INSTITUTE FOR DEFENSE ANALYSES

Strategic Choice in Cyberspace: The *Fait Accompli* and Persistent Engagement

Michael P. Fischerkeller, *Project Leader*

May 2020

IDA Non-Standard
NS D-13214

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 C5107, "Cyberspace Operations Working Group," for the 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.

Acknowledgements

Emily Goldman, Michael Warner, Brian David A. Mussington

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

Rigorous Analysis | Trusted Expertise | Service to the Nation

Strategic Choice in Cyberspace: The *Fait Accompli* and Persistent Engagement

Michael Fischerkeller, Institute for Defense Analyses

In several *Lawfare* essays, Richard Harknett and I have argued that, in the cyber strategic environment, coercion theory aligns well with the cyber strategic space of militarized crises and armed conflict.[1] Our arguments have been both explicitly and implicitly inclusive of the extensively studied and well understood strategic bargaining concepts associated therewith: deterrence, compellence, signaling, brinksmanship, cost imposition, and escalation. We have further argued, as have others, that these concepts do not describe well states' strategic cyber behaviors and interactions in the cyber strategic competitive space short of armed conflict.[2] This essay demonstrates how a lesser-studied strategic bargaining concept—the *fait accompli*—better describes such behaviors, albeit still imperfectly. Moreover, because the strategic logic behind the *fait accompli* aligns with the structural imperative and strategic incentives identified by cyber persistence theory, it provides additional grounds for committing to a strategic approach of persistent engagement and adopting its core strategic principle of seizing the initiative in setting the conditions of security as an anchor for national cyber strategy.[3]

The *Fait Accompli*

Dan Altman's research on the *fait accompli* in terrestrial disputes 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).[4] Fearon argued for the importance of both, but focused on the former.[5] International relations theorists leveraged Fearon's insights on competitions in risk taking to develop a strategic bargaining paradigm that places central emphasis on the concepts of coercion, signaling resolve, brinkmanship, and escalation.[6] It was a natural inclination to adopt these concepts to describe

---

[1] See, for example, Michael P. Fischerkeller and Richard J. Harknett, "A Response on Persistent Engagement and Agreed Competition," *Lawfare*, June 27, 2019, https://www.lawfareblog.com/response-persistent-engagement-and-agreed-competition and 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.

[2] Ibid.

[3] Michael P. Fischerkeller, "The Cyberspace Solarium Report and Persistent Engagement," *Lawfare*, March 23, 2020, https://www.lawfareblog.com/cyberspace-solarium-commission-report-and-persistent-engagement.

[4] 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.

[5] James D. Fearon, "Threats to Use Force: Costly Signals and Bargaining in International Crises" (PhD diss., University of California, Berkeley, 1992).

[6] 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

and explain state cyber behaviors.[7] But as Harknett, I, and many others have argued, those concepts fail to explain most state cyber behavior short of armed conflict. Fearon's less-explored alternative better describes this behavior; its premise is captured in the strategic bargaining concept of the *fait accompli*.

The *fait accompli* is described with little variance in international relations strategic bargaining literature.[8] Altman says the "*fait accompli* imposes a limited unilateral gain at an adversary's expense in an attempt to get away with that gain when the adversary chooses to relent rather than escalate in retaliation."[9] Alexander George describes it as altering the status quo in one's favor through a quick decisive transformation of the situation that avoids unwanted retaliatory escalation.[10] Altman uncomfortably bins the *fait accompli* under coercive bargaining, but only because *faits accomplis* in the conventional strategic environment (i.e., the terrestrial frame) normally represent the failure of deterrence.[11]

The strategic logic behind the *fait accompli* in terrestrial disputes hinges on finding vulnerabilities in "red lines." Altman defines red lines as the part of a coercive demand, which distinguishes compliance from violation.[12] When red lines are arbitrary, imprecise, incomplete, or unverifiable, states are incentivized to act unilaterally to achieve their limited desired gain.[13] When they do act, 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."[14]

Finally, although the *fait accompli* may fail in outcome for several reasons, including, for example, the defender choosing not to relent and marshalling superior forces to take back the gain made, it fails in execution for only one reason—the defender's anticipating the unilateral action and setting the conditions of security in its favor. This is in stark contrast to the several ways coercive strategies can fail: lack of commitment, ambiguity of demands, or non-credible capability.

