#ACcyber

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

What Do We Know About Cyber Operations During Militarized Crises?

JANUARY 2022

MICHAEL P. FISCHERKELLER

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

EXECUTIVE SUMMARY

The Department of Defense (DoD) will soon kick off the drafting of its cyber strategy and cyber posture review to align US cyber capabilities and operating concepts with the foreign policy objectives of the Joseph Biden-Kamala Harris administration. Given that the administration describes China as the "pacing threat," debates over the best use of cyber operations and campaigns will likely be framed by US-China interaction in day-to-day competition, and by a potential militarized crisis and war over the status of Taiwan. This essay focuses on how cyber operations employed during militarized crises are likely to impact escalation management. Policymakers may be attracted to the idea that cyber operations could serve as de-escalatory offramps in a crisis. Such expectations should be tempered, if not completely set aside, for two reasons. First, there is no experience with cyber operations employed during a militarized crisis between two nuclear-armed peers. Absent direct experience, all one can rely on is academic research. Yet, secondly, deductive and empirical academic research provides no basis for confidence that cyber operations are either de-escalatory or non-escalatory in the context of militarized crises.[1] In fact, cyber operations intended as offramps in a crisis could have an outcome opposite than that intended. Given the absence of direct experience, policymakers must critically examine assumptions and claims that cyber operations can serve as de-escalatory crisis offramps.[2]

1 A version of this essay was simultaneously published by the author through the Institute for Defense Analyses: Michael Fischerkeller, "What Do We Know about Cyber Operations During Crises?" Institute for Defense Analyses, December 2021, https://www.ida.org/research-and-publications/publications/all/w/wh/what-do-we-know-about-cyber-operations-during-crises.

2 The 2021-2022 National Defense Authorization Act judiciously calls for an assessment of the current operational assumptions of US Armed Forces for cyber operations during potential crises. See S. 1605, 117th Congress National Defense Authorization Act (2021–2022), Section 1509, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.

A CONDITION OF CRISIS

Among international relations scholars, the term "crisis" describes a unique condition, qualitatively different from both war and day-to-day interactions in strategic competition short of armed conflict.[3] Although no consensus exists on specific indicators or measures of militarized crises, there is agreement that a militarized crisis comprises a national stake of strategic import, a heightened probability of war, and an increased salience of time.[4] Richard Ned Lebow, for example, describes a crisis as a condition in which policymakers "perceive that the action or threatened action of another international actor seriously impairs concrete national interests, the country's bargaining reputation, or their own ability to remain in power"; policymakers on both sides perceive themselves to be working under time constraints (not time per se, but a sense of urgency); and, policymakers perceive that any actions on their part designed to counter this threat (aside from capitulation) will raise a significant prospect of war.[5] These understandings and conceptualizations of "crisis" extend into US military doctrine, where the DoD describes a crisis as "a condition of such national security importance that the President or SecDef may consider a commitment of US military forces and resources to achieve or defend national objectives. Crises may evolve over time or develop quickly with little or no warning and require accelerated decision making."[6] This definition is offered for two reasons: to scope the arguments being made in this essay, and to properly contextualize claims made by others regarding the de-escalatory potential of cyber operations or options during crises.

A recognition of this unique condition of crisis spawned several significant bodies of empirical and deductive academic research investigating, respectively, what factors are associated with the onset of militarized crises between states and what strategic bargaining choices may increase or decrease the likelihood that a militarized crisis erupts into war. The deductive body of work provides the logical foundation for most of the arguments presented here, starting in the next section, which considers generally the serious deleterious consequences of key characteristics of cyber operations or options interacting with the core attributes of crises. Reversible cyber operations or options are then considered specifically, to contest the often-uncritical presumption that they will provide de-escalatory offramps in crises. Others' claims that cyber operations or options offer de-escalatory offramps and limit risk in crises are then properly contextualized, revealing their severely constrained policy relevance for crises. Finally, DoD cyber strategy and policy are considered in light of all of these arguments, which offers important insights that should be taken into account in cyber posture review and strategy deliberations.

3 See, for example: Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Glenn H. Snyder and Paul Diesing, *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton, NJ: Princeton University Press, 1977); Alexander L. George, ed., *Avoiding War: Problems of Crisis Management* (Boulder, CO: Westview Press, 1991).

