Cyber and Crisis Escalation: Insights from Wargaming

Jacquelyn Schneider

United States Naval War College

Views expressed are my own and do not represent those of the U.S. Navy or the U.S. Naval War College

Abstract: Does the advent of cyber operations make the international system more unstable? The overwhelming scholarly consensus is no, but practitioners paint a far more dangerous picture. Empirical analysis and hypothesis testing about cyber and stability have been difficult for a series of reasons. The interesting question, therefore, may not be whether scholars or practitioners are right about cyber and stability, but instead how states perceive the impact of cyber operations. In this article I examine data from a crisis wargame conducted at the U.S. Naval War College from 2011 to 2016. The data from the wargames reveals a strong tendency across scenarios, players, and cyber capabilities to choose risk adverse cyber strategies in order to decrease the risk of escalation. Despite this concern about escalation, however, in no game did the blue team choose to escalate or respond to adversary cyber operations. These games, therefore, reveal a potential cognitive dissonance within U.S. decision-makers in which they curtail their own use of cyber operations for fear of escalation, while not responding to similar adversary actions in cyberspace.

Does the advent of cyber operations make the international system more unstable? The overwhelming scholarly consensus is no,[1] but practitioners paint a far more dangerous picture. Time and time again, U.S. policy makers have testified about the de-stabilizing nature of cyber, warning of "a cyber Pearl Harbor,"[2] "the single biggest existential threat,"[3] and "the no.1 threat facing the nation."[4] Neither the scholars nor the practitioners have empirical precedent for their assumptions. Indeed, the body of work on cyber and stability has so far articulated a series of competing hypotheses about the impact of cyber on conflict initiation as well as a series of unsatisfying analogies with little ability to test any the validity of most of the assertions.[5]

Empirical analysis and hypothesis testing about cyber and stability are difficult for a series of reasons: the virtual nature of the domain, the technical difficulty to understand balance of capabilities, the covert nature of cyber, as well as the general infancy of its use. In some ways, these difficulties may be hurdles that are impossible to

---

[1] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal*, April 10, 2012: http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0; Stephen Walt, "Is the cyber threat overblown?" Foreignpolicy.com March 30, 2010, http://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/; Erik Gartzke, "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38, no. 2 (2013): 41-73; Jon R. Lindsay, "Stuxnet and the limits of cyber warfare." *Security Studies* 22.3 (2013): 365-404; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39, no. 3 (2015): 7-47; Thomas Rid, "Cyber war will not take place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

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

[3] Micah Zenko, "Admiral McMullen: Thank You and Farewell," *Council on Foreign Relations*, September 29, 2011: http://blogs.cfr.org/zenko/2011/09/29/admiral-michael-mullen-farewell-and-thank-you//

[4] Aaron Boyd, "DNI Clapper: Cyber bigger threat than terrorism," *Federaltimes*, February 4, 2016: http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-biggerthreat-terrorism/79816482/.

[5] Emily Goldman and John Arquilla, *Cyber Analogies*. No. NPS-DA-14-001. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2014; Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: Rand Corporation, 2012); Herbert Lin. "Escalation Dynamics and Conflict Termination in Cyberspace." *Air University* (2012).

overcome, not only for researchers but also for foreign-policy decision makers faced with extreme uncertainty when making decisions about how to respond and use cyber operations in a crisis. The interesting question, therefore, may not be whether scholars or practitioners are right about cyber and stability, but instead how states perceive the impact of cyber operations. We can, therefore, make significant strides toward our understanding of the impact of cyber on crisis stability by shifting from an analysis of capabilities to an exploration of states' perceptions about the impact of cyber on escalation. By bypassing technical questions of capabilities, we can focus instead on how decision-makers process the uncertainties of cyber, with implications not only for potential behaviors during crisis situations but also for understanding the variables that shape foreign policy decision-makers' understandings of the cyber domain.

The focus on perceptions vice capabilities is not entirely novel; the study of nuclear escalation was also plagued by a lack of empirical precedent. Similarly, research conducted during the Cold War focused not only on the pure capability balance between the major powers, but also on how those states perceived their capabilities and how institutional, cognitive, and strategic variables influenced nuclear decision-making.[6] It was during this time that wargaming emerged as a prominent mechanism to understand nuclear dynamics. From Schelling to Robert Mandel and games played not only at the

[6] Robert Jervis, "Deterrence and perception." *International security* 7, no. 3 (1982): 3-30; Robert Jervis, *Perception and misperception in international politics* (Princeton: Princeton University Press, 1979); Robert Jervis, Robert, Richard Ned Lebow, and Janice Gross Stein. *Psychology and deterrence* (Baltimore: Johns Hopkins University Press, 1989); Graham Allison and Phillip Zeilkow. *Essence of Decision* (New York: Longman, 1999).

