INSTITUTE FOR DEFENSE ANALYSES

What Do We Know about Cyber Operations During Crises?

Michael P. Fischerkeller, Project Leader

December 2021

IDA Non-Standard D-32909

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 HQ0034-19-D-0001, Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," 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.

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

What Do We Know about Cyber Operations During Crises?

Michael P. Fischerkeller

The Department of Defense (DoD) will soon kick-off the drafting of its cyber strategy and cyber posture review to align U.S. cyber capabilities and operating concepts with the foreign policy objectives of the Biden-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 U.S.-China interaction in day-to-day competition and in a potential militarized crisis and war over the status of Taiwan. This essay focuses on how cyber operations employed in militarized crises are likely to impact escalation management. Policymakers may be attracted to the idea that cyber operations could serve as de-escalatory offramps to manage escalation in a crisis. Such expectations should be tempered for two reasons. First, we have no experience with cyber operations employed during a militarized crisis between two nuclear-armed peers. Absent direct experience, all we can rely on is academic research. Yet, secondly, existing empirical and deductive academic research provides no basis for confidence that cyber operations are either de-escalatory or non-escalatory in the context of crises. In fact, employing cyber operations intended as offramps in a crisis could have the opposite intended outcome—reversibility, for example, is a vice and not a virtue in crises. Given the absence of direct experience, policymakers must critically examine research claims that cyber operations can serve as crisis offramps. Prudent policy and resource allocation requires rigor in assessing the effectiveness of cyber capabilities in competition, crises, and war.

Empirical Research on Cyber Operations and Crises

A 2019 Atlantic Council Issue Brief summarized empirical research investigating the question of whether cyber operations alter how states respond to international crises in a way that creates incentives for decision makers to cross the Rubicon and use military force to settle disputes.[1] Based on the authors' own empirical study of cyber rivals,[2] 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.[3] Citing other simulation and survey research, the brief also claims that "cyber options can help de-escalate deadly militarized disputes" and "limit risk."[4] However, these claims are extrapolations rather than direct findings because the research designs employed were not structured to address the question of whether cyber operations during militarized crises are de-escalatory. Consequently, the research does not directly help us understand the impact of cyber operations on crisis management and, from a prescriptive perspective, does not provide empirical or deductive guidance to

[1] See Benjamin Jensen and Brandon Valeriano, "What Do We Know About Cyber Escalation: Observations from Simulations and Surveys," Atlantic Council Issue Brief, November 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf, and Brandon Valeriano and Benjamin Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran," MonkeyCage, June 25, 2019, https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

[2] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

[3] Jensen and Valeriano, "What Do We Know About Cyber Escalation."

[4] Ibid.

policy, or more specifically, crisis decision making about if and how cyber operations should be employed during militarized crises. It is important to understand what this research was designed to investigate and what it did not.

Cyber Rivals

A large body of scholarship on rivalries defines a *rivalry* as a long-standing animosity with a high degree of competitiveness and a series of reciprocated engagements over a long period of time.[5] In their 2018 book, Valeriano, Jensen, and Maness built on this body of work to construct a dataset of "cyber rivals" and to assess if the use of cyber operations increases the likelihood that a crisis or war might erupt among rivals.[6] Starting with a set of rivalrous dyads primarily identified in this body of scholarship, Valeriano et al. reviewed open-source data on rival states' cyber behaviors from 2000–2014.[7] Cyber behaviors are coded as cyber incidents, where an *incident* is defined as "an event comprising a manipulation of code or hardware for malicious purposes."[8] Additionally, a *cyber dispute* is said to comprise a series of cyber incidents between two rivalrous states over a limited period of time.

The authors concluded that cyber operations employed between rival states are not correlated with escalation to crisis or war. This finding aligns with research that concludes cyber operations employed below the threshold of armed conflict have not escalated into militarized crisis or war.[9] Importantly, however, the finding that cyber operations between rivals do not correlate with escalation into crises or war tells us nothing about whether cyber operations employed during a crisis are de-escalatory or non-escalatory. Studying disputes, militarized or cyber, is not the same as studying crisis. Dispute is a particular form/classification of relations between states, whereas a crisis is a specific condition under which interstate relations are conducted.

