INSTITUTE FOR DEFENSE ANALYSES

Cyber Persistence Theory, Intelligence Contests and Strategic Competition

Michael P. Fischerkeller, *Project Leader*
Richard J. Harknett, *University of Cincinnati*

June 2020

IDA Non-Standard
NS D-13230

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

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project CB-5-4600, "Supporting and Maturing the Strategy of Persistent Engagement," for the U.S. CYBER COMMAND. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

David Mussington, Dr. Michael Warner (USCYBERCOM), Dr. Emily Goldman (NSA)

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

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-13230

Cyber Persistence Theory, Intelligence Contests and Strategic Competition

Michael P. Fischerkeller, *Project Leader*

Richard J. Harknett, *University of Cincinnati*

Cyber Persistence Theory, Intelligence Contests, and Strategic Competition

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

Introduction

How should we understand state cyber behavior and interaction dynamics? In this article, we examine two alternative sets of explanations—cyber as strategic competition and as an intelligence contest—and argue that, as a theoretical construct, strategic competition provides greater explanatory power. In presenting this case, however, we also note that the two perspectives share important common ground, which may be overlooked when highlighting differences, and we suggest a bridge between them that can inform policy.

Setting the frame correctly is essential for ensuring sound theory development and relevant policy prescription. For a better part of a decade, much of both cyber theory and policy revolved around the construct of cyberwar. In a March 2020 article, Richard Harknett and Max Smeets examined in detail the cyberwar debate and concluded that "strategy must be unshackled from the presumption that it deals only with the realm of coercion, militarized crisis, and war in cyberspace,"[1] in large part because much of state behavior in cyberspace is not captured through the construct of war and coercion. In doing so, they align with work from Michael Fischerkeller, Michael Warner, and Emily Goldman (among others) in arguing that strategic outcomes in, through and from cyberspace are possible short of war. An alternative view has taken shape principally around the work of Eric Gartzke, John Lindsay, and Josh Rovner, who argue that the bulk of cyber activity short of war is best understood as anchored to the use of deception and, thus, as an intelligence contest. Both perspectives share the common ground that most cyber state activity is not war and agree that states are incentivized to increase this activity. However, they differ on classifying the activity (strategic campaigns versus intelligence operations) and on their explanations of why ever-increasing cyber interactions do not ipso facto presage war. In this article, we argue that cyber competitive interactions are bound in a strategic calculus that is reinforced by the structure of the cyber strategic environment itself. The alternative perspective argues that constraints flow from states' cyber operations being both limited by and subject to deception.

This article has three sections. First, we outline core elements of these two alternative perspectives. Second, we offer a framework based on their common ground. And third, we present an alternative framework to the intelligence perspective's approach to assessing strategic significance, which supports an argument that strategic competition, and not an intelligence contest, best describes state's cyber behavior short of armed conflict.

[1] Richard Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes: The Other Means," *Journal of Strategic Studies* (March 2020) DOI: 10.1080/01402390.2020.1732354

Structure and Deception as Anchors

Michael Fischerkeller and Richard Harknett have advanced a theory of cyber persistence that draws from the structuralist tradition in international relations theory.[2] Kenneth Waltz identified the underlying ordering principle of the international system to be one of anarchy (as opposed to the traditional notion of hierarchy found in domestic political systems) and created a logic chain that identified self-help as a core condition that ultimately leads to a state's imperative to balance against power for survival.[3] This parsimonious explanation of international politics launched variations in theoretical emphasis within realism and, of course, a significant set of competing theories with fundamentally different assumptions, constructs, and measures.