Harknett and I argue that policymakers and scholars developing cyberspace strategy should not uncritically adopt strategic concepts created to describe or explain state behavior in nuclear and/or

---

University Press, 1999); Branislav L. Slantchev, *Military Threats: The Costs of Coercion and the Price of Peace* (Cambridge: Cambridge University Press, 2011).

[7] Emily O. Goldman, "The Cyber Paradigm Shift," Newport Papers, Naval War College Press, 2020 forthcoming.

[8] Dan Altman, "Advancing Without Attacking: The Strategic Game around the Use of Force", op. cit.; Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Glenn H. Snyder and Paul Diesing, *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton, NJ: Princeton University Press, 1977); and Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* (22:4, Spring 1998).

[9] 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.

[10] Alexander L. George, "Strategies for Crisis Management," in Alexander L. George, ed., *Avoiding War: Problems of Crisis Management* (Boulder, CO: Westview Press, 1991).

[11] Dan Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis" (PhD diss., Massachusetts Institute of Technology, June 2015), https://dspace.mit.edu/bitstream/handle/1721.1/99775/927329080-MIT.pdf?sequence=1&isAllowed=y.

[12] Ibid.

[13] Ibid.

[14] Dan Altman, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries," op. cit.

conventional environments.[15] For example, we adapted and caveated aspects of Kahn's concept of agreed battle when creating the concept of agreed competition to describe tacitly bounded strategic interaction in the cyber competitive space short of armed conflict.[16] The same tack is taken with the *fait accompli*.

The *Fait Accompli* in Cyberspace

The *fait accompli* in the cyber strategic environment is 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. George's "quick" adverb is eschewed because, although gains can be realized quickly through cyber exploitation, gains are also realized through sustained exfiltration supported by on-network persistent presence. Altman's verb "imposes" is also excluded because it harkens to a key phrase—cost imposition—that is tightly coupled with coercion theory.

"Unilateral" means that the defender does not participate in the activity, which is rooted in exploitation.[17] Thus, the *fait accompli* is distinct in principle from coercion, which describes demands, signaling, and interaction. Moreover, making gains at the expense of an adversary is not the same as threatening to impose costs or actually doing so, as Harknett and I recently argued.[18] Once a benefit/gain is realized, it may subsequently serve as a foothold for future coercive cyber strategic bargaining, depending on the target's coercive political value; however, first and foremost, the *fait accompli* is about seeking unilateral gains through exploitation.

As in the terrestrial frame, states adopting the *fait accompli* have a strategic incentive to pursue their desired gain in, through, and from cyberspace in ways that do not invite escalatory retaliation. This is consistent with the empirical record to-date of most behaviors in cyberspace between states not already engaged in militarized crises or armed conflict. Again, as in the terrestrial frame, the strategic logic behind the *fait accompli* in cyberspace hinges on finding vulnerabilities. However, unlike the terrestrial frame, those vulnerabilities do not lie in the ambiguity of a coercive demand, but rather *in the very fabric of cyberspace itself*. Harknett and I describe cyberspace as a vulnerable yet resilient technological system.[19] Others describe it as organically offering an "abundance of opportunities to exploit user trust and design oversights."[20] These opportunities provide a strategic incentive for states to pursue unilateral gains in, through and from cyberspace. This incentive is further enhanced because, while the *fait*

---

[15] Michael P. Fischerkeller and Richard J. Harknett, "A Response on Persistent Engagement and Agreed Competition", op. cit.
[16] 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.
[17] Dan Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis," op. cit.
[18] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect" op. cit.
[19] 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.
[20] Erik Gartzke and John 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.

accompli in physical space returns a limited gain, cyberspace enables *faits accomplis* at scale, potentially generating strategic gains. That the source of vulnerability is not an ambiguous coercive demand has another important implication—it eliminates Altman's rationale for coupling the *fait accompli* with coercive bargaining in cyberspace.

