest – the recognition of a need to collaborate with an enemy in wartime to reach understandings that transcend the formalities of explicit communication; the recognition of a mutual interest in avoiding accidents, incidents, misunderstandings, and unnecessary alarms and in holding to any constraints that can be found – can provide potent sanctions that need not rest on explicit negotiation and formal agreements."[39]

The Importance of Action and Interaction

[34] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *op. cit*., p. 900.

[35] Ibid., p. 901.

[36] Ibid., p. 904.

[37] Thomas C. Schelling, *The Strategy of Conflict, op. cit.*, p. 53.

[38] Ibid.

[39] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *op. cit*., p. 904.

Schelling argues that in both arms control and limited war the role of action and interaction deserves special emphasis in tacit bargaining. For example, the limits in limited war, he observed, are arrived at "not by verbal bargaining, but by maneuver, by actions, and by statements and declarations that are not direct communication to the enemy. Each side tends to act in some kind of recognizable pattern, so that any limits that it is actually observing can be appreciated by the enemy; and each tries to perceive what restraints the other is observing."[40] Stated differently, increased clarity and reduced uncertainty regarding limits, and the predictably and potential stability they engender, are a consequence of action and interaction.[41] Actions and interactions, therefore, are critical in tacit bargaining and substantially contribute to the collaborative process of arriving at understandings on limits.

Salience to the Cyberspace Strategic Environment and Agreed Competition

As a reminder, the primary motivation for and objective of this article is to identify an effective process through which adversaries can increase clarity and reduce uncertainty regarding understandings of acceptable/unacceptable behavior in *agreed competition*. To be clear, this article is not endorsing the notion that arms control in cyberspace is likely to be an effective process toward that end.[42] Nor does this article equate the substance of limited war (the strategic space of armed conflict) with *agreed competition* (strategic competition below the threshold of armed conflict). That said, three important findings from Schelling's work in these areas can contribute to this article's objective:

- informal agreements between adversaries that contribute to stability can be arrived at through mechanisms other than formal bargaining processes;
- in arriving at such informal agreements, understandings and shared expectations may more likely converge around what one does with weapons (capabilities) rather than what weapons (capabilities) one possesses;
- and, (informal) understandings around what one does and does not do (i.e., focal points and boundary conditions) in arms, control, limited war, or even limited competition are arrived at not through verbal bargaining, but through tacit bargaining characterized by action and interaction (e.g., deploying resources and strategic maneuvering).

Regarding the first finding, Schelling concludes that in challenging strategic environments, such as contemporary cyberspace, where mutual, common interests are

[40] Ibid.

[41] This argument is consistent with that made by Fischerkeller and Harknett for the strategic competitive space of *agreed competition*, i.e., action and interaction does not *ipso facto* equate with escalation. See, Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation, op. cit.*, …

[42] For arguments that formal arms control agreements cannot be reached in cyberspace, see Erica D. Borghard and Shawn W. Lonergan, "Why Are There No Cyber Arms Control Agreements?", https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements and Defense Science Board, *Cyber Deterrence, Task Force Report, op. cit.* p. 8.

nonetheless present among and between adversaries, there are potentially effective alternatives to explicit bargaining for developing understandings and norms of behavior. Interestingly, in the preface to the reprint of *Strategy and Arms Control*, authored 25 years after the publication of Schelling's *Daedalus* article on informal agreements, Schelling and Halperin lament that informal understandings seem to have taken a back seat to the quest for formal agreements. Although they support and applaud explicit bargaining efforts that arrive at such agreements, they remain convinced that other processes may often be more effective in pursuing the same goals.[43]

Regarding the second and third findings, a tacit bargaining process diverges from explicit bargaining in that informal agreements are arrived at through operational engagement, maneuver, and/or restraint. Stated differently, increased clarity and reduced uncertainty regarding boundaries or limits on behaviors, and the predictably and potential stability they engender, are a consequence of action and interaction. A strategic process of tacit bargaining, then, would be supported by structural features that facilitate action and interaction between adversaries. The cyberspace strategic environment's structural feature of interconnectedness not only facilitates action and interaction, it demands it of any state seeking to secure its national interests in the cyberspace strategic environment.[44] Thus, tacit bargaining is a strategic process that is structurally aligned with and supported by the cyberspace strategic environment.

In efforts to arrive at tacit understandings of acceptable/unacceptable behavior in *agreed competition*, the tasks states face will be a function of the alignment of their national interests with mutual or common interests as manifested in cyberspace. Where those interests converge, states should engage in cyber behaviors around those cyber focal points that communicate shared interests and a willingness to collaborate on ranges of acceptable/unacceptable behavior about those interests. Where those interests are in conflict, states will communicate as much through cyber behaviors seeking to outmaneuver each other to achieve an advantage, or at least avoid a disadvantage.[45] Such communication is, literally, easier said than done through non-verbal action and interaction; a challenge states face in the tacit bargaining process is ensuring that such communications are understood. Schelling recognized this challenge, and the next section presents his observations and guidance on what considerations adversaries should take into account to increase their likelihood of contributing positively to the collaborative tacit process of arriving at understandings on what is acceptable/unacceptable behavior.