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] The theory of cyber persistence begins with the recognition that this technical environment rests on a fundamental ordering principle—interconnectedness—that is distinct from other structures such as anarchy and hierarchy.[5] Just as anarchy creates a distinct condition (self-help), so too does interconnectedness. Interconnectedness means that states are in contact with not just adversaries, but with all other actors in this global system, and that this contact is not imminent, potential, nor episodic, but instead, being structurally derived, is constant. If states technically segment themselves (i.e., they leave the interconnected environment), this condition falls away, but to be in an interconnected environment is to be in constant contact.[6] Set against his ordering principle and condition, Waltz examined the distribution of capability (military, economic, and social power) and determined it was inherently uneven and thus, in the pursuit of security under anarchy in a condition of self-help, states would have to balance their power relative to others. The struggle for power in order to balance, which Hans Morgenthau identified as the core dynamic in international politics was, for Waltz, a structural imperative. If states did not balance, they would not survive.

An examination of the distribution of capabilities in cyberspace reveals the nature and substance of the technology itself—a vulnerable and resilient technological system with very low entry costs for core

---

[2] Michael P. Fischerkeller, Richard J. Harknett, and Jelena Vicic, "The Limits of Deterrence and the Need for Persistence," in Aaron Brantly, Ed., *The Cyber Deterrence Problem*, (Rowman and Littlefeld, forthcoming 2020), and Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 63 1 (Summer 2017): 381–393. See also Richard J. Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare*, 15 (2) Spring 2016: 81–88.

[3] Kenneth Waltz, *Theory of International Politics* (NY: McGraw-Hill, 1979); In Richard J. Harknett and Hasan Yalcin, "The Struggle for Autonomy: A Realist Structural Theory of International Relations" *International Studies Review* Volume 14 (2012): 499-521, the authors modify the Waltzian constructs and argue that anarchy creates the condition of self-reliance and a state imperative to seek autonomy.

[4] Joint Pub 3-12, "Cyber Operations," https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[5] The notion that cyberspace is global and interconnected is a general default of most policy documents and common parlance, but the theoretical implications have typically been missed. See White House, *International Strategy for Cyberspace* (May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[6] Richard J. Harknett, "Reframing the Fundamentals of Cyberspace: CAG Talk 2016," https://www.youtube.com/watch?v=tA1Uixj44ic

access, high fluidity in both character and use, and high value (a global warehouse of and gateway to troves of sensitive, strategic assets that translate into wealth and capacity to act). The fact that cyberspace is both vulnerable and resilient creates a distinct dynamic—one can seek to exploit vulnerabilities at scale without concern over destabilizing the environment. As the potential for exploitation is ever-present and states are in constant contact due to interconnectedness, they must assume their sources of national power may be vulnerable; from a national security perspective, states must now be concerned that core economic, political, social, and military capability and capacity could be undermined. This elevates the potential of cyber activity to a strategic concern and, thus, a state's only logical choice to be more secure than others is to anticipate and proactively mitigate the exploitation of its vulnerabilities. The structural imperative thus becomes persistence in seizing the initiative in setting the conditions of security by exploiting adversary vulnerabilities and reducing the potential for exploitation of its own. If states do not persist, they cannot secure national interest in, through and from cyberspace.[7]

Alternatively, Erik Gartzke and Jon Lindsay argue that advantages in cyberspace do not result from "categorical features or attributes of the internet" but, rather, from "relative organizational capacity for employing deception and integrating it with broader strategic initiatives." [8] Thus, an actor's capacity for deception is a core feature for explaining state behavior in cyberspace. To gain advantage, this capacity is applied against cyberspace's organic "abundance of opportunities to exploit user trust and design oversights", thus, "no deception, no attacks,"—but the attacker can also be fooled, and the defender can also deceive.[9] Similarly, Lindsay argues that "most cyber operations rely on deception to collect intelligence or steal intellectual property, exert influence through propaganda or sabotage, or defend against these activities."[10] Given the centrality of deception to intelligence operations, Gartzke and Lindsay (and Rovner) draw on the field of intelligence studies to claim that "cyber warfare is not a 'sui generis' phenomenon, but rather a member of a class of phenomena—intelligence and covert operations" and "Nothing in cybersecurity makes sense except in the light of intelligence".[11] Thus, both perspectives agree that cyberspace is rife with the opportunity to exploit, but offer a different explanatory frame in which to examine it.