4 See, for example: Russel J. Leng and J. David Singer, "Militarized Interstate Crises: The BCOW Typology and Its Applications," *International Studies Quarterly* 32, 2, June 1988, 155–173, https://www.jstor.org/stable/2600625; J. Joseph Hewitt, "Dyadic Processes and International Crises," *Journal of Conflict Resolution* 47, 5, October 2003, 669–692, https://doi.org/10.1177%2F0022002703252973.

5 Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore, MD: Johns Hopkins University Press, 1981), 10–12.

6 "Joint Publication 5.0, Joint Planning," US Department of Defense, December 1, 2020, I–12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf?ver=us_fQ_pGS_u65ateysmAng%3d%3d.

DEDUCTIVE RESEARCH ON CRISIS DYNAMICS AND CYBER OPERATIONS

Of the three core attributes of a crisis—strategic import, salience of time, and probability of war—the lion's share of scholarship focuses on the third, how misperceptions of intentions and actions could increase the probability of war between states.[7] When considering the role that cyber operations or options could play in crisis escalation management, prudent states must, therefore, consider if and how the characteristics of cyber operations impact this probability.[8]

Prudent Cyber Behavior in Militarized Crises and the Potential Unpredictability of Cyber Effects

The term "probability" suggests an element of uncertainty. As Thomas Schelling noted in his crisis bargaining scholarship, "The essence of a crisis is its unpredictability. The 'crisis' that is confidently believed to involve no danger of things getting out of hand is no crisis."[9] At a minimum, there is uncertainty regarding opponents' intentions. If each opponent knew what the other intended to do, and also knew its own intentions in light of that knowledge, there would be no uncertainty and, thus, no crisis.[10] Of course, actions follow from intentions, and so uncertainty and unpredictability regarding actions make an equally troublesome contribution to crises.[11] Unintended escalation, or "getting out of hand," has been delineated into two types: inadvertent and accidental escalation.[12] The current state of mutual understandings of responsible state behaviors in and through cyberspace, and the characteristics of cyber operations (or actions) themselves, increase, respectively, the probability of inadvertent and of accidental escalation in a militarized crisis.[13]

Inadvertent escalation occurs when a party deliberately takes an action it does not believe is escalatory, but which is interpreted as escalatory by another party to the crisis.[14] Such misinterpretation may be born of uncertainties over intentions, thresholds, or reference frames. Inadvertent escalation in a militarized crisis could result from the application of any instrument of national power or any military capability. The limited scope and immaturity of formal and informal mutual understandings of acceptable and unacceptable cyber behaviors in militarized crises, however, likely increase the probability of inadvertent escalation. Despite extensive formal, international efforts to establish a set of principles of "responsible behavior" in the context of cyberspace, today no comprehensive set addressing cyber capabilities exists that could serve to reduce uncertainties

7 The seminal volume examining the role of perception in international political decision-making, generally, is Robert Jervis, *Perceptions and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

8 This essay rests on the assumption that a condition of crisis differs from the conditions of day-to-day competition and war. Were this not the case, the terms would be analytically interchangeable, a position that no scholar of international relations would find tenable. Fischerkeller, Goldman, and Harknett argue in various forums that the novel strategic utility of cyber operations or campaigns rests in a condition of day-to-day competition, an argument derived from considerations of a strategic imperative and strategic incentives, presented by a cyber strategic environment that reinforces continuous, exploitative behavior in a competitive space, with a tacit upper bound short of use of force and armed-attack-equivalent effects. This essay presumes that those factors, and the behavior and bounded competitive space they engender, do not hold and are not present, respectively, in the distinct condition of militarized crisis as, by definition, militarized crises comprise coercive behavior that has breached the use-of-force ceiling of the competitive space. See, for example: Michel 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; Emily O. Goldman, "The Cyber Paradigm Shift," in Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, *Ten Years In: Implementing Strategic Approaches to Cyberspace* (Newport, VA: Naval War College Press, 2020), 31–46, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers.