This distinction between "relations" and "conditions" originally surfaced in the scholarship on militarized interstate disputes (MIDs) and rivalries in the 1980s.[10] Recognizing that disputes should not *ipso facto* be considered crises, MIDs scholars interested in gaining insights into rivals' behaviors during crises

---

[5] On rivalries, see, for example, James P. Klein, Gary Goertz, and Paul F. Diehl, "The New Rivalry Dataset: Procedures and Patterns," *Journal of Peace Research* 43, no. 3 (2006): 331–348, https://doi.org/10.1177/0022343306063935 and William R. Thompson, "Identifying Rivals and Rivalries in International Politics," *International Studies Quarterly* 45, no. 4 (December 2001): 557–586, https://www.jstor.org/stable/3096060.

[6] Valeriano, Jensen, and Maness, *Cyber Strategy*. For a deep dive on the U.S.-Iran rivalry over the period early-2019 to July 2020, see Matthias Schulze, Josephine Kerscher, and Paul Bochtler, "Cyber Escalation: The Conflict Dyad USA/Iran as a Test Case," SWP Working Paper No. 1, December 2020, https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Schulze_December20_Cyber_Escalation_Research_01.pdf. For a typology of how states employ cyber operations in interstate disputes, see Florian J. Egloff and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," *Journal of Global Security Studies* 7, no. 1 (2021): 1–18, https://doi.org/10.1093/jogss/ogab028.

[7] The primary sources for rivals are Klein, Goertz, and Diehl, "The New Rivalry Dataset: Procedures and Patterns" and Thompson, "Identifying Rivals and Rivalries in International Politics." Valeriano et al. added the rivals of Russia in the post-Soviet era (Estonia, Lithuania, Georgia, and Ukraine). See Valeriano et al., 56 (fn 3).

[8] Valeriano, Jensen, and Maness, *Cyber Strategy*, 57.

[9] These view 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/.

[10] See, for example, Charles S. Gochman and Zeev Maoz, "Militarized Interstate Disputes, 1816–1976," *Journal of Conflict Resolution* 28, no. 4 (December 1984): 585–616, https://doi.org/10.1177/0022002784028004002.

pursued additional efforts to remedy this weakness in the MIDs dataset. A summary of their efforts reveals the dangers of extending findings about rivalrous disputes to the context of managing crises.

MIDs scholars used the Correlates of War[11] (COW) dataset to code individual military acts (incidents) into temporally bound "militarized interstate disputes."[12] From this work, the initial concept of "rivalry" was birthed, providing an important history-informed context for identifying factors associated with the onset of crises or war.[13] To complement the COW dataset, parallel dataset-building efforts proceeded to "obtain more microscopic descriptions of conflict bargaining" to identify factors that lead to escalation during international crises.[14]

Early on, scholars recognized that interstate crises are qualitatively different from militarized disputes among rival states.[15] MIDs scholars Russel Leng and J. David Singer characterized a militarized interstate crisis as when "a member of the interstate system on each side of the dispute indicates by its actions its willingness to go to war to defend its interests or to obtain its objectives."[16] No scholarly consensus exists on the sufficient conditions for classifying a militarized dispute as a crisis, although there is agreement that a necessary distinguishing feature of crisis is a dangerously high probability of war, which Leng and Singer operationalized as the presence of a threat of force, display of force, or the use of force by both sides.

When applying this criterion to the MIDs dataset, only 62 percent of all militarized disputes qualified as crises. Additionally, Leng and Singer applied a second common behavioral manifestation of crisis: an unusually high intensity of interaction between the participants on the two sides, which they associated with the perceptual phenomenon of a sense of time pressure. While they did not report how much applying this additional criterion further reduced the set of militarized disputes that could be classified as militarized crises, other researchers using a similar definition of crisis did. The classification of crises in the International Crisis Behavior dataset 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.[17] When

---

[11] https://correlatesofwar.org/data-sets.