A Self-limited Cyber Competitive Space

The theory of cyber persistence argues that cyber strategic competition will primarily play out in the competitive space short of armed conflict because there exists a structural imperative for states to act persistently short of armed conflict. Interconnectedness creates vectors to others' instruments of

[7] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review – Special Edition* (2019), https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

[8] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies* (24:2), pp. 316–348, http://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf.

[9] Ibid.

[10] Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cyber Security*, Ed. Paul Cornish (New York: Oxford University Press, (forthcoming)), https://drive.google.com/file/d/0B7IN_AGAVuy-WFFFX04yNVVjM3c/view.

[11] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs," op. cit., and Jon R. Lindsay, "Cyber Espionage," op. cit.

national power in a technology environment that provides significant opportunities to "exploit user trust and design oversights," to borrow Gartzke and Lindsay's phrase,[12] within an overall environment of technological resilience. Through significant experimentation, states have discovered this combination enables the realization of strategic gains through competition via cyber operations and campaigns short of armed conflict, thus presenting a *strategic incentive* for continued activity and further experimentation. We argue there is an additional strategic incentive for operating predominantly short of armed conflict—once an armed attack threshold is violated, states could legitimately respond with cross-domain, conventional, kinetic weapons and justify it as self-defense, thereby introducing a very different, and likely less predictable, set of risks, costs, and challenges.[13] (Note there is a presumption of likely attribution at the level of cyberattack underpinning this argument.) We have introduced the construct of agreed competition to capture how the interplay of the strategic imperative and incentives results in a self-limited cyber strategic competitive space.[14]

Gartzke and Lindsay, along with Rovner, explain that intelligence agencies have historically operated in the competitive space short of armed conflict and argue that the global reach of cyberspace and its opportunities for deception, which is essential for secret intelligence, have increased opportunity for intelligence activity. They do not offer a structural theory (i.e., those opportunities are not structurally derived), but their logic argues that cyberspace minimally creates a strong *intelligence incentive*, if not an imperative, to invest in deception capacity and expand the scope of operations in cyberspace (one could surmise that, if you do not keep pace with the intelligence activities of your competitors in this hyperactive space, you will fall behind more quickly).[15] They also argue there is a strong intelligence incentive to avoid operations that cause serious effects or are against "most valuable targets" because such efforts increase the risk of cross-domain response or retaliation.[16] Gartzke and Lindsay offer an intelligence argument as to why concern over exposure is likely—the most valuable targets are complex and the risk of attacker compromise increases with the complexity of a target (which makes it more likely the attacker will leave forensic clues behind) and the seriousness of the attack (which makes it more likely the victim will mount a major investigation). Lindsay argues that successful deception becomes more difficult with the political value of the target.[17] Gartzke and Lindsay further argue this intelligence rationale to self-limit is supported by an operational incentive to do the same as the necessity for secrecy limits the breadth of an operation—intelligence history has taught that broad conspiracies are difficult to keep secret from competitors and may also confuse one's own troops, allies, or partners who are not in on the ruse. In sum, "cyber attackers do not run rampant like raiders on the steppe because they are both limited by and subject to deception."[18] The difference in categorization

---

[12] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs," op. cit.

[13] A *structural imperative* is a theoretically derived absolute, but it does not mean that states can't make bad decisions and suffer the consequences. A *strategic incentive* is a set of cost/benefit calculations that creates a rationale for a certain set of choices.

[14] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation", op. cit.

[15] This is also argued by Joshua Rovner, another proponent of adopting an intelligence contest perspective for better understanding cyberspace activity and dynamics. See Joshua Rovner, "Cyber War as an Intelligence Contest", *War on the Rocks*, September 19, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[16] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs," op. cit.

[17] Jon R. Lindsay, "Cyber Espionage," op. cit.

[18] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs," op. cit.

and explanation is thus important to note between these two perspectives—one seeing limits set through strategic pursuits reinforced by structure; the other, through tactical action reinforced by operational constraints.