9 Schelling, *Arms and Influence*, 97.

10 Snyder and Diesing, *Conflict Among Nations*, 8.

11 Along this line, it is instructive to consider "McNamara's Law," formulated by Robert McNamara, the US secretary of defense during the Cuban Missile Crisis: "In the nuclear age, it is impossible to predict with a high degree of certainty the effects of the use of military force by the superpowers, because the risks of accident, misperception, miscalculation, and inadvertence." Robert McNamara, "American View," in Graham T. Allison, William L. Ury, and Bruce J. Allyn, eds., *Windows of Opportunity: From Cold War to Peaceful Competition in U.S.-Soviet Relations* (Cambridge, MA: Ballinger Publishing Company, 1989), 127–130.

12 George, *Avoiding War*, 7–9.

13 Schelling, *Arms and Influence*, 97.

14 Forrest E. Morgan, et al., "Dangerous Thresholds: Managing Escalation in the 21st Century," RAND, 2008, 23.

regarding their use in a militarized crisis.[15] Although this has not yet resulted in inadvertent escalation, out of a condition of day-to-day competition and into militarized crisis, this observation should not be extrapolated to a condition of militarized crisis in which there are heightened tensions and increased time pressure to act.

The character of cyber operations increases a second risk of *accidental escalation*, in which the direct effects of an operational action are unintended by those who ordered the action.[16] Henry Farrell and Charles Glaser cite three factors of cyber operations that make their effects potentially unpredictable, despite planners' best efforts.[17] First, the complexity of the target system could render operational effects unpredictable by obscuring what might happen if the system is disrupted. Second, because most computer systems are not "air gapped," operational effects could unexpectedly spread across a network. Or, a network may serve both commercial and military purposes, such that an operation intending only counterforce effects (via targeting an opponent's military forces, installations, and assets) also causes countervalue effects (via impacting civilians, civilization infrastructure, and assets).[18] Third, operations that deliberately cause local physical, destructive effects could unpredictably cascade. For example, a cyberattack against computers controlling a micro-grid may be connected to a wide-area grid and lead to much more far-reaching damage. The potential for accidental escalation is heightened in a condition of militarized crisis, given the perception of urgency and increased concerns that an opponent is seeking immediate advantages. What under a non-crisis condition might be managed as an accident will more likely be perceived as suspicious in a crisis.[19]

These deductive conclusions regarding an increased likelihood of unintended escalation (inadvertent or accidental) are consistent with empirical findings on the perception of cyber operations during a crisis. In crisis scenario-based strategic war games conducted at the Naval War College from 2011 to 2016, participants believed that the use of cyber operations in a crisis would be escalatory. In all of the games, the participants—150–200 US government experts and senior leaders—were situated within crisis scenarios and then allowed to play all instruments of national power to resolve the crisis.[20] Over the many games analyzed, Jacquelyn Schneider noted in a WordPress posting that there was variation in the adversary, the intensity of the crisis, the participants, and the way cyber capabilities were designed into the games. However, the way players utilized cyber operations in the crises was "remarkably consistent" across the games: in five of the six games, players launched offensive cyber operations only after first launching conventional-weapons attacks.[21] "Over and over," Schneider states, "players cited concerns about escalation in their cyber restraint, articulating fears that cyberattacks could 'lead to nuclear war'" and that "cyber operations were generally viewed as highly escalatory."[22] Schneider noted that in one game, a player explaining their cyber restraint remarked "this is

15 The United Nations (UN) Group of Government Experts and Open-Ended Working Group processes are the most notable efforts in this regard. Recent reports from each make clear that, although states agree that the UN Charter applies in the context of cyberspace and that international humanitarian law applies to the context of cyber operations in armed conflict, there is no consensus on *how* either applies. See: "Report of the Group of Governmental Experts on Advancing responsible State Behaviour in Cyberspace in the Context of International Security," May 28, 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf; "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: A/AC.290/2021/CRP.2," United Nations General Assembly, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

16 Morgan, et al., *Dangerous Thresholds*, 26. For a discussion on how planners can attempt to decrease this likelihood, see: Steven M. Bellevin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, 1, March 2017, 59–68, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809463.

17 Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, 1, 2017, 7–17, https://www.semanticscholar.org/paper/The-role-of-effects%2C-saliencies-and-norms-in-US-Farrell-Glaser/59a81219fccac95bc954086df795919b341c1f95.

18 George H. Quester, *Deterrence Before Hiroshima* (New Brunswick: Transaction Books, 1986).

19 Richard Ned Lebow, "Accidents and Crises: The Dogger Bank Affair," *Naval War College Review* 31, 1, Summer 1978, 66–75, https://www.jstor.org/stable/44643155.