[12] Gochman and Maoz, "Militarized Interstate Disputes, 1816–1976."

[13] See Daniel M. Jones, Stuart A. Bremer, and J. David Singer, "Militarized Interstate Disputes, 1816–1992: Rationale, Coding Rules, and Empirical Patterns," *Conflict Management and Peace Science* 15, no. 2 (September 1996): 163–213, https://doi.org/10.1177%2F073889429601500203.

[14] See, for example, Russel J. Leng and J. David Singer, "Militarized Interstate Crises: The BCOW Typology and Its Applications," *International Studies Quarterly* 32, no. 2 (June 1988): 155–173, https://www.jstor.org/stable/2600625 and J. Joseph Hewitt, "Dyadic Processes and International Crises," *Journal of Conflict Resolution* 47, no. 5 (October 2003): 669–692, https://doi.org/10.1177%2F0022002703252973.

[15] See, for example, 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 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

[16] Leng and Singer, "Militarized Interstate Crises," 159.

[17] Hewitt, "Dyadic Processes and International Crises," 671. Also see Michael Brecher, *Crises in World Politics: Theory and Reality* (Oxford: Pergamon Press, 1993). This perception-based set of conditions is similar to the conditions proposed by Lebow: policy-makers perceive that the action taken or threatened by another international actor seriously impairs concrete national interests, the country's bargaining reputation, or own ability to remain in power; policy-makers on both sides perceive themselves to be working under time constraints (not time, per se, but sense of urgency); and policy-makers perceive that any actions (aside from capitulation) will raise a significant probability of conflict. Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore, MD: Johns Hopkins University Press, 1981).

mapping this characterization of crisis to the MIDs dataset, J. Joseph Hewitt concluded that only 23 percent of militarized disputes included a crisis event.[18]

In sum, MIDs scholars explicitly recognized that inferences from researching militarized disputes should not be made to crisis behavior.[19] Consequently, they created separate datasets based on generally agreed-upon criteria for identifying a crisis, where one dataset was culled from the larger militarized dispute dataset and another was constructed from other data sources. The Valeriano et al. dataset examines disputes, not crises, among cyber rivals. Moreover, no cyber disputes in their dataset satisfy the characterizations of crisis based on the consensus of international relations scholars. Therefore, practitioners and scholars should be skeptical of claims or inferences derived from the cyber rivalry dataset for whether cyber operations are de-escalatory or non-escalatory in crises.

Surveys and Simulations

The Issue Brief also argues that simulation and survey research further support the claim that cyber options can help de-escalate deadly militarized disputes and limit risk. Yet, again, this research is not structured to assess whether cyber options or operations are de-escalatory or non-escalatory in a crisis (or limit risk in the same).

The research cited in the brief to justify the de-escalatory claim placed simulation and survey participants in a rivalrous relationship and a condition of militarized crises to ascertain if the presence of cyber options, in and of itself, leads to escalatory cyber behavior. According to the authors, their research design was motivated in part, by Ben Buchanan's argument that this is likely to be the case.[20] The authors claim that "the findings were clear: Cyber options can help de-escalate deadly militarized disputes."[21] Yet this conclusion is well beyond the scope of their inquiry. Understanding how they arrived at this claim, therefore, is critical.

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.[22] Response options aligned to each of these postures were pre-designated by the researchers. Once participants' postures were communicated, half were given a set of pre-designated response options that included cyber and non-cyber options, and half were given a set of pre-designated response options including only non-cyber options. To summarize, the posture preferences across the two groups for de-escalation, proportional response, and escalation were proportionally similar (which serves as an important control); participants who wanted to de-escalate

---

[18] Ibid, 679.

[19] See, for example, Michael Colaresi and William R. Thompson, "Strategic Rivalries, Protracted Conflict, and Crisis Escalation," *Journal of Peace Research* 39, no. 2 (May 2002): 262–287, https://doi.org/10.1177%2F0022343302039003002.