Importantly, even though they are of different origin, dissimilar orientation, and they employ largely distinct logic, cyber persistence theory and the intelligence studies-derived perspective both conclude that state cyber behavior will primarily play out in a self-limited cyber competitive space—a conclusion supported by the empirical record to-date of reported operations and campaigns between states not already engaged in militarized crises or armed conflict.[19]

Interaction Dynamics

Cyber persistence theory argues that the dominant strategic interaction dynamic in cyberspace is *competitive interaction* within a definable operational space. States abiding by the structural imperative to act persistently will continuously execute campaigns populated by cyber operations short of armed conflict seeking, over time and space, to generate cumulative strategic effects (i.e., to achieve strategic outcomes).[20] Competitive interaction is measured primarily as relative changes in scale, scope, and/or intensity of cyber campaigns conducted within the implicit boundaries of restraint and armed-attack equivalent effects.[21]

Gartzke, Lindsay, and Rovner argue that deception matters most, politically, in increasing the options available for competitive and aggressive interactions other than war, and consequently, interaction in a deception-prone world is typically also something other than war. "Cyber warfare," and perhaps all forms of deception-dependent interactions, they argue, are best understood as low-intensity conflict behavior.[22] Indeed, in contrast to the escalation dynamic characterizing the threat or actual use of force, Gartzke and Lindsay argue that cyber operations could provide a safety valve to help de-escalate crises and promote caution among adversaries that either fear being duped or discount the expected gains of aggression. In fact, Lindsay argues that resorting to covert action often reflects a desire to keep conflicts

[19] According to Lindsay, one reason why cyberattacks seem difficult to deter is that attackers intentionally target them below some threshold where they expect retaliation to be more likely. Jon R. Lindsay, "Cyber Espionage", op. cit. Although he doesn't specify what that threshold is, Fischerkeller and Harknett have argued that it is aligned with U.N. Charter articles 2(4) and 51 addressing use of force and armed attack, respectively. Michael P. Fischerkeller and Richard J. Harknett, "What is Agreed Competition in Cyberspace?" *Lawfare* (February 19, 2019), https://www.lawfareblog.com/what-agreed-competition-cyberspace.

[20] For more on the pursuit of strategic effects, advantage and outcomes through campaigns, see Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes," op. cit.

[21] *Cyber persistence theory* assumes that all states act in their best interests—thus, there is a convergence of behavior above restraint (because restraint means states lose) and short of armed conflict (because war means states sub-optimize cyberspace's novel contribution to strategic competition). The competition that ensues is thus "agreed" behaviorally at first and can become more explicitly agreed to as rules of the game or norms of cyber competition emerge. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (November 2018). https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

[22] Erik Gartzke and John R. Lindsay, "Weaving Tangled Webs," op. cit.

limited.[23] Again, the two perspectives, while offering different logics, share the view that the cyberspace competitive environment does not incentivize leveraging coercive escalation strategies nor create dynamics that induce inadvertent escalation. Both see the majority of state cyber behavior as best characterized by interaction, rather than escalation dynamics.

Complementarity: Building a Bridge

Given these common conclusions, albeit from different origins, it may be possible to find a more robust explanation for and understanding of cyber behaviors and interaction dynamics that consider these perspectives in tandem. For the cyberspace strategic environment, a composite framework using the terminology of imperatives and incentives would include:

- a structural imperative to operate persistently,
- an operational and tactical imperative/incentive to invest in the capacity to deceive,
- strategic and operational incentives to self-limit campaigns and operations within a bounded cyber competitive space short of armed conflict,

as well as:

- an operational imperative/incentive to use deception in "offensive" operations,[24]
- and an operational incentive to use deception in defensive operations.[25]

Although cyber persistence theory and the application of intelligence studies to cyber interactions have some intersections, they diverge substantially on whether cyber strategies short of armed conflict being practiced by hostile, peer competitors generate effects or outcomes that are independently strategically significant—that is, whether there is an ongoing strategic competition vice an intelligence contest.