20 Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming," US Naval War College, 2017, https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf; Jacquelyn Schneider, "What War Games Tell Us About the Use of Cyber in Crises," Net Politics, June 21, 2018, https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.

21 Schneider, "What War Games Tell Us About the Use of Cyber in Crises."

22 Schneider, "Cyber and Crisis Escalation."

cyber—it's different psychologically."[23] Additional experimental research on public views of escalation in a crisis buttresses this claim by noting that, following a hypothetical operation targeting a US power plant by either cyber, conventional, or nuclear means, participants presented with the same means for an "escalatory" response were far more reluctant to escalate using cyber means; cyber options are perceived as qualitatively different.[24]

Reversible Cyber Operations in Crisis Bargaining

An additional feature of cyber operations to consider is their potential for offering reversible effects in crises, a feature that has become casually accepted as a virtue in some national security circles.[25] DoD's joint publication on cyber doctrine implies a de-escalatory role for reversibility by stating, "Effects that can be recalled, recovered, or terminated by friendly forces…may represent a lower risk of undesired consequences, including discovery or retaliation."[26] This is a dangerous presumption because it is professed without consideration of conditional context, such as an ongoing crisis.[27]

Most of the deductive scholarship on reversibility does not specify context. Herb Lin implied that reversibility is virtuous when broadly discussing "cyber conflict." He argued, "To the extent national decision makers have incentives to refrain from conducting offensive operations that might induce a strong kinetic reaction, the obvious approach would be to conduct cyberattacks that are in some sense smaller, modest in result, targeted selectively against less-provocative targets, and perhaps more reversible."[28] Lin and Max Smeets implied that reversibility is virtuous in their argument that "offensive cyber capabilities do have value in compellence. The potential opportunity for the [state seeking to compel] to control the reversibility of effect of an OCC [offensive cyber capability] may also encourage compliance [of the opponent]."[29] The opponent may know that, if it backs down, the "old" situation can be restored.[30] This reasoning describes reversible cyber operations as an offramp for an opponent—but, again, without specifying the context.

In a 2019 article, Richard Harknett and I proposed that reversibility is a virtue in the specific context of strategic competition short of militarized crises, because it allows a disaffected state to convey dissatisfaction with the status quo in a manner that facilitates managing the risk of escalation and avoiding a militarized crisis.[31] But, that work also did not address the conditional context of crisis itself.

The question of whether reversible cyber operations might (or might not) serve as valuable de-escalatory offramps in a crisis is best informed by previous scholarship on crisis bargaining and escalation dominance. The characteristics of the cyber strategic environment are not so peculiar as to obviate the relevance of the core arguments of this scholarship. Schelling argued that advantage in a crisis often goes to the one who arranges the status quo in his favor; that is, the one who achieves escalation dominance and leaves to his opponent the "last clear chance" to stop or turn aside to avoid disaster.[32] Herman Kahn makes clear in his seminal volume that escalation dominance is not merely (or necessarily) established through a favorable balance of capabilities. Another important factor is instilling in the opponent the fear of eruption into armed conflict, which, when translated into a crisis-management strategy, manifests as presenting the opponent with a last clear chance to avoid escalation into war.[33]

---

23 Schneider, "What War Games Tell Us About the Use of Cyber in Crises."

24 Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity* 5, 1, September 2019, https://doi.org/10.1093/cybsec/tyz007.

25 For a review of techniques of "reversibility," see: Neil C. Rowe, "Towards Reversible Cyber Effects," Proceedings of the 9th European Conference on Information Warfare and Security, July 2010, Thessaloniki, Greece, https://faculty.nps.edu/ncrowe/rowe_eciw10.htm.

26 "Joint Publication 3-12, Cyberspace Operations," US Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, 3-IV.

27 Recall that DoD doctrine recognizes a crisis as a condition, so this presumption is unfortunate.

28 Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, 3, Fall 2012, 46–70, https://www.jstor.org/stable/26267261.

29 Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2018, https://ccdcoe.org/uploads/2018/10/Art-03-Offensive-Cyber-Capabilities.-To-What-Ends.pdf.