[20] Ben Buchanan, *The Cyber Security Dilemma: Hacking, Trust, and Fear Between Nations* (London: Oxford University Press, 2016).

[21] Valeriano and Jensen, "How cyber operations can help manage crisis escalation with Iran."

[22] See, Benjamin Jensen and Brandon Valeriano, "Cyber Escalation Dynamics: Results from War Game Experiments," International Studies Association, Annual Meeting Panel: War Gaming and Simulations in International Conflict, March 27, 2019, http://web.isanet.org/Web/Conferences/Toronto%202019-s/Archive/71e7820c-e61c-4187-ab8c-28de83dfd660.pdf and Jensen and Valeriano, "What Do We Know About Cyber Escalation?"

and had pre-designated de-escalatory cyber options in their response set tended to use those options; those who wanted to escalate and had pre-designated escalatory cyber operations in their response set tended to not use those cyber options.

To support a conclusion that *cyber options can help de-escalate deadly militarized disputes* and *limit risks* during crises, a research design would have to be structured to examine whether specific response choices helped to de-escalate, stabilize (reciprocate), or escalate militarized disputes or crises. The Valeriano and Jensen research is not structured in this manner—rather, it examines whether participants who were already predisposed to de-escalate absent awareness of potential response choices tended to prefer cyber options that were pre-designated as being de-escalatory, a designation (and conclusion) determined by the researchers themselves. Valeriano and Jensen conceded that "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 continued with the claim that "[s]ocial science research suggests the public and military operators view these cyber moves as ways of avoiding war."[23] In fact, this question is not answered by this research, nor, given its research design, could it be.

Cyber Operations and Crisis Dynamics

The 2019 Issue Brief further cited research findings that participants in wargames are reluctant to employ cyber operations during a militarized crisis. However, these findings do not speak to the de-escalatory claims in the brief and do not inform the question of whether cyber operations are de-escalatory or non-escalatory in crises. For example, the brief cited an analytic wargaming approach using a fictitious militarized crisis scenario between the United States and China.[24] In the wargame, after the participants are introduced to the scenario, they are then given a range of action cards: cyber actions, which generally allow players to snoop on their opponents and subtly degrade their capabilities; military actions; and diplomatic actions. On each turn, a player attempts some (or no) actions, which are assessed by an umpire who determines whether or not the players' choices were successful by rolling a die. After resolving the actions, the umpire sends players a report with updates, and the next turn begins. In the course of eight games (three turns for each player), both sides (participants representing the U.S. and China) were less aggressive than expected, even in regard to their use of offensive cyber operations. Notably, the authors of this research do not draw any escalation-management-related conclusions regarding why participants were cautious in their use of cyber options in crises because their research design did not accommodate investigating this specific question.

Other research cited in the Issue Brief actually concluded that cyber operations are viewed as escalatory in crises, which is contrary to the Brief's de-escalatory claims. A review of crisis scenario-based strategic war games conducted at the Naval War College from 2011 to 2016 reported that participants believed that the use of cyber operations in a crisis would be perceived as escalatory. In all of the games, the participants—150–200 U.S. government experts and senior leaders—were situated within crisis

[23] Valeriano and Jensen, "How Cyber Operations Can Help Manage Crisis Escalation with Iran."
[24] Benjamin Jensen and David Banks, *Cyber Operations in Conflict: Lessons from Analytic Wargames* (Center for Long-Term Security, 2016), https://cltc.berkeley.edu/wp-content/uploads/2018/04/Cyber_Operations_In_Conflict.pdf .

scenarios and then allowed to play all instruments of national power to resolve the crisis.[25] Over the many games analyzed, the author noted in a WordPress posting variation in the adversary, the intensity of the crisis, the participants, and the way cyber capabilities are 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.[26] "Over and over," the author states, "players cited concerns about escalation in their cyber restraint, articulating fears that cyberattacks could 'lead to nuclear war'"[27] and that "cyber operations were generally viewed as highly escalatory."[28] The author noted that in one game, a player explaining their cyber restraint remarked "this is cyber—it's different psychologically."[29] Additional experimental research on public views of escalation in a crisis buttresses this claim by noting that, following a hypothetical operation targeting a U.S. power plant by either cyber, conventional, or nuclear means, participants presented the same means for an "escalatory" response were far more reluctant to escalate using cyber means—cyber options are perceived as qualitatively different.[30]