Divergence: Cyber as Strategic Competition Versus Cyber as Intelligence Contest

Intelligence contest scholars argue that computer network operations should mainly be understood as "expanding the scope of intelligence and covert operations" and that cyber warfare "is best understood as low-intensity conflict behavior … rather than as a separate form of strategic warfare."[26] They offer strategic and operational arguments to support this perspective. The strategic argument is as follows. Gartzke asserts that for cyber operations to be independently relevant in "grand strategic terms" or

[23] Jon R. Lindsay, "Cyber Espionage," op. cit.
[24] Gartzke and Lindsay argue that deception is necessary for offensive operations. Erik Gartzke and John R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," op. cit. Fischerkeller and Harknett argue, instead, that there is merely an incentive for deception in such operations, whose degree of use for advantage is a function of political and/or operational objective and/or target technical complexity.
[25] Ibid. Gartzke and Lindsay argue that "Deception [in defense] adds to the ambitious attacker's already significant intelligence burden by: creating more use cases that attack code is required to handle; covering up heterogeneity so that all targets look similar; and hiding factors that can lead to failure against particular targets."
[26] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," op. cit.

"pivotal in world affairs" they would have to "accomplish tasks typically associated with terrestrial military violence," including deterring or compelling (i.e., generating influence through the prospect of damage or loss, maintaining or altering the balance of power, and resisting or imposing disputed outcomes).[27] Lindsay explores the deterrence/compellence task through a lens of strategic bargaining, arguing that the strategic significance of offensive cyber operations would be found in their ability to unambiguously communicate cyber capability and resolve in a coercive bargaining process (deterrence and compellence). He concludes that such clear communication is "especially problematic" in cyberspace because deception is a permissive condition for cyber operations.[28] Thus, Gartzke and Lindsay conclude that cyber operations cannot independently generate strategic effects or outcomes.

The operational argument flows from limits on effects or outcomes due to the burdens of deception. Lindsay argues that the political effects of cyber operations are ambiguous because of the constraints of deception—that is, the operational needs required to sustain large deceptions in fact create limits.[29] Thus, "deception is useful for only a subset of political aggression, and *it does not scale*" (emphasis added). He describes deception's failure to scale on two different axes. First, offensive deception becomes more difficult and defender attribution efforts are more likely the higher the political value of a target (i.e., failure to vertically scale). Second, offensive deception constrains pursuing multiple, simultaneous operations against heterogeneous and/or well defended (higher value) targets because each intrusion requires significant and unique deception efforts (i.e., failure to horizontally scale).[30] Consequently, though cyberspace facilitates expanding the scope of intelligence and covert operations, due to the burdens of deception, the resulting effects or outcomes merely represent a difference in degree from historical intelligence operations' results.

There is no dispute that many cyber operations rely on deception and are informed by the traditional practices of intelligence. We contend, however, that Gartzke and Lindsay have adopted the wrong strategic concepts against which to assess the potential strategic significance of states' cyber behaviors short of armed conflict and, consequently, are drawing incorrect strategic and operational conclusions regarding their significance.

A More Appropriate Frame for Assessing Strategic Significance

Dan Altman notes that James D. Fearon, in reviewing the literature on strategic interaction during crises, drew a basic distinction between crises as competitions in risk taking and crises as competitions in tactical cleverness (i.e., as attempts to outmaneuver the adversary).[31] Fearon argued for the importance of both but focused on the former.[32] Many scholars leveraged and built on his insights regarding

---

[27] Ibid.
[28] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity*, 1(1), 2015, 53–67, https://academic.oup.com/cybersecurity/article/1/1/53/2354517.
[29] Jon R. Lindsay, "Cyber Espionage," op. cit.
[30] Jon R. Lindsay, "Tipping the Scales," op. cit.
[31] Dan Altman, "Advancing without Attacking: The Strategic Game around the Use of Force," *Security Studies*, 27:1, 58–88, https://doi.org/10.1080/09636412.2017.1360074.
[32] James D. Fearon, "Threats to Use Force: Costly Signals and Bargaining in International Crises," (PhD diss., University of California, Berkeley, 1992).