Arriving at Understandings on Focal Points and Boundary Conditions

[43] Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control, op. cit.*, p. xiii.

[44] Farrell and Glaser also considered the potential role of focal points in cyber strategy, but they focused on the strategic space of armed conflict rather than agreed competition (the strategic space below armed conflict). See Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliency and Norms in US Cyberwar Doctrine", *Journal of Cybersecurity*, 3(1), 2017, 7-17.

[45] Edward J. Lawler and Rebecca Ford, "Bargaining and Influence in Conflict Situations" in K.S. Cook, G.A. Fine, and J.S. House (eds.), *Sociological Perspectives on Social Psychology* (Allyn & Bacon: Needham Heights, MA, 1995), pp. 236-256, p. 238.

Schelling maintains that because understandings regarding focal points and boundary conditions are arrived at through action and interaction, increasing their likelihood of being mutually understood requires adversaries ensuring they possess attributes of a certain nature and character. When adversaries seek to informally communicate and arrive at understandings that align with their interests, Schelling refers to this class of focal points and boundary conditions as being *preference-informed*. He further proposes a distinction between preference-informed and problem-informed and also raises the issues of potential asymmetries and dynamism.[46] Each of these is discussed, in turn.

Preference-informed

In order to increase the likelihood of successful tacit bargaining, in their *nature* focal points and boundary conditions must be clear cut; must have simplicity; must involve all-or-none distinctions or across-the-board distinctions like that between land and water, between material and manpower, between two sides of a border, or even some arbitrary but potent suggestive feature like a parallel of latitude; and must be based on qualitative distinctions rather than matters of degree.[47] It is worth quoting Schelling at length where he gives special attention to the latter when considering atomic weapons' use in limited war.

> "Whether limits on the use of atomic weapons, other than the particular limit of no use at all, can be defined in a plausible way is made more dubious, not less so, by the increasingly versatile character of atomic weapons. It is now widely recognized that there is a rather continuous gradation in the possible sizes of atomic-weapon effects, a rather continuous variation in the forms in which they can be used, in the means of conveyance, in the targets they can be used, … and so forth. There seems consequently to be no 'natural' break between certain limited uses and others. If we ask, then, where we might draw a line if we wished to limit somehow the size of the weapons, the means of conveyance, the situations in which or the targets on which they can be used, the answer is that we are – in a purely technical sense – free to draw a line anywhere we please. There is no cogent reasoning for drawing it at any particular gradation rather than another. … There is no degree of use, or size of weapon, or number of miles, that is so much more plausible than other degrees, sizes, or distances that it provides a focal point for both sides' expectations. Legalistic limits have to be qualitative and discrete, rather than quantitative and continuous. This is not just a matter of making violations easy to recognize, or of making adherence easy to enforce on one's own commanders; it concerns the need for any stable limit to have an evident symbolic character, such that to

[46] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *op. cit.*, pp. 902-903. Note that in this article, Schelling uses the term "limits" rather than the phrase "focal points and boundary conditions."

[47] Ibid.

breach it is an overt and dramatic act that exposes both sides to the danger that alternative limits will not easily be found."[48]

This argument was offered in full because it applies just as well to the challenge of arriving at understandings on quantitative focal points and boundary conditions for the use of cyber capabilities in *agreed competition*. Cyber capabilities are also extraordinarily versatile in their ability to generate effects, in the forms in which they can take, in the ways in which they can be conveyed, and in the targets they can be used against, and it is unlikely that any party could anticipate the creativity of an adversary in regard to any or all of these features.

With regard to the *character* of focal points and boundary conditions, Schelling argues that in order to increase the likelihood of successful tacit bargaining they must be of an "obvious" character; must attach themselves to benchmarks, demarcation lines, and distinctions that come naturally; must take advantage of existing conventions, traditions, and precedents even if those are biased against any party or a nuisance to all; and must not be too selective or too gerrymandered in discriminating between what is inside and outside the focal point or boundary condition. [49]

Problem-informed

Though adversaries will first and foremost seek understandings on focal points and boundary conditions aligning with their strategic preferences, they cannot be ignorant of the possibility that structural features of the problem they are seeking to resolve may dictate focal points or boundary conditions that do not align with the same.[50] "When agreement must be reached with incomplete communication," Schelling notes, "the participants must be ready to allow the situation itself to exercise substantial constraint over the outcome."[51] This may result in boundary conditions that discriminate against one or more competitors. He argues that an absolute ban on weapon tests or, more generally, any other categorically across-the-board prohibition is arbitrary in the way it distributes advantages. As a cyber strategic environment example, consider that an across-the-board ban on the use of botnets may disadvantage Russia more than others as their use tends to be a core feature of many Russian cyber campaigns/operations.[52]

---

[48] Thomas C. Schelling, *The Strategy of Conflict, op. cit.*, pp. 261-262.

[49] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization", *op. cit.*, pp. 902-903.

[50] Ibid., p. 904.

[51] Thomas C. Schelling, *The Strategy of Conflict, op. cit.*, p. 75.