In sum, none of this cited crisis scenario-based research speaks to the Issue Brief's claims of de-escalatory offramps or answers the question of whether cyber operations are de-escalatory or non-escalatory in crises. Some of the findings actually cast doubt on the Brief's claim that cyber options may "limit risk" in a crisis. The pairing of a qualitatively different means (cyber operations vs. other instruments of national power) with a qualitatively different interstate dynamic (crises vs. day-to-day competition) seems to increase, not limit, perceptions of risk of inadvertent or accidental escalation. This alternative viewpoint is far more consistent with deductive research examining how the characteristics of cyber operations may affect crisis dynamics.

Deductive Research on Cyber Operations and Crises

What are the particular qualities of cyber operations that feed fears of inadvertent escalation in crises?[31] Uncertainty likely tops the list. In the definitions of crises presented thus far, a dangerous probability of

---

[25] See Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming," https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf and 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.

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

[27] Ibid.

[28] Schneider, "Cyber and Crisis Escalation."

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

[30] Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics," *Journal of Cybersecurity* 5, no 1 (September 2019), https://doi.org/10.1093/cybsec/tyz007.

[31] 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 fora that the novel strategic utility of cyber operations/campaigns rests in a condition of day-to-day competition, an argument derived from a considerations of a strategic imperative and strategic incentives presented by the 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.

war was cited as a defining characteristic of a crisis. The term *probability* suggests the element of unpredictability and uncertainty. As Thomas Schelling noted "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."[32] At a minimum, there is uncertainty regarding the opponents' intentions. If each opponent knew what the other intended to do and also knew its own intentions in the light of that knowledge, there would be no crisis.[33] Actions, of course, follow from intentions, so uncertainty and unpredictability regarding actions make an equally troublesome contribution to crises.[34] "Getting out of hand" is a synonym for unintended escalation, a concept that has been delineated into two types: inadvertent and accidental escalation.[35] The current state of mutual understandings of responsible state behaviors in and through cyberspace and characteristics of cyber operations (actions) themselves increase, respectively, the probability of inadvertent or accidental escalation in a militarized crisis.

Inadvertent escalation occurs when a party deliberately takes an action it does not believe is escalatory but is interpreted as escalatory by another party to the crisis.[36] Such misinterpretation may be born of uncertainties, including, for example, the other's intentions, lack of shared reference frames, or one party's thresholds. Inadvertent escalation in a crisis could result from the application of any instrument of national power or, within the military instrument itself, from any capability. The current immaturity of mutual understandings of acceptable and unacceptable cyber behaviors, however, suggests that a lack of shared reference frames and misunderstandings regarding thresholds are more salient when considering cyber vice other options during a crises.[37] Despite extensive formal, international efforts to establish a set of principles of "responsible behavior" in the context of cyberspace, no comprehensive set of principles addressing coercive (or exploitative) uses of cyber capabilities exists today that could serve to reduce uncertainties regarding the use of coercive cyber operations/options in a militarized crisis.[38] Although this has not yet resulted in inadvertent escalation out of a condition of day-to-day

---

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 and 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: Naval War College Press, 2020), 31–46, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers.

[32] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 97.

[33] Snyder and Diesing, *Conflict Among Nations*, 8.

[34] Along this line, it is instructive to consider "McNamara's Law," formulated by Robert McNamara, the U.S. 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." See 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.

[35] George, *Avoiding War*, 7–9.

[36] Forrest E. Morgan, Karl P. Mueller, Evan S. Madeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008), 23.

[37] 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.

[38] The United Nations (U.N.) 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 U.N. 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-

competition and into militarized crisis, this observation should not be extrapolated as a finding applicable to a condition of militarized crisis, a condition in which there are heightened tensions and increased time pressure to act.