Pentagon but also at Yale and MIT, wargaming provided much-needed insights into the motivations and perceptions of nuclear decision-making.[7]

Following the precedent set by those who explored wargaming to explain nuclear decision-making, in this article I examine data from a crisis wargame conducted at the U.S. Naval War College from 2011 to 2016. By conducting the analysis over six years, I am able to explore the evolution of the use of cyber and perceptions about the escalatory nature of cyber's use while examining how changes in context, capabilities, and sample influence those perceptions. My research shows that these decision-makers view cyber operations as highly escalatory and are therefore cautious about using offensive cyber operations and cyber network exploitation, even after conventional conflict has begun. Additionally, I find that these decision-makers—despite their concern about escalation—chose not to respond to cyber attacks by the adversary in any of the wargames. These findings suggest that U.S. policymakers may believe cyber is escalatory, but that perception may induce risk-adverse cyber policies that keep at least U.S. cyber operations from negatively influencing escalation dynamics.

The analysis proceeds as follows—in the first section I explore existing cyber and conflict escalation literature. Next I introduce the method and explain the benefits and limitations of the wargaming data to explore cyber and crisis escalation. I then generate a series of hypotheses about cyber and escalation and introduce the data and discuss findings. Finally, I provide conclusions and implications for our understandings of escalation and state policies on the use of cyber operations.

---

[7] Robert Mandel, "Political gaming and foreign policy making during crises." *World Politics* 29.04 (1977): 610-625; Robert Mandel, Garry D. Brewer, Martin Shubik, Alfred H. Hausrath, and Stuart A. Bremer. "Policy-making perspectives on war simulations." (1980): 359-375; Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword*. (New Haven: Yale University Press, 2008).

Cyber and Crisis Escalation

From rifles to tanks, to aircraft and nuclear weapons, there is an expansive set of empirical and theoretical analyses that explore the impact of technologies on crisis escalation.[8] These examinations of conflict and technological development present a knot of conflicting explanations for when and why crises escalate to conventional or nuclear war. From the structural and material,[9] norms of behavior,[10] behavioral perceptions,[11] and organizational dynamics[12]—the diverse variables impacting crisis escalation are often so intertwined that it is difficult to generalize the effects revolutionary technologies have (if any) on the potential for conflict erupting from crises.

Perhaps because of the extraordinary complexity and breadth of literature on crisis stability, cyber creates a particularly puzzling case in which conflicting

[8] Richard Smoke. *War: Controlling Escalation* (Cambridge: Harvard University Press, 1977); Barry Posen, "Crisis Stability and Conventional Arms Control," *Daedalus* 120, no.1 (1991): 217-232; Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca: Cornell University Press, 1991); Robert Powell, "Crisis Stability in the Nuclear Age." *American Political Science Review* 83, no.1 (1989): 61-76; Herman Kahn, *On Escalation: Metaphors and Scenarios* (New Brunswick: Transaction Publishers, 2012); Caitlin Talmadge, "Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security*, Forthcoming; Barry Nalebluff, *Brinkmanship and nuclear deterrence: the neutrality of escalation* (Princeton: Princeton University Press, 1987).

[9] J.D. Fearon, "Domestic political audiences and the escalation of international disputes." *American Political Science Review* (1994): 577-592; J.D. Fearon, "Rationalist explanations for war." *International Organization*, 49 (1995): 379-399; John Mearsheimer, *The tragedy of great power politics*. (New York: WW Norton & Company, 2001); Stephen Van Evera, *Causes of war: Power and the roots of conflict* (Ithaca: Cornell University Press, 1999); Robert Jervis, "Cooperation under the security dilemma," *World Politics* Vol 30, no.2 (1978): 167-214.

[10] Martha Finnemore, *The purpose of intervention: changing beliefs about the use of force* (Ithaca: Cornell University Press, 2004); C.Gelpi, *The power of legitimacy: Assessing the role of norms in crisis bargaining* (Princeton: Princeton University Press, 2003); I. Hurd, "Breaking and making norms: American revisionism and crises of legitimacy," *International Politics*, vol. 44, no.2 (2007): 194-213.

[11] Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976); Richard Lebow, *Between Peace and War* (Baltimore: Johns Hopkins University Press, 1984).

[12] Jeffrey Legro, "Military culture and inadvertent escalation in World War II," *International Security* (1994): 108-142; Barry Posen, *The sources of military doctrine: France, Britain, and Germany between the world wars* (Ithaca: Cornell University Press, 1986); Jack Snyder, "Civil-Military Relations and the Cult of the Offensive, 1914 and 1984," *International Security* (1984): 108-146; Graham Allison and P. Zelikow, *Essence of decision: Explaining the Cuban missile crisis* (Vol. 2) (New York: Longman, 1999).

explanations predict starkly different effects of cyber on crises.[13] For some, the complexity and interdependence of cyber operations and technology decreases the probability for conflict eruption.[14] For these scholars, the technical difficulty of creating physical effects through cyberspace operations make