30 Ibid.

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

32 Schelling, *Arms and Influence*, 44.

33 Herman Kahn (with a new introduction by Thomas C. Schelling), *On Escalation: Metaphors and Scenarios*, (London: Routledge, 2017), 290. This can be accomplished through a strategic posture, for example.

A defender leaving loopholes in its escalation dominance strategy—through which it can exit an implied or explicit commitment to escalate further—would undermine this necessary clarity.[34] Schelling argued that, in so doing, an opponent will expect the defender to be under strong temptation to make a graceful exit (or even a somewhat graceless one) from the crisis. This is precisely what reversible cyber operations may communicate: a weak commitment and, thus, an offramp *for the defender.* Successful crisis management offers an offramp *for the opponent* rather than introducing one for the defender. A defender employing a reversible cyber operation, which is communicated to an opponent as such, does not put the opponent in a position of having the last clear chance to avoid disaster. In fact, it places itself in that position by ceding escalation dominance through signaling a lack of will, thereby inviting an opponent to consider intensifying their activities. As a crisis option, reversible cyber operations are a vice, rather than a virtue, as they undermine a core tenet of crisis management. Therefore, if the United States wants to offer an opponent an escalation offramp in the midst of a crisis, rather than employ a reversible cyber option, it should take heed of Kahn's comment that "there are typical de-escalation gestures that do not have the simple character of a reversal of a previous escalation."[35]

The immaturity of mutual understandings of prudent cyber behavior in militarized crises and the potential unpredictability of cyber operations' effects, when coupled with the wargaming findings previously cited, suggests that cyber operations or options independently employed in a crisis are as likely—or, arguably, more likely—to increase the likelihood of unintended escalation as they are to provide a stabilizing, non-escalatory function or serve as a de-escalatory offramp. Crisis-bargaining scholarship applied in the context of cyberspace also supports the conclusion that reversible cyber operations employed in crises will not serve as de-escalatory offramps; rather, they will more likely encourage escalatory adventurism by an opponent.

Notably, this conclusion sharply contrasts with proliferating claims offered in a previous Atlantic Council Issue Brief summarizing research findings regarding the relationship between cyber operations or options and escalation. The basis for this discordance is important for the US policy community to understand as the drafting of a new cyber strategy begins, as well as for academic practitioners working to advance collective understanding of escalation for, and critically within, militarized crises.

CONTEXTUALIZING AND SCOPING DE-ESCALATORY CLAIMS

In a November 2019 Atlantic Council Issue Brief entitled *What Do We Know About Cyber Escalation: Observations from Simulations and Surveys*, Benjamin Jensen and Brandon Valeriano summarize empirical research that, they claim, provides insights into "how cyber operations alter how states *respond to international crises*."[36] Based on the authors' empirical study of cyber rivals, the brief asserts that cyber operations "have tended to offer great powers escalatory offramps" to shape an adversary's behavior without engaging military forces and risking military escalation.[37] Additionally, citing other simulation and survey research they've conducted, Jensen and Valeriano claim that "cyber options can help de-escalate deadly militarized disputes" and "limit risk."[38] However, these claims are extrapolations rather than direct findings, as none of the research designs

34 Schelling, *Arms and Influence*, 48.

35 Kahn, *On Escalation*, 231–232.

36 Author's emphasis. See: Benjamin Jensen and Brandon Valeriano, *What Do We Know About Cyber Escalation: Observations from Simulations and Surveys*, Atlantic Council, November 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf. For an associated essay, see: Brandon Valeriano and Benjamin Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran," *Washington Post*, June 25, 2019, https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

37 Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018); Jensen and Valeriano, *What Do We Know About Cyber Escalation*.

38 Ibid.

for the work cited are structured to support these claims. Consequently, from a prescriptive perspective, the 2019 issue brief should not be a basis of policy guidance for crisis management. The research cited is not without merit, but it is important to understand what the research was and was not designed to investigate, so that its findings are properly contextualized and scoped.[39]

In previous work, Valeriano, Jensen, and Ryan Maness concluded that cyber operations employed between rival states are not correlated with escalation to crisis or war.[40] This finding aligns with research by Goldman, Harknett, and I, which concludes that cyber operations employed below the threshold of armed conflict have not escalated into militarized crisis or war.[41] Valeriano et al.'s findings do not provide insights into *how states respond to international crises*; nor do they support the claim that cyber operations in the context of crisis offer *escalatory offramps*. Conclusions from studies of rivalrous disputes, militarized or cyber, speak to day-to-day competition between rivals, not crisis behaviors.