The character of cyber operations increases a second risk of accidental escalation, when the direct effects of an operational action are unintended by those who ordered the action.[39] Henry Farrell and Charles Glaser cite three factors of cyber operations that make their effects potentially unpredictable, despite cyber operational planners' best efforts.[40] First, the complexity of the target system could render an attack unpredictable by obscuring what might happen if it is disrupted. Second, because most computer systems are not "air gapped," a disruption could inadvertently spread across a network, or a network may serve both commercial and military purposes such that an operation intending only counterforce effects also causes countervalue effects. And third, disruptions that intentionally cause local physical destructive effects could unexpectedly cascade. For example, a cyberattack against computers controlling a micro-grid connected to a wide-area grid could lead to much more far-reaching damage.

In sum, the immaturity of mutual understandings in militarized crises of prudent cyber behavior and the potential unpredictability of cyber operations' effects suggests that cyber operations/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.

Reversibility—Virtue or Vice?

An additional, and perhaps more important, feature of cyber operations for consideration is their potential for offering reversible effects in crises.[41] I say "more important" because it seems that the notion of reversibility being a virtue has become casually accepted, conventional wisdom. DoD's joint publication on cyber doctrine implies a virtuous 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."[42] This is a dangerous presumption regarding risk because it is uninformed by a consideration of conditional context (i.e., strategic competition short of

---

advance-copy.pdf and United Nations General Assembly, "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," March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[39] Ibid, 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, no. 1 (March 2017): 59–68, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809463.

[40] Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (2017): 7–17, https://www.semanticscholar.org/paper/The-role-of-effects%2C-saliencies-and-norms-in-US-Farrell-Glaser/59a81219fccac95bc954086df795919b341c1f95.

[41] 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.

[42] U.S. Department of Defense, *Joint Publication 3-12, Cyberspace Operations* (Washington, DC: Department of Defense, June 8, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, 3-IV.

militarized crises, militarized crises, or war). This essay discusses the distinct condition of crisis, so reversibility will be scrutinized in that context.

Most of the deductive scholarship on reversibility does not specify a 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."[43] Lin and Max Smeets also implied that reversibility is virtuous in their arguments regarding the impact that offensive cyber operations could have on the four strategic roles that force can serve: defense, deterrence, compellence, and "swaggering." They concluded 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]."[44] The [opponent] may know that, if it backs down, the "old" situation can be restored.[45] This reasoning describes reversible cyber operations as an offramp for an opponent but, again, not within any conditional context.

An exception to this context-free research is an argument offered by Richard Harknett and me.[46] In our 2019 article, we proposed that reversibility is a virtue in the 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. But our work does 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 informed by scholarship on crisis bargaining and escalation dominance. Schelling argued that advantage in a crisis goes often to the one who arranges the status quo in his favor and leaves to his opponent the "last clear chance" to stop or turn aside to avoid disaster.[47] Arranging the status quo in one's favor is a euphemism for achieving escalation dominance. Importantly, as Herman Kahn's 1965 work makes clear, 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 disaster.[48]

An action that undermines this strategic approach is a defender leaving loopholes in its escalation dominance strategy through which it can exit an implied or explicit commitment to escalate further.[49]

---

[43] Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70, https://www.jstor.org/stable/26267261.

[44] 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.

[45] Ibid.

[46] 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.

[47] Schelling, *Arms and Influence*, 44.

[48] 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.

[49] Schelling, *Arms and Influence*, 48.

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 (i.e., a weak commitment and thus an offramp for the defender). Successful crisis management offers an offramp to the opponent rather than introducing one for the defender. A defender employing a reversible cyber operation that 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, reversibility is a vice rather than a virtue as it undermines a core tenet of crisis management. Therefore, if the United States wants to offer an adversary 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."[50]

Strategy and Policy Implications

As policymakers debate how to maximize the effectiveness of U.S. 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 empirical or deductive evidence to support a prioritized investment in or the deployment of independent cyber 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] As policymakers weigh the utility of cyber means for various policy objectives, they should also heed the near-consensus view that independent cyber options are not directly useful for strategic deterrence (or restoring strategic deterrence).[52]

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 options for crisis management. When coupled with near-consensus views that independent cyber options lack

---

[50] Kahn, *On Escalation*, 231–232.