[52] Two examples will serve to bookend the last decade of Russia's use of botnets in cyber operations. The first was the use of at least 85,000 machines in support of a 2007 Distributed Denial of Service attack against Estonian government websites. More recently, in May 2018, researchers discovered a botnet army of over 500,000 routers and storage devices infected with a piece of highly sophisticated Internet of Things botnet malware likely designed by a Russia-sponsored or state-affiliated group. See, respectively, Rebecca Grant, *Victory in Cyberspace.* (Air Force Association Special Report: Washington D.C. October 2007) and "New VPNFilter

While not discussed by Schelling, the problem may also encourage convergence around focal points and boundary conditions that potentially advantage all (or most) competitors. An example of this for the cyberspace strategic environment is the superordinate-focal point and boundary condition of *agreed competition* (i.e., an apparent prohibition on engaging in cyber operations that generate effects equivalent with armed conflict). The general problem in this example is rooted in the age-old challenge of international politics (i.e., seeking to secure/advance one's own sources of national power and/or degrade, usurp, or circumvent others' sources of national power). The specific problem is a state realizing these ends without providing a justification for other states to engage in armed conflict against it. This suggests a generic focal point (i.e., an international convention speaking to the use of force and the right of self-defense). The two most prominent such conventions are United Nations Charter Article 2(4) and Article 51: The former states that all members shall refrain from the use of force in their international relations, and the latter supports the right of self-defense in the event of armed attack.[53] States understand that using cyber capabilities generating effects equivalent with use of force could invite a justifiable armed conflict, and that outcome would represent a failure in avoiding the specific problem. Over the past decade, however, states have come to realize that the same strategic ends historically achieved through armed conflict can now be achieved through strategic cyber campaigns/operations generating cumulative effects short of armed conflict. In U.N. Charter articles 2(4) and 51, states tacitly agreed to set a boundary condition of not crossing force thresholds specified in those articles, thereby resolving the general problem.

Asymmetrical Focal Points and Boundary Conditions

Schelling also argues that within the context of arms control agreements, tacitly arrived at or otherwise, there may be "important asymmetries" or even potentially "striking differences between the weapons systems allowed" to the adversaries.[54] For reasons ranging from geography, military tradition, intelligence, technology, and the nature of alliances, adversaries may develop very different interests in, or attitudes toward, certain weapons and how they are used. Consequently, certain asymmetries are inevitable.[55] This same reasoning can be applied to focal points and boundary conditions in *agreed competition*. It should be expected that some states will gravitate more strongly toward certain focal points or boundary conditions than others for the same reasons, or, alternatively, they may have near opposite perspectives on the same focal point and boundary conditions. Regarding the latter, it can be expected, for example, that China and the United States will have vastly different perspectives on the same focal points and

malware targets at least 500K networking devices worldwide", *Talos*, 23 May 2018, https://blog.talosintelligence.com/2018/05/VPNFilter.html.

[53] *Charter of the United Nations*. For Article 2(4), see http://www.un.org/en/sections/un-charter/chapter-i/index.html and for Article 51, see http://www.un.org/en/sections/un-charter/chapter-vii/index.html.

[54] Schelling and Halperin, *Strategy and Arms Control*, *op. cit*., p. 54.

[55] Ibid.

boundary conditions associated with censorship due to cultural and technological reasons, respectively.[56]

Dynamism and Discovery

Sometimes a focal point or boundary condition may be inherently or intentionally unstable. In such cases, it serves not as a tacit agreement on an understanding, but as a sign of where to look for agreement. Schelling offers a "test vote" in a legislative body as an example, the purpose of which is to ascertain the positions of others with regard to the issue.[57] Conceptually, this is the same as floating a policy trial balloon, a tactic often seen from the U.S. Executive Branch. In this way, tacit bargaining supports discovery of new (or unanticipated) focal points and boundary conditions.

Salience for Agreed Competition

Schelling offers four primary considerations, a conceptual framework for focal points and boundary conditions, if you will, adversaries should reference to increase their likelihood of positively contributing to the collaborative process of arriving through tacit bargaining at understandings on focal points and boundary conditions in *agreed competition*.

- to increase the likelihood of arriving at tacit agreements or understandings arrived at through incomplete communication, indirect communication or strategic maneuver, focal points and boundary conditions should be of a certain nature and character (e.g., qualitatively distinguishable from the alternatives and not simply be a matter of degree);
- when tacit agreements are pursued, adversaries must be ready to allow the situation itself to exercise substantial constraint over the outcome; specifically, "a solution that discriminates against one party or the other or even involves 'unnecessary' nuisance to both of them may be the only one on which their expectations can be coordinated";[58]
- adversaries must be prepared to accept that any tacit agreement may be comprised of asymmetries in focal points and boundary conditions;
- and, the process of tacit bargaining is dynamic and, as such, may lead to the identification of unanticipated focal points and boundary conditions.

[56] Consider, for example, the report that China initiated an intense, 6-day DDOS attack against two GitHub pages: one hosting the anti-censorship page GreatFire.org and the second a mirror site of the New York Times' Chinese edition. See, https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/

[57] Thomas C. Schelling, *The Strategy of Conflict, op. cit.*, p. 112.