Extrapolating research findings from day-to-day competition to a condition of crisis is an unsound scientific practice, and a potentially dangerous policy practice. Just how unsound it is can be illustrated by the work of several militarized interstate disputes (MIDs) scholars who were interested in gaining insights into rivals' behaviors *during* crises.[42] Recognizing that militarized disputes are not ipso facto crises, these scholars constructed crisis datasets to complement the MIDs dataset. An important initial insight from one of those efforts was summarized by J. Joseph Hewitt, who noted that when correlating a dataset of crises to militarized disputes identified in the MIDs dataset, only 23 percent of militarized disputes actually included a crisis event.[43] A review of the cyber disputes populating the cyber rivals dataset reveals an even more startling percentage—zero. That is, not a single dispute in the dataset includes an incident that would be considered a crisis event, as crisis is described by scholars of international relations.[44]

One need only consider the deductive arguments presented earlier to conclude just how potentially dangerous extrapolating day-to-day competition findings to a condition of crisis could be as a policy practice. The deductive arguments conclude that using cyber operations during a crisis will increase the likelihood of unintended escalation, an opposite and far more dangerous outcome.

Additionally, in their 2019 piece, Jensen and Valeriano summarize empirical research that, they claim, shows how "cyber options can help de-escalate deadly militarized disputes" and "limit risk."[45] Instead, their research placed participants in a rivalrous relationship and a current condition of militarized crisis *in order to ascertain if the presence of cyber options, in and of itself, leads to escalatory cyber behavior*.[46] Thus, their claim that "the findings were clear: Cyber options can help de-escalate deadly militarized disputes" is well beyond the scope of their inquiry.[47]

In order to support a conclusion that *cyber options can help de-escalate deadly militarized disputes and limit risks during crises*, a research design would need to be structured to examine whether specific response choices helped to de-escalate, stabilize (reciprocate), or escalate militarized disputes or crises. The 2019 Jensen and Valeriano brief is not structured in this manner. Rather, it examines whether participants who were already predisposed to de-escalate, absent any awareness of potential response choices, tended to prefer cyber options that were pre-designated as being de-

39 For a more comprehensive review of the research cited in this issue brief, see: Michael P. Fischerkeller, "IDA NS D-32909, What Do We Know About Cyber Operations During Crises," 2021, https://www.ida.org/research-and-publications/publications/all/w/wh/what-do-we-know-about-cyber-operations-during-crises.

40 Valeriano, Jensen, and Maness, *Cyber Strategy*.

41 These views are summarized in Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence: Redefining National Security in Cyberspace* (New York: Oxford University Press, forthcoming), https://bridgingthegapproject.org/btgseries-2/.

42 See, for example, Russel J. Leng and J. David Singer, "Militarized Interstate Crises: The BCOW Typology and Its Applications," *International Studies Quarterly* 32, 2, June 1988, 155–173, https://www.jstor.org/stable/2600625; J. Joseph Hewitt, "Dyadic Processes and International Crises," *Journal of Conflict Resolution* 47, 5, October 2003, 669–692, https://doi.org/10.1177%2F0022002703252973.

43 Hewitt, "Dyadic Processes and International Crises," 679. The classification of crises in the International Crisis Behavior dataset was quite similar to Lebow's description; i.e., a crisis hinges on the presence of three necessary conditions: a perception of a threat to one or more basic values, a perception of finite time for response to the value threat, and a perception of heightened probability of involvement in military hostilities.

44 To review the codebook, see: Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, "Code Book for the Dyadic Cyber Incident and Dispute Dataset (Version 1.1)," http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.1_codebook.pdf. The dataset itself is available at https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.

45 Ibid.

46 This research design was motivated, in part, by Ben Buchanan's argument that this is likely to be the case. Ben Buchanan, *The Cyber Security Dilemma: Hacking, Trust, and Fear Between Nations* (London: Oxford University Press, 2016).