[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* (Santa Monica, CA: Rand Corporation, 2009); Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: Rand Corporation, 2012); Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 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, no. 2 (2015): 316–348, https://www.tandfonline.com/doi/full/10.1080/09636412.2015.1038188; Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (New York: Oxford University Press, forthcoming 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, no. 3 (2017): 452–481, https://doi.org/10.1080/09636412.2017.1306396; and 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.

direct utility for strategic deterrence, policymakers would be prudent to maximize the novel strategic contribution cyber capabilities can make to security: inhibiting adversaries' continuous efforts to cumulate gains in strategic competition short of militarized crisis and war.[53]

Much of the 2018 DoD cyber strategic approach of defend forward / persistent engagement should continue to anchor the next DoD cyber strategy.[54] 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, it helps set the conditions for success in and through cyberspace should either of those contingencies come to pass.[55] Stated differently, cyber capabilities can support crisis and contingency operations not primarily through episodic, independent operations during crises, but rather 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.[56] It is important for scholars and policymakers 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.[57] Indeed, American and Soviet scientists and scholars have 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."[58]

Policymakers should recognize that the tacitly bounded cyber strategic competitive space short of armed conflict in which day-to-day cyber competition plays out, like the United Nations, is 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 and into militarized crises. They would further serve to reduce the likelihood of unintended escalation from employing independent cyber operations/options of that same character in a militarized crisis. Whereas the United Nations supports an institutional approach,

---

[53] Fischerkeller, Goldman, and Harknett, *Cyber Persistence.*

[54] 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.

[55] Defend forward / persistent engagement can also serve as the foundation for cyber norms construction. See 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] Most state behaviors in day-to-day competition are best described as being exploitative rather than coercive, whereas a militarized crises 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: Special Issue – Cyber Competition (September 17, 2020)*, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

[57] 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.

[58] Graham T. Allison, "Primitive Rues of Prudence: Foundations of Peaceful Competition" 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): 9–37.

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 independently provides.

Finally, the next DoD cyber strategy should 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.

Conclusion

There is no evidence to-date—empirical or deductive—that cyber operations serve, or could serve, as de-escalatory "offramps" in crises. The empirical cyber escalation research cited in the 2019 Issue Brief was either not structured to investigate that question or, alternatively, suggests that cyber operations in the midst of a militarized crisis are, in fact, perceived as escalatory. Deductive research based on the characteristics of cyber operations and the logic of escalation dynamics cast further doubt on the Issue Brief's conclusions, as the uncertainties introduced by cyber operations into an escalation dynamic invariably increase the risk of inadvertent and accidental escalation. Additionally, the use of 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 leading to escalation by an opponent.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-12-21	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
What Do We Know about Cyber Operations During Crises?	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5224
	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-32909

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 focuses on how cyber operations employed in militarized crises are likely to impact escalation management. Policymakers may be attracted to the idea that cyber operations could serve as de-escalatory offramps to manage escalation in a crisis. Such expectations should be tempered for two reasons. First, we have no experience with cyber operations employed during a militarized crisis between two nuclear-armed peers. Absent direct experience, all we can rely on is academic research. Yet, secondly, existing empirical and deductive academic research provides no basis for confidence that cyber operations are either de-escalatory or non-escalatory in the context of crises. In fact, employing cyber operations intended as offramps in a crisis could have the opposite intended outcome—reversibility, for example, is a vice and not a virtue in crises. Given the absence of direct experience, policymakers must critically examine research claims that cyber operations can serve as crisis offramps. Prudent policy and resource allocation requires rigor in assessing the effectiveness of cyber capabilities in competition, crises, and war.

15. SUBJECT TERMS

Cyber strategy, crisis management, escalation

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	12	19b. TELEPHONE NUMBER (Include Area Code)