There is a second way in which the *fait accompli* in cyberspace diverges from that in the conventional strategic environment. As referenced, Alexander George describes the *fait accompli* as a strategic bargaining concept adopted to change the status quo in the international system. The *fait accompli* describes strategic bargaining behavior in cyberspace only when states are seeking to alter the status quo within cyberspace by changing the conditions of security in their favor. This strategic interaction would be representative of *tacit bargaining*, which Harknett and I have described elsewhere.[21] That said, in the cyber competitive space most adversary cyber *faits accomplis* do not seek to change the status quo in cyberspace itself, but they often seek to cumulate strategic gains in, through, and from cyberspace to change the status quo in the international system. Thus, the *fait accompli* more often describes a strategic choice in the cyber competitive space than it describes strategic bargaining within the same. As my colleague Richard Harknett stated, "All strategic bargaining is competition, but not all strategic competition is bargaining."[22]

The *fait accompli*, then, while imperfect, is a more appropriate strategic concept than coercion (and its associated concepts) for describing and explaining states' cyber behaviors short of armed conflict. It accounts for both unilateral operations seeking gains from often significantly disparate targets and mutual efforts to routinely avoid operations that could justify armed retaliation. In 2012, former U.S. Secretary of Defense Leon Panetta expressed concerns regarding a cyber Pearl Harbor (i.e., a *fait accompli*) that were met with both skepticism and support.[23] This essay suggests that Panetta highlighted an important strategic concept upon which policymakers should be focused in cyberspace. However, by fixing only on the *fait accompli* as a potential strategic bargaining concept in the cyber strategic space of militarized crises and armed conflict, he failed to recognize the *fait accompli* as an adversary's actual, ubiquitous, and significantly consequential strategic choice in the cyber strategic competitive space short of armed conflict.

The *Fait Accompli*, Cyber Persistence Theory, and Persistent Engagement

Cyber persistence theory argues that, as the potential for exploitation is ever-present in cyberspace (i.e., the *fait accompli* is incentivized), and states are in constant contact due to interconnectedness, states must assume their sources of national power are vulnerable. From a national security perspective,

[21] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

[22] E-mail exchange on April 28, 2020.

[23] See, respectively, Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136, and Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense . . . and Is Possible," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405.

states must be concerned that core economic, political, social, and military capability and capacity could be undermined.[24] Thus, a state's only logical choice to ensure its security 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.

States acting on this cyber strategic imperative are, in fact, securing national interests in, through and from cyberspace from other states' cyber *faits accomplis*. The strategic principle of seizing the initiative is the essence of persistent engagement.[25] Understanding state's cyber behaviors as *faits accomplis* bolsters the argument for adopting a cyberspace strategy of persistent engagement, which anticipates the unilateral actions of aggressors and sets the conditions of security in the defender's favor.

Policy Implications

The *fait accompli* in the conventional strategic environment (the terrestrial frame) is described as a form of "partial deterrence failure."[26] Thus, policy recommendations for eliminating it as a viable adversary strategic bargaining choice are derived from coercion theory. Altman, for example, argues that precise, complete, and verifiable red lines (i.e., the part of a coercive demand that distinguishes compliance from violation) would discourage adversaries from adopting the *fait accompli* strategic bargaining option. If one were to embrace whole cloth the conventional environment's description of the *fait accompli* for cyberspace, policy recommendations would look the same. The 2018 National Cyber Strategy of the United States promotes this approach to cyber security, arguing that "increased public affirmation [of security enhancing standards] by the United States and other governments will lead to accepted expectations of state behavior" and strengthen the ability to deter.[27] There are other recent promotions of the same, calling for a stronger signaling strategy and declaratory policy.[28] Unfortunately, this misconstrues how the *fait accompli* concept actually applies to this competitive space, where the incentive for the strategic choice derives not from the absence of a declaratory policy or ambiguous red lines, but from the vulnerabilities inherent in cyberspace itself. When taking this perspective, the misalignment between a coercion-centric strategy and the strategic realities of the cyber competitive space becomes obvious and can be highlighted through an example.