[58] Ibid., p. 75.

Having now argued that tacit bargaining is a more appropriate strategic process than explicit bargaining for developing cyber norms in *agreed competition* and offered a conceptual framework, adversaries should consider seeking convergence of behaviors around relevant focal points and boundary conditions. In the next two sections, evaluations are made regarding the degree to which the United States is presently postured to support a process of tacit bargaining toward this end. This evaluation will be approached from two vectors: first, determining if the U.S. has in place a cyber strategic approach that supports this process, and second, determining if it has established any policy guidance that supports the same.

A Strategy of Persistent Engagement

In March 2018, USCYBERCOM published a *Command Vision* in which it offered an assessment of the cyberspace strategic environment and proposed a strategy for responding to the same that protected and advanced U.S. national interests.[59] That strategy is *persistent engagement* and it is intended to thwart adversary cyberspace campaigns in competition by continuously anticipating and exploiting their vulnerabilities while denying their ability to exploit those of the United States.[60] The *Command Vision* also proposes that a strategy of *persistent engagement* will serve to clarify the distinction between acceptable and unacceptable behavior in cyberspace and, consequently, contribute to the stability of *agreed competition*.[61] This objective is certainly consistent with what would be the intended outcome of a process of tacit bargaining in *agreed competition*, but does the operational design of the strategy support this objective?

Comprised of continuous cyber operations that seamlessly support resiliency, forward defense, contesting, and countering to sustain U.S. strategic advantage, USCYBERCOM argues that superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and, consequently, reducing their confidence in their abilities and capabilities. The *Command Vision* describes how the Cyber Mission Force 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.[62]

In emphasizing what it would do with cyber capabilities rather than focusing on what cyber capabilities it would possess (i.e., continuously engaging and contesting adversaries and

[59] *Command Vision for U.S. Cyber Command, op. cit.*

[60] "Competition" as offered in the *Command Vision* is considered to occur in the strategic competitive space below the level of armed conflict and, therefore, is aligned with the description of *agreed competition.* Ibid., p. 5.

[61] Ibid., p. 6.

[62] Ibid.

maneuvering for advantage below the threshold or armed conflict), *persistent engagement's* operational design aligns directly with a fundamental feature of tacit bargaining: it is a strategy grounded in strategic maneuver and in action and interaction with adversaries. Thus, it is reasonable to conclude that *persistent engagement* will support a process of tacit bargaining in the pursuit of both securing and advancing U.S. national interests and arriving at mutual understandings with adversaries on acceptable/unacceptable behavior in *agreed competition*. The success of that strategic pursuit, however, will also be affected by the substance of the preferred U.S. focal points and boundary conditions of *agreed competition* around and about which convergence will be sought. The next section, then, offers an evaluation of the same against the conceptual framework Schelling recommends to increase the likelihood of convergence.

Recent U.S. Declaratory Policy Addressing Focal Points and Boundary Conditions

When the United States formally recognized cyberspace as an operating domain in 2011, it also declared its dominant strategic approach to the same would be a strategy of deterrence.[63] From 2011–2015, several strategic guidance documents offered insights into U.S. thresholds that, were they exceeded, could warrant a significant response.[64] The White House's 2011 International Strategy for Cyberspace stated that "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests"[65] The Department of Defense's 2011 Strategy for Operating in Cyberspace declared "The Department will work with interagency and international partners to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate."[66] In October 2012, U.S. Defense Secretary Leon Panetta said, "If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president."[67] And, on April 1, 2015, the White House broadcasted that "the President announced a new sanctions program that authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to sanction malicious cyber actors whose

[63] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Sept/Oct. 2010.

[64] For a concise summary, see James Andrew Lewis, "Cyber Deterrence Declaratory Policy, 2011-2015" (May 4 2015), https://www.csis.org/blogs/strategic-technologies-blog/cyber-deterrence-declaratory-policy-2011-201

[65] *International Strategy for Cyberspace* (The White House: May 2011), p. 14.

[66] *Department of Defense Strategy for Operating in Cyberspace* (Department of Defense: July 2011), p. 10.

[67] Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

actions threaten the national security, foreign policy, or economic heath or financial stability of the United States."[68]

All of these declarations are summarized well in the Obama administration's December 2015 report to Congress on cyber deterrence. In that report, the White House declared that, as part of its deterrence policy, it would be "[p]romoting a nuanced and graduated declaratory policy and strategic communications that highlight the United States Government commitment to using its capabilities to defend against cyberattacks, but remains ambiguous on thresholds for response and consequences to discourage preemption or malicious cyber activities just below the threshold for response."[69]