47 Valeriano and Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran."

escalatory, a designation (and conclusion) determined by the researchers themselves.[48] The authors concede, "The question remains how the opposition is likely to perceive these moves. Will they recognize them as methods to tamp down the drums of war or see them as aggressive moves that require escalatory responses?" Nevertheless, they continue with the claim that "[s]ocial science research suggests the public and military operators view these cyber moves as ways of avoiding war."[49] This conclusion relates only to the perception of the actor that employed the cyber operation or option, and is substantively distinct from the assertion that "cyber operations offer a valuable escalatory offramp."[50]

STRATEGY AND POLICY IMPLICATIONS

As policymakers in strategy and posture review deliberations debate how to maximize the effectiveness of US cyber capabilities across the strategic-competition continuum, they should recognize that the utility of cyber means varies across the conditions of competition, militarized crisis, and war (which is not unique to cyber means). At this time, there is no deductive or empirical evidence to support a prioritized investment in, or the deployment of, independent cyber operations or options for crisis management. In fact, the evidence suggests that this policy choice may, more likely than not, result in unintended escalation under a condition of crisis. This is particularly likely with regard to reversible cyber operations in the context of a China-Taiwan crisis. As Michelle Flournoy has argued, China holds "strong beliefs" that the United States is a declining power, so any reversible cyber operation employed by the United States will likely be viewed as weakness.[51]

Cyber scholarship is providing increasingly precise recommendations about how policymakers can leverage cyber capabilities independently and in conjunction with other military capabilities and non-military national instruments of power. This essay argues for a de-emphasis on independent cyber operations or options for crisis management. Instead, when coupled with near-consensus views by scholars that independent cyber operations or options lack direct utility for strategic deterrence, policymakers would be prudent to maximize the novel independent strategic contribution that cyber capabilities can make to security: inhibiting adversaries' continuous efforts to cumulate gains in strategic competition short of militarized crisis and war.[52]

Much of the 2018 DoD cyber strategic approach of defend forward and persistent engagement should continue to anchor the next DoD cyber strategy.[53] Not only does the 2018 strategic approach position the United States to compete with adversaries in the cyber strategic competitive space short of militarized crises and war, but it helps set the conditions for success in and through cyberspace should either of those contingencies come to pass. Cyber capabilities can support crisis and contingency operations not primarily through episodic, independent operations or options during crises, but through continuous campaigning in day-to-day strategic competition to set the conditions for success before crises and war erupt.

The next cyber strategy should adopt and support the position that continuous campaigning in day-to-day competition can aid in the construction of tacit agreements comprising mutual understandings of acceptable and unacceptable non-coercive cyber behaviors.[54] It is important for scholars and policymakers

48 After participants were placed in a rivalrous crisis scenario, and before seeing any possible response options, they were asked to specify their response posture; i.e., if they wanted to de-escalate, respond proportionally, or escalate. Thus, before reviewing any response options, participants had declared their predispositions for managing the crisis.

49 Valeriano and Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran."

50 Jensen and Valeriano, *What Do We Know About Cyber Escalation*.

51 Michele A. Flournoy, "How to Prevent a War in Asia," *Foreign Affairs*, June 18, 2020, https://www.foreignaffairs.com/articles/united-states/2020-06-18/how-prevent-war-asia.

52 See, for example: Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND, 2009; Martin C. Libicki, "Crisis and Escalation in Cyberspace," RAND, 2012; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, 2, Fall 2013, 41–73, https://www.belfercenter.org/sites/default/files/files/publication/IS3802_pp041-073.pdf; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies* 24, 2, 2015, 316–348, https://www.tandfonline.com/doi/full/10.1080/09636412.2015.1038188; Jon R. Lindsay, "Cyber Espionage," in Paul Cornish, ed., *The Oxford Handbook of Cyber Security* (New York: Oxford University Press, January 2022), https://global.oup.com/academic/product/the-oxford-handbook-of-cyber-security-9780198800682?cc=us&lang=en&#; Erica D. Borghard and Shawn Lonergan, "The Logic of Coercion in Cyberspace," Security Studies 26, 3, 2017, 452–481, https://doi.org/10.1080/09636412.2017.1306396; Martin C. Libicki, "Expectations of Cyber Deterrence," *Strategic Studies Quarterly*, Winter 2018, 44–57, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf; Fischerkeller, et al., *Cyber Persistence*.