Consider vulnerability CVE-2017-0144 in the Common Vulnerabilities and Exposures catalog.[29] While well known for prompting a more public disclosure of the United States' Vulnerabilities Equities Policy and Process, its value for this essay is in highlighting that, within two months of its public appearance (April 2017), an exploit of the vulnerability manifested as Wannacry ransomware. It then manifested one

[24] 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).
[25] Michael P. Fischerkeller, "The Cyberspace Solarium Report and Persistent Engagement," op. cit.
[26] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), pp. 536–540.
[27] *National Cyber Strategy of the United States*, The White House (September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[28] United States of America Cyberspace Solarium Commission, March 2020, https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline.
[29] https://cve.mitre.org/.

month later as Notpetya, a purely destructive attack disguised as ransomware; a couple of months later as Retefe, a banking trojan that routes traffic to and from the targeted banks through various proxy servers often hosted on the TOR network; and again in October 2017 as Wannamine, a cryptocurrency miner.[30,31] Assuming all of these behaviors are considered unacceptable, this set of very different CVE-2017-0144 exploits and their rapid sequential emergence presents implementation challenges that a security approach based on declaratory policy and red lines would struggle to overcome.

The range of gains for which CVE-2017-0144 was exploited illustrates how imaginative and clever adversaries seeking gains can be. States have demonstrated an abundance of creativity by routinely creating novel ways to exploit vulnerabilities in the pursuit of unilateral gains—exploitations that the United States most often learns of after the gain has already been realized. A coercion-centric strategy suggests two potential policy responses to this strategic reality. The first is to establish red lines and declaratory policy informed by *faits accomplis*—an *ex post* approach that would likely portend U.S. strategic decline as it is akin to putting on a bandage after one has already bled out. The second is to try to anticipate the novel gains states may seek and establish *ex ante* affiliated declaratory policy and red lines as a deterrent hedge. Cyberspace's brief history does not suggest that the United States, nor any other state, possesses such foresight—recall that CVE-2017-0144 was exploited for four different gains by different actors. Further, it is reasonable to expect novel gains are currently being contemplated as states continue developing innovative ways to exploit this now well-known vulnerability.[32] Emergent vulnerabilities compound this concern with another: a need for agility. It is unlikely the U.S government embodies the agility to quickly assess the novel gains states may seek through exploitation of an emergent vulnerability and transition that knowledge swiftly into declaratory policy and red lines before that vulnerability is widely exploited—consider that CVE-2017-0144's four different exploits manifested within seven months of its revelation. Given these implementation challenges to halting the *fait accompli* in the cyber strategic competitive space short of armed conflict (where most state cyber behavior manifests), declaratory policy and stronger signaling should not be a central focus of national cyber strategy.

Removing the *fait accompli* as a viable adversary strategic choice instead requires policies that support seizing the initiative in setting the conditions of security in cyberspace by exploiting adversary vulnerabilities and reducing the potential for exploitation of the state's own vulnerabilities (i.e., the strategic principle of persistent engagement). As an example of the latter, Harknett and I recently described Cyber Command's ongoing efforts to inoculate vulnerable systems from potential adversary exploitation by posting to VirusTotal adversary malware discovered through persistent operations.[33] This effort is complemented by persistent operations seeking out vulnerabilities themselves. Focusing on cyberspace's inherent vulnerabilities to obviate the *fait accompli* strategic choice requires no foresight regarding an adversary's purpose for exploiting vulnerabilities; rather, it only requires efforts

[30] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.
[31] Yiftach Keshet, "ETERNALBLUE: The Lethal Nation-state Exploit Tool Gone Wild", *Cynet*, January 2, 2020, https://www.cynet.com/blog/eternalblue-the-lethal-nation-state-exploit-tool-gone-wild/.
[32] SentinelOne, "Eternal Blue | The NSA Exploit that Just Won't Die," May 27, 2019, https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/.
[33] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," op. cit.