Evaluation of Focal Points and Boundary Conditions

Before offering an evaluation against Schelling's conceptual framework for increasing the likelihood of convergence around and about focal points and boundary conditions, it is important to note that what was presented in the previous paragraphs was considered by the Obama administration to be, and expressed as, *thresholds* from the perspective and through a strategic approach of deterrence and a strategic process of explicit bargaining, not as focal points and boundary conditions of and through a strategic approach of persistent engagement and a strategic process of tacit bargaining. The difference is important because *in a strategy of deterrence and through explicit bargaining, the defender declares thresholds to adversaries, whereas in persistent engagement and through tacit bargaining, understandings on focal points and boundary conditions of agreed competition would be arrived at with adversaries through a non-verbal bi- or multi-lateral interactive and collaborative process of strategic maneuver*. That said, since a strategy of deterrence has been until recently the comprehensive strategic approach to the cyberspace strategic environment and *agreed competition,* declaratory statements in support of that approach offer the only clues for how the United States is thinking about unacceptable behavior in the same. As such, those thresholds can offer insights into likely U.S. preferences for focal points and boundary conditions around and about which tacit understandings could be pursued through a strategy of *persistent engagement* in *agreed competition* and, therefore, are worthy of evaluation from that perspective.

A cursory evaluation of the December 2015 deterrence report finds that its approach to defining focal points and boundary conditions is, in many ways, antithetical to the first consideration for success recommended by Schelling. Rather than offer clear-cut, unambiguous, non-continuous and qualitatively discrete thresholds, the policy argues for nuance, ambiguity, and graduation. A deeper examination of how this policy manifested in executive orders derived from the 2015 sanctions program, and how that line of thinking persists in 2018, offers additional richness to that assessment and argues that it is still valid today.

---

[68] Lisa Monaco, *Expanding Our Ability to Combat Cyber Threats*, https://obamawhitehouse.archives.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats

[69] For the content of the report, see https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/dec2015/cs2015_0133.pdf

The Obama administration's Executive Orders 13694 (April 2015) and 13757 (December 2016) embody the 2015 policy for the purpose of imposing sanctions and, most recently, House Resolution 5576 (Cyber Deterrence and Response Act 2018) expands upon it for the same end.[70] An excerpt from the 2018 House Resolution is offered below because it incorporates all of the language offered in 13694 and 13757.

"(1) IN GENERAL.—The President, acting through the Secretary of State, shall designate as a critical cyber threat—

(A) each foreign person and each agency or instrumentality of a foreign state that the President determines to be responsible for or complicit in, or have engaged in, directly or indirectly, state-sponsored cyber activities that are reasonably likely to result in, or have contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of—

(i) causing a significant disruption to the availability of a computer or network of computers;

(ii) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(iii) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(iv) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;

(v) destabilizing the financial sector of the United States by tampering with, altering, or causing a misappropriation of data; or

(vi) interfering with or undermining election processes or institutions by tampering with, altering, or causing misappropriation of data"[71]

Each of these clauses represents a focal point and boundary condition and has been deconstructed in Table 1 in a manner that allows one to consider their discriminant attributes.

---

[70] See, Executive Order 13694 of April 1, 2015: *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*. Edited by Executive Office of the President of the United States of America. Washington, DC: Federal Register. Accessed April 10, 2017. https://www.treasury.gov/resourcecenter/sanctions/Programs/Documents/cyber_eo.pdf and Executive Order 13757 issued in December of 2016, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, https://www.treasury.gov/resourcecenter/sanctions/Programs/Documents/cyber2_eo.pdf

[71] *H.R.5576 - Cyber Deterrence and Response Act of 2018 (115th Congress 2017-2018)*, https://www.congress.gov/bill/115th-congress/house-bill/5576/text. Note that items (i)-(iv) were in Executive Order 13694 and item (vi) was in Executive Order 13757.

Discriminant Attributes of U.S. Policy Focal Points and Boundary Conditions					
		Boundary Conditions			
U.S. Policy Focal Points and Boundary Conditions	*Focal Point*	*Information Security Property* (Confidentiality, Availability, Integrity (data/system))	*Information Type* (e.g., PII, PI, IP,* Public, Confidential)	*Intention*	*"Damage" Type*
(i) Causing a significant disruption to the availability of a computer or network of computers	Availability	Availability			Significant disruption
(ii) Harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector	Critical infrastructure (any)	Confidentiality Integrity (system)			Harming or significantly compromising
(iii) Significantly compromising the provision of services by one or more entities in a critical infrastructure sector	Critical infrastructure (any)	Confidentiality Integrity (system)			Significantly compromising
(iv) Causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain	Commercial or competitive advantage, or private financial gain	Confidentiality	PII, IP, PI	Commercial or competitive advantage or private financial gain	Causing a significant misappropriation
(v) Destabilizing the financial sector of the United States by tampering with, altering, or causing a misappropriation of data	Critical infrastructure (financial)	Confidentiality Integrity (data)	PI, Confidential, Public		Destabilizing
(vi) Interfering with or undermining election processes or institutions by tampering with, altering, or causing misappropriation of data	Critical infrastructure (elections)	Integrity (data)	PII, Confidential		Interfering with or undermining

Table 1: Focal Points, Boundary Conditions, and their Attributes: U.S. Declaratory Policy from 2015–2018

Sources: Executive Order 13694 of April 1, 2015; Executive Order 13757 of December 28, 2016; and House Resolution 5576 Cyber Deterrence and Response Act of 2018