competitions in risk taking, creating in international relations theory an "established view" of strategic bargaining placing central emphasis on the concepts of coercion, signaling resolve, and brinkmanship.[33] Gartzke and Lindsay have adopted this established view in their studies of cyber behaviors. In fact, Fearon's lesser-explored alternative—the *fait accompli*—better, albeit still imperfectly, describes state's behaviors in, through and from cyberspace and, therefore, serves as a more appropriate frame through which to assess the potential independent strategic significance of the same.[34]

The *fait accompli* in the cyber strategic environment is described as a limited unilateral gain at a target's expense where that gain is retained when the target chooses to relent rather than escalate in retaliation.[35] "Unilateral" means that the defender is not a participant in the activity.[36] The pursuit of a unilateral gain aligns with cyber persistence theory (and intelligence-contest) arguments that a strategic incentive is present for exploitation deriving from cyberspace's inherent vulnerabilities. Additionally, a concern with inviting retaliation through escalation is consistent with cyber persistence theory (and intelligence-contest) arguments that incentives exist for bounding cyber behaviors. Regarding boundaries specifically, based on his historical study of territorial acquisitions, Altman concludes that "*faits accomplis* are more likely to succeed at making a gain without provoking war when they take that gain without crossing use-of-force red lines." [37] This upper bound is consistent with the empirical record to-date of most state behaviors in cyberspace between states not already engaged in militarized crises or armed conflict.

Embracing the *fait accompli* concept instead of the concepts of coercion, signaling resolve, and brinkmanship broadens understanding of the political value of cyberspace targets. Rather than presuming that states equate high political value with future coercive value, as Lindsay appears to do, the calculus of political value for the *fait accompli* becomes determining which targets, if exploited, result in positive gains or benefits today.[38] The *fait accompli*, then, is superior to coercion for describing and explaining states' cyber behaviors short of armed conflict. It accounts for both unilateral operations

---

[33] James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs," *Journal of Conflict Resolution*, 41, no. 1 (February 1997): 68–90; Paul K. Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science*, 2, no. 1 (June 1999): 25–48; James D. Morrow, "The Strategic Setting of Choices: Signaling, Commitment, and Negotiation in International Politics," in *International Relations: A Strategic Choice Approach*, Ed. David Lake and Robert Powell (Princeton, NJ: Princeton University Press, 1999); Branislav L. Slantchev, *Military Threats: The Costs of Coercion and the Price of Peace* (Cambridge: Cambridge University Press, 2011).

[34] A more complete argument, including imperfections, is presented in Michael P. Fischerkeller, "Strategic Choice in Cyberspace: The *Fait Accompli* and Persistent Engagement," June 24, 2020, *War on the Rocks*, https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/

[35] Ibid.

[36] Ibid.

[37] Dan Altman, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries," *International Studies Quarterly* (2017) 61, 881–891, https://www.researchgate.net/publication/322126880_By_Fait_Accompli_Not_Coercion_How_States_Wrest_Territory_from_Their_Adversaries.

[38] For a related argument on how cost imposition should be reconceptualized in the cyber competitive space short of armed conflict, see Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," *Lawfare*, February 6, 2020, https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

seeking gains from often significantly disparate targets and mutual efforts to routinely avoid operations that could justify armed retaliation.

Consequently, in the terrestrial realm, the *fait accompli* "land grab" is said to be unsuitable for maximalist aims such as conquering an adversary outright, changing a regime, or other effects or outcomes that are undeniably strategic.[39] We argue that the same conclusion should not be uncritically applied to the *fait accompli* in cyberspace. Although the *fait accompli* comprising a single cyber operation short of armed conflict may only generate a limited gain of marginal significance, a cyber campaign comprising *faits accomplis* executed at scale (horizontally) could generate cumulative gains of potential strategic significance. This path to strategic effects or outcomes does not square with Lindsay's conclusion that offensive deception fails to scale horizontally by constraining the pursuit of multiple, simultaneous operations against heterogeneous, well-defended high political value targets—but his conclusion only holds because Lindsay views the political utility of cyber operations through a coercion lens.