to discover vulnerabilities and assess their potential for exploitation. Mitigation, if warranted, or exploitation, if desired, can be pursued in a number of ways by various actors to preclude adversary *faits accomplis*. Consider, the National Security Agency's (NSA) recent sharing of the discovery of a critical Windows 10 vulnerability with Microsoft.[34] When sharing its discovery, the NSA assessed that it "makes trust vulnerable" and "places Windows endpoints at risk to a broad range of exploitation vectors."[35] By sharing it, Microsoft's January 14, 2020, patch effectively made *faits accomplis* non-viable for adversaries that might have targeted the vulnerability had it become widely known.[36] Harknett and I also recently referenced U.S. Cyber Command reportedly taking initiative to exploit vulnerabilities in the cyber infrastructure of the Internet Research Agency (IRA) in Russia to defend the 2018 U.S. mid-term elections.[37] These examples confirm that the United States is already acting to anticipate and address vulnerabilities through which states could execute *faits accomplis*. There is opportunity for improvement, however.

I recently asserted that persistent engagement's strategic principle should be the basis of a national cyber strategy and highlighted exemplars of ongoing efforts to seize the initiative and stem the tide of strategic effects from China's cyber-enabled illicit efforts to acquire intellectual property in, through, and from cyberspace.[38] All of these efforts are important, but some, including the Department of Justice's China Initiative, are reactions to gains already realized by adversaries and thus indicative of the United States contesting the outcomes of rather than precluding cyber *faits accomplis*.[39] Many of the recommendations in the Cyberspace Solarium Commission Report are indicative of the same, which signifies that the U.S. is playing catch-up. That is not to say the recommendations are not valuable—when you are behind, you must make up ground. As Congress considers legislative proposals informed by the Commission's recommendations, however, it should not advance such recommendations at the expense of supporting others that will better enable the United States to continuously anticipate and act, creating a necessary national capability for obviating the *fait accompli* as a viable strategic choice for adversaries. This capability is necessary if we are to get and stay ahead of our adversaries in a cyberspace environment where technology, terrain, targets (and their political value), capabilities, and intentions are ever-changing. From this perspective, two Cyberspace Solarium Commission recommendations stand out as candidates for fast tracking through the legislative process: Create or Designate Critical Technology Security Centers and Commit Significant and Consistent Funding toward Research and Development in Emerging Technologies.[40] These efforts would help the United States to

---

[34] National Security Agency | Cyber Security Advisory, "Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers," January 14, 2020, https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF.

[35] Davey Winder, "Windows 10 Security Flaw 'Makes Trust Vulnerable' Says NSA," *Forbes*, January 14, 2020, https://www.forbes.com/sites/daveywinder/2020/01/14/national-security-agency-confirms-windows-10-security-flaw-makes-trust-vulnerable/#2eba049cdb73.

[36] Neil Ziring, "A Very Important Patch Tuesday," January 14, 2020, https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2056772/a-very-important-patch-tuesday/.

[37] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect" op. cit.

[38] Michael P. Fischerkeller, "The Cyberspace Solarium Report and Persistent Engagement," op. cit.

[39] https://www.justice.gov/opa/page/file/1223496/download

[40] United States of America Cyberspace Solarium Commission, op. cit.

see around the vulnerabilities corner, stay ahead of its cyberspace adversaries, and consequently make the *fait accompli* in cyberspace a less viable strategic choice for adversaries.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-05-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategic Choice in Cyberspace: The Fait Accompli and Persistent Engagement	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-13214

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

This essay demonstrates how a lesser studied strategic bargaining concept—the *fait accompli*—better describes cyber behaviors short of armed conflict than does coercion and signaling. Moreover, because the strategic logic behind the *fait accompli* aligns with the structural imperative and strategic incentives identified by cyber persistence theory, it provides additional grounds for committing to a strategic approach of persistent engagement and adopting its core strategic principle of seizing the initiative in setting the conditions of security as an anchor for national cyber strategy.

15. SUBJECT TERMS

Fait accompli, persistent engagement, cyber strategy

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	7	19b. TELEPHONE NUMBER (Include Area Code)