* PII = personally identifiable information, PI = proprietary information, and IP = intellectual property

When reviewing the nature and character of each focal point and boundary condition's attributes as presented in Table 1, it is difficult to argue that many satisfy the "must-haves" that Schelling recommended. To begin, all of the damage types of the boundary conditions are ambiguous and/or gradated. This ambiguous nature is antithetical to that which Schelling describes as necessary to increase the likelihood of arriving at tacit understandings with adversaries. In addition, several focal points have associated with them boundary conditions that include three of the same attributes but with different values for each, thus being contrary to the simplistic nature for which Schelling argues. Further, some of the focal points are specific critical infrastructure whereas others are non-specific critical infrastructure, with the former perhaps violating Schelling's guidance that focal points must not be too selective, or too gerrymandered in discriminating between what is inside and outside the focal point. Finally, while several of the six focal points are qualitatively differentiable, the timeline of their development suggests this distinction was in reaction, quite reasonably, to a series of events rather than a purposeful effort to define them in ways that would facilitate arrivals at understandings of and about them through tacit bargaining.[72]

Exemplars and Other Considerations

The evaluation of existing U.S. declaratory policy that could inform focal points and boundary conditions for *agreed competition* suggests that perhaps the best next course of action in this regard is to go back to square one and employ an approach aligned with Schelling's conceptual framework, rather than one based on recent events or other fears of the day.[73] The

[72] This perspective is supported by the following analysis. The first limit reflects that the first wave of adversary cyber campaigns/operations initially targeted the availability of U.S. systems (e.g., through Distributed Denial of Service operations). The second and third limits reflect the second wave of campaigns/operations and their primary targets (i.e., accessing critical infrastructure systems by exploiting confidentiality). The fourth is a response to the massive Chinese theft of U.S. intellectual property, also by exploiting confidentiality. The fifth likely reflects a combination of evidence that operations targeting data integrity, a potential third wave, were now appearing and the consequence such operations could have if directed against the U.S. financial sector. Finally, the sixth limit is clearly a reaction to the Russian campaign targeting the 2016 U.S. national election. In order of focal point, see Ellen Nakashima, "U.S. Rallied Multination Response to 2012 Cyber Attacks on American Banks" 11 April 2014, https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html?noredirect=on&utm_term=.9ebd0726c050; Industrial Controls Systems Cyber Emergency Response Team, *Alert (ICS-ALERT-14-281-01E), Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*, Original release date: December 10, 2014, Last revised: December 09, 2016, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B; *U.S.-China Economic and Security Review Commission 2016 Annual Report to Congress*, https://www.uscc.gov/Annual_Reports/2016-annual-report-congress; Katie Bo Williams, "Officials worried hackers will change your data, not steal it", *The Hill*, 27 September 2015, http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it; and "Russian Hacking and Influence in the U.S. Election", *The New York Times*, https://www.nytimes.com/news-event/russian-election-hacking.

[73] There is evidence that an updated policy speaking to the same is in works, albeit from an improper perspective (in this article's view) due to its objective of supporting a strategy of deterrence through a unilateral declaration of thresholds rather than a strategy of *persistent engagement* that would seek to collaboratively arrive at tacit understandings on focal points and boundary conditions with adversaries. The 2018 U.S. State Department response to Executive Order 13800 (Strengthening the Cybersecurity of Federal Networks and Critical

exemplars offered in this section are intended to serve primarily as examples that are aligned with Schelling's framework and are not intended to suggest policy positions. With that perspective, several all-or-nothing focal point and boundary condition preferences for *agreed competition* are offered below, expressed in terms of the triad of information security properties – confidentiality, availability and integrity – rather than specific effects operations may generate.[74]

The first focuses on botnets as the focal point and a prohibition on their use as the boundary condition.[75] This is a particularly salient issue given the explosion of connected devices available for exploitation through the Internet of Things.[76] As noted previously, although this would likely disproportionately disadvantage Russia, it would also disadvantage the United States and its allies and partners. As such, in addition to being simplistic, it satisfies a second of Schelling's must-have focal point/boundary condition attributes by being a "nuisance to all." For example, the British spy agency unit known as Joint Threat Research Intelligence Group used botnets to take down Anonymous' chat rooms (and France is suspected of doing the same). In addition, the U.S. Federal Bureau of Investigation replaced the GameOver Zeus botnet with its own botnet to take it down and arrest its operators.[77]

A second focal point and boundary condition could be the global financial infrastructure and a prohibition on any operations exploiting any information security property: confidentiality, integrity, or availability. All major states have a significantly vested interest in the stability of this infrastructure, thereby making it less likely that many would contest it and, perhaps more importantly, making it more likely that many would converge behaviors in support of it by collaborating to dissuade, deny, or disrupt other actors it knows may be or are considering such attacks, including criminal actors.