Lindsay argues that an implication of offensive cyber operations' reliance on deception is that "deception will be more useful for pursuing some positive benefit today … rather than coercively threatening harm tomorrow."[40] We agree with this argument but disagree that it disqualifies cyber operations from having potential strategic political utility. Lindsay argues that a target's technical complexity and political value are usually correlated and appears to equate high political value (and, therefore, complexity) with future coercive value.[41] He also observes that there are "many targets of low value connected to the internet, and many of them are poorly defended."[42] And, further notes that most attacks tend to fall on the "lower end" of the value spectrum, as he defines value.[43] These "low value" targets, using his reasoning, are likely less complex and would, therefore, loosen a primary constraint on offensive deception's ability to scale horizontally.

If one replaces Lindsay's coercion-based perspective for ascribing political value with the *fait accompli* perspective, it could be argued that many of Lindsay's "low value," less complex targets are, in fact, of high political value to states seeking through cyber operations to realize positive gains or benefits today. States holding this perspective would most certainly see potential strategic political utility in pursuing campaigns at scales maximizing desired gains or benefits, as offensive deception would no longer constrain campaigns at scale. Consider the hundreds, if not thousands, of companies targeted by Chinese cyber operators seeking to illicitly acquire U.S. intellectual property (IP) as a case in point.[44]

Changing the strategic frame from coercive bargaining to the *fait accompli* leads to a conclusion that deception need not act as a constraint on a state's quest to realize strategic effects or outcomes through cyber behaviors short of armed conflict. By pursuing unilateral campaigns at scale (horizontally) against low complexity, high political value targets, states can transition from single operations generating a

[39] Dan Altman, "By Fait Accompli, Not Coercion," op. cit.
[40] Jon R. Lindsay, "Tipping the Scales," op. cit.
[41] Ibid.
[42] Ibid.
[43] As an example, Lindsay mentions critical infrastructure in a discussion of high value political value targets.
[44] This suggests Lindsay's contention that "it is not very controversial to assume that attacker costs will scale with target value" is, in fact, controversial when considered in light of the *fait accompli* versus coercion-based strategic concepts.

limited gain or benefit of marginal significance to substantial campaigns generating cumulative gains and, potentially, independent strategic effects or outcomes. Michael Warner makes a related argument associating opportunities for operating at scale with potential strategic significance. Where the influence of covert operations had been at "the margins of state practice," Warner claims that it may become more strategic now that cyberspace allows states to execute covert operations at scale.[45] The ability to execute continuous, cyber campaigns at scale, he says, allows for individual, marginal effects to aggregate into the class of strategic effects. Thus, whereas covert operations have historically been a secret, supplemental factor in international relations, Warner argues that cyberspace now facilitates their functioning through scale as a secret, independent strategic factor.[46]

These arguments are consistent with cyber persistence theory. The empirical record makes clear that an expansion in scope of operations, the only expansion predicted by the intelligence perspective, has been accompanied by an expansion in scale, which together arguably result in a difference in kind, not merely degree, and in a strategic competition, not merely an intelligence contest. Indeed, a recognition of and concerns over adversaries operating "at scale" played an important role in elevating the importance of cyberspace in U.S. Department of Defense thinking.[47] These concerns proved prescient as nearly every annual U.S. Director of National Intelligence threat assessment report for the past decade references year-over-year increases in scope and scale of adversary operations targeting U.S. national interests (and the same can be found in private sector threat reports).[48]

Assessing Strategic Significance through the New Frame

The *fait accompli* concept better describes and explains states' cyber behaviors than do coercion, signaling resolve, and brinksmanship (the concepts adopted by the intelligence contest perspective), and, therefore, is a more appropriate frame through which to assess the potential strategic significance of the same. Of Gartzke's aforementioned three criteria for assessing significance—deterring or compelling, maintaining or altering the balance of power, and resisting or imposing disputed outcomes—Lindsay and Gartze argue cyber operations short of armed conflict fail to satisfy the first criterion. We agree but argue the remaining criteria have been, and continue to be, met by states executing *faits accomplis* at scale.