53 The strategy's reference to deterring adversaries should instead be updated to reflect the notion of setting conditions for the success of a deterrence strategy.

54 Most state behaviors in day-to-day competition are best described as being exploitative, not coercive, whereas a militarized crisis is characterized by coercive behaviors. Thus, tacit norms constructed through operational interactions in day-to-day competition would comprise understandings regarding non-coercive (exploitative) behaviors. See: Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence Theory, Intelligence Contests, and Strategic Competition," *Texas National Security Review*, September 17, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

to recall that many Cold War tacit "rules of prudence" were constructed through observing the operational behaviors of the opponent, rather than through formal deliberations at the United Nations to arrive at mutually agreed-upon principles.[55] Indeed, US and Soviet scientists and scholars concluded that even though such rules were "ambiguous, fuzzy at the edges, and evolving," where they became embedded in interpretations of self-interest "they constrained behavior much more powerfully than would mere declarations of principle."[56]

Policymakers should recognize that the tacitly bounded cyber strategic competitive space short of armed conflict, in which day-to-day cyber competition plays out, is—like the United Nations—a strategic venue in and through which rules of prudence, or norms, can be constructed. Such norms would speak directly to responsible, non-coercive cyber behaviors, and serve to reduce the likelihood of unintended escalation from day-to-day competition into militarized crises. They would further serve to reduce the likelihood of unintended escalation from employing independent cyber operations or options of that same character in a militarized crisis. While the United Nations supports an institutional approach, the tacit strategic competitive space supports a behavioral/operational approach. These approaches are complementary; pursuing them simultaneously would create a norms-construction process that is more stable, comprehensive, and faster than either approach provides independently.

Finally, the next DoD cyber strategy should continue to call for the use of cyber capabilities in concert with other military capabilities and non-military instruments of national power to bring armed conflict to a swift and decisive conclusion. Cyber capabilities coupled as such in a condition of war can complement the coercive effects of conventional capabilities and other instruments. They can also provide novel options for disrupting, degrading, or destroying targets whose profiles challenge the efficacy of non-cyber military options and non-military instruments of power.

CONCLUSION

There is still much research to do on the role that independent cyber operations or options play, or could play, in militarized crises. This essay intended to make clear through deductive research, and a review of recent claims, what cyber policy actions in a condition of crisis are prudent. Uncertainties regarding mutual understandings of acceptable or unacceptable cyber behaviors, and the unpredictability of cyber operations' effects, support a deductive conclusion that independent cyber operations or options in a condition of crisis may increase the likelihood of unintended escalation, rather than provide a stabilizing, non-escalatory function or serve as a de-escalatory offramp. Additionally, crisis-bargaining scholarship applied to the context of cyberspace supports a deductive conclusion that reversible cyber operations—considered by some to be a valuable option in the midst of a crisis, because they hypothetically offer an offramp to an opponent—arguably serve an opposite purpose, ceding escalation dominance to an opponent and, thus, potentially encouraging escalatory adventurism by the same. Research findings that are extrapolated to suggest otherwise are not based on research designs that can support such claims. Thus, what is known about cyber operations in militarized crises is limited, and that limited knowledge suggests caution should be the starting point of any crisis-management strategy considering independent cyber operations or options.

Michael P. Fischerkeller is a research staff member in the Information, Technology and Systems Division at the Institute for Defense Analyses, where he has spent nearly 20 years supporting the Office of the Secretary of Defense, Joint Chiefs of Staff, and Combatant and Multi-National Force commanders.

The author would like to thank Dr. Emily Goldman and Dr. Richard Harknett for their input and comments on previous drafts of this article.

CYBER STRATEGY SERIES

The Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security, presents the Cyber Strategy Series to curate and present new and expanded perspectives on the most pressing topics in cybersecurity strategy. This series is intended to challenge existing assumptions and spark discussion, to help build a better understanding of how the United States can and should operate in the cyber domain.

55 Michael P. Fischerkeller, "Initiative Persistence and the Consequence for Cyber Norms," Lawfare, November 8, 2021, https://www.lawfareblog.com/initiative-persistence-and-consequence-cyber-norms.

56 Graham T. Allison, "Primitive Rules of Prudence: Foundations of Peaceful Competition," in Allison, et al., eds., *Windows of Opportunity*, 9–37.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org