Infrastructure) offers evidence for a potential fresh start where the Department identified the need for creating a policy to "provide criteria for the types of malicious cyber activities that the U.S. government will seek to deter" with a goal of "A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force." See Office of the Coordinator for Cyber Issues, Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats (*Prepared pursuant to Executive Order 13800, Section 3(b)*), May 31, 2018. https://www.state.gov/s/cyberissues/eo13800/282011.htm

[74] See, *ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*, https://www.iso.org/standard/73906.html.

[75] A prohibition implies that malware cannot be employed in any ways that exploit the confidentiality, availability, or integrity of a target. In 2017, Senators Whitehouse and Graham pushed (unsuccessfully) for legislation that would "weed the garden of the Internet for botnets before they become an actual fraud or national security risk." Interestingly, the legislation was intended to support the United States Department of Justice. See Morgan Chalfant, "Senators push for enhanced powers to battle botnets", May 24, 2017, http://thehill.com/policy/cybersecurity/335007-senators-push-for-enhanced-powers-to-battle-botnets

[76] For a description of a DARPA program that would support this prohibition, see Jack Corrigan, "DARPA Wants to Find BOTNETS Before They Attack", September 11, 2018, https://www.nextgov.com/cybersecurity/2018/09/darpa-wants-find-botnets-they-attack/151182/

[77] See Lorenzo Franceschi-Bicchierai, "Botnets Can be Good, Despite What the FBI Says", *Motherboard*, December 10, 2015, https://motherboard.vice.com/en_us/article/vv7gwd/botnets-can-be-good-despite-what-the-fbi-says.

A third focal point and boundary condition could be a prohibition on any operations against nuclear command, control, and communications networks exploiting any information security property. The rationale for nuclear armed states to converge around and about this focal point and boundary condition should be obvious. Strategic nuclear deterrence is, in large part, underpinned by the assured destruction associated with the possession of nuclear capability. Consequently, any cyber operation that would introduce uncertainty into that assuredness, by threatening launch order communications, for example, would be strategically destabilizing.[78]

Other Considerations

When taking a strategic perspective on the substance of focal points and boundary conditions for *agreed competition*, U.S. policymakers should take care to not adopt the perspective of selecting or arriving at them in a manner that U.S. advantage would always be the outcome of convergence. Not being advantaged by a focal point and boundary condition is not the same as being disadvantaged by the same. In addition, as Schelling notes, asymmetries in focal points and boundary conditions should be expected as a function of differing cultural, technological and other factors. In cases where an asymmetry may disadvantage the United States, those cases should be evaluated against national security and the totality of tacit agreements in place in *agreed competition*, rather than from the perspective of convergence on each and every focal point and boundary condition being an isolated, zero-sum contest. Two examples of potential asymmetric focal points and boundary conditions, from the perspective of the United States, could be the Great Firewall of China and Russia's System of Operative Investigative Activities (SORM), the Russian domestic surveillance system for monitoring Internet and telephone communications.[79] Both focal points are deeply rooted in cultural histories of censorship and population control, and the United States should expect China and Russia to gravitate toward them as focal points. While China may accept cyber operations that exploit confidentiality of systems comprising the Great Firewall's technical architecture as part of the boundary condition, they would likely seek convergences against behaviors that would impact availability or integrity (system or data). Russia would likely take a similar stance toward SORM.[80]

---

[78] A concern over such operations is expressed in *Nuclear Posture Review, 2018* (U.S. Department of Defense: February 2108).

[79] For a discussion Chinese censorship of internet content, see April Rabkin, "Cyberattack Shows that China Isn't Content to Censor its Own Internet", Slate, 6 April 2015, http://www.slate.com/blogs/future_tense/2015/04/06/github_ddos_attack_shows_china_isn_t_content_to_censor_its_own_internet.html. For a discussion of SORM, see Ben Buchanan and Michael Sulmeyer, Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration, (Carnegie Endowment for International Peace, December 13, 2016), http://carnegieendowment.org/2016/12/13/russia-and-cyber-operations-challenges-and-opportunities-for-next-u.s.-administration-pub-66433 and Andrei Soldatov and Irina Borogan, Russia's Surveillance State, 12 September 2013, https://worldpolicy.org/2013/09/12/russias-surveillance-state/.

[80] U.S. convergence around this focal point and boundary condition would not suggest a U.S. abandonment of the principle of internet freedom. The U.S. Department of State's Bureau of Democracy, Human Rights, and Labor (DRL) could continue to work to advance the exercise of human rights and fundamental freedoms online through a diverse set of Internet freedom policy and programming activities. DRL works to advance Internet freedom

The exemplars offered all seem to be of an obvious character, as Schelling would say, and would likely increase the likelihood of convergences around the focal point and, perhaps, a U.S. preferred boundary condition. However, the latter convergence need not necessarily follow the former. It should not be expected that all competitors in *agreed competition* will converge about boundary conditions for every focal point around which they converge (i.e., contestation, rather than convergence, may become the shared behavioral expectation). But one should not conclude such contestation will necessarily lead to escalation out of *agreed competition*. Tacit bargaining provides value not only by illuminating focal points and boundary conditions about which tacit understandings can converge, it also makes clear those that require an alternative process for resolution.[81] Similarly, it should not be expected that all competitors in *agreed competition* will converge about a focal point that seems obvious to one party. It is important to remember that tacit bargaining, as executed through a strategy of *persistent engagement*, would provide an opportunity for the discovery of unanticipated focal points. Tacit bargaining, after all, is a process of discovery as much as it is of communication. The more action and interaction that occurs through *persistent engagement*, the more opportunities there will be for the development of comprehensive understandings between adversaries of acceptable/unacceptable behavior in *agreed competition*.