Consider the Democratic People's Republic of Korea's (DPRK's) response to the "toughest and most comprehensive sanctions regime ever imposed" by the U.N. Security Council via Resolution 2321 (2016) as an example of a state employing a cyber campaign to resist a disputed outcome and achieve a

[45] Michael Warner, "A Matter of Trust: Covert Action Reconsidered", *Studies in Intelligence* (63:4), pp. 33–41, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-4/index.html.
[46] Ibid.
[47] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," op. cit.
[48] As bookends, consider the 2010 and 2018 annual threat assessments. Dennis C. Blair, "Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," February 2, 2010, https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf, and Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. For an example of private sector reporting, see FireEye's M-Trends reports, https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

strategic gain.[49,50] DPRK leadership responded to this challenge through persistent military exploitation of the international banking system in and through cyberspace and other financial digital manipulation. In August 2019, the United Nations Panel of Experts charged with assessing the sanctions placed on the DPRK concluded that the North Koreans generated an estimated $2 billion for its weapons of mass destruction programs, including efforts to continue enhancing its nuclear and missile programs, through "sophisticated use by the Democratic People's Republic of Korea of cyber means to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges, launder stolen proceeds and generate income in evasion of financial sanctions."[51] In this case, the targets of highest political value for the regime are those that facilitate the acquisition of currencies today, not those that might provide future coercive value. Moreover, these efforts are resulting in strategic effects and outcomes that are arguably pivotal to world affairs—undermining strategic objectives of both the United Nations and the United States while bolstering a nuclear capability.

Conclusion

Two research efforts of different origin, dissimilar orientation, and employing largely distinct logics conclude that cyber competition will primarily play out in a self-limited cyber competitive space short of armed conflict and that escalation is not the dominant strategic interaction dynamic in the cyberspace strategic environment. These conclusions are supported by the empirical record to-date of reported operations between states not already engaged in armed conflict. Cyber persistence theory further argues that operational persistence is required to achieve security, and the intelligence perspective argues a capacity to deceive in operations is required for the same. Thus, although they disagree importantly on the classification of the space and the potential strategic importance of the activity, in tandem they offer a robust framework for recommendations to serve policymakers responsible for cyber policy and strategy.

To see cyber as strategic competition does not necessitate losing the important observations that can flow from seeing an intelligence contest nested within that strategic competition. Admittedly, however, the reverse is not true. Although convergence of theoretical perspectives is not common in international relations theory, perhaps the parsimony of cyber persistence theory can be enhanced through the specifics of intelligence studies. This article contends such a pursuit would bear fruit for both better explanation and better policy.

[49] United Nations, "Security Council Strengthens Sanctions on Democratic Republic of Korea, Unanimously Adopting Resolution 2321 (2016)," https://www.un.org/press/en/2016/sc12603.doc.htm.
[50] For another example, see Michael P. Fischerkeller, "Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace," (Institute for Defense Analyses: April 2020).
[51] United Nations, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)"; S/2019/691.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Persistence Theory, Intelligence Contests, and Strategic Competition	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller, Richard J. Harknett	CB-5-4600
	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-13230

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Steve Peterson, Special advisor to COMUSCYBERCOM / DIRNSA U.S. CYBER COMMAND Ft. Meade, MD	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

How should we understand state cyber behavior and interaction dynamics? This document examines two alternative sets of explanations—cyber as strategic competition and as an intelligence contest—arguing that, as a theoretical construct, strategic competition provides greater explanatory power. In presenting this case, however, the article also notes that the two perspectives share important common ground that may be overlooked when highlighting differences and suggests a bridge between them that can inform policy.

15. SUBJECT TERMS

Cyber strategy, persistent engagement, intelligence contest, strategic 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	Unlimited	11	Steve Peterson, Special advisor to COMUSCYBERCOM / DIRNSA
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER (Include Area Code)