Conclusion

The overall strategic competitive space of *agreed competition* is still maturing. Consequently, the potential exists for some states to seek to legitimize significantly disruptive cyber actions/operations short of armed conflict-equivalence, whereas others, with benign objectives, may risk unintended or non-deliberate escalation out of *agreed competition* merely because of differing perspectives, ambiguity, or uncertainty over what are "acceptable" campaigns/operations. These immediate concerns, coupled with the limited success to date of explicit bargaining, motivated in this article the identification of a strategic process through which adversaries, without escalating to armed conflict, could collaborate to increase clarity and reduce uncertainty regarding understandings of acceptable/unacceptable behavior in *agreed competition*.

---

through bilateral and multilateral engagement, partnership with civil society and the private sector, and foreign assistance programming efforts.
See https://www.state.gov/j/drl/internetfreedom/index.htm?wpisrc=nl_cybersecurity202&wpmm=1. For an argument that China, itself, will have to relax its restrictions on censorship in order to leverage its cyber infrastructure or platforms for the purpose of power projection, see Robert Potter, *PacNet #45: Cybersecurity: The China Problem*, Center for Strategic and International Studies, 28 June 2018, https://www.csis.org/analysis/pacnet-45-cybersecurity-china-problem.

[81] A good example of this dynamic is the experience and process through and by which the United States and Soviet Union arrived at the Incidents at Sea Agreement. For the history of engagement that led to the agreement, see David F. Walker, *INCIDENTS AT SEA, American Confrontation and Cooperation with Russia and China, 1945-2016* (Naval Institute Press: Annapolis, 2017). For the agreement itself, see *Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas*, https://www.state.gov/t/isn/4791.htm.

After reviewing Schelling's scholarship on informal agreements and tacit bargaining and considering its relevance to the cyberspace strategic environment and *agreed competition*, it was concluded that tacit bargaining is a promising strategic process for inducing adversaries to collaborate on increasing clarity and reducing uncertainty regarding understandings of acceptable/unacceptable behavior in *agreed competition.* This approach comes with its own challenges, of course, and so a conceptual framework derived from Schelling's scholarship on focal points and boundary conditions was offered to guide the practical application of the approach. It was further concluded that a *strategy of persistent engagement*, described in USCYBERCOM's *Command Vision* and reiterated in the 2018 DoD Cyber Strategy, is well suited to supporting a strategic process of tacit bargaining in *agreed competition*. It was also made clear, however, as a consequence of the approach taken by the United States to date to define its preferences for unacceptable behavior, that convergence around and about those focal points and boundary conditions would not be likely. This conclusion was based not on the presence of significantly divergent interests, but rather on the nature and character of the focal points and boundary conditions offered in U.S. declaratory policy. Following Schelling's conceptual framework for increasing the likelihood of convergence, this article offered exemplars highlighting how the United States might define focal points and boundary conditions such that they are more likely to lead to convergence.

Although the notion of relying on tacit bargaining to arrive at understandings of acceptable/unacceptable behavior in *agreed competition* may make some uncomfortable, particularly those with the perspective that explicit bargaining and the formal agreements they engender are "more clear cut" or "more binding" and, therefore, better to have in hand, a closing reminder is offered: After all of his significant study on bargaining and agreements, Schelling concluded it is the understanding that matters, not the instrument (if any) in which the understanding is expressed.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-11-18	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5107
	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-9282

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 Interactions in the strategic competitive space below the threshold of armed conflict in the cyberspace strategic environment represent an *agreed competition*, a structure and dynamic characterized by actors seeking to gain strategic advantage through cyber campaigns/operations. This strategic competitive space is still maturing, however, and the potential exists for differing perspectives, ambiguity, or uncertainty over specific types of "acceptable" campaigns/operations short of armed conflict that could lead to unintended or non-deliberate escalation out of *agreed competition*. It is imperative, then, that a strategic process be identified through which states, without escalating to armed conflict, can arrive at understandings of acceptable behavior, expressed in this article as boundary conditions of *agreed competition* but more routinely called cyber norms. Thomas Schelling invested considerable time studying this same conceptual problem and this article applies his scholarship on informal agreements and tacit bargaining to the cyberspace strategic environment and *agreed competition.* It is concluded that the process of tacit bargaining is well-suited for the challenge of developing cyber norms in *agreed competition*, a *strategy of persistent engagement* supports that process, but existing U.S. policy guidance needed to facilitate its implementation falls short of what is necessary to increase the likelihood of its success.

15. SUBJECT TERMS

Cyberspace, cyber strategy, persistent engagement, norms, tacit bargaining

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	25	19b. TELEPHONE NUMBER (Include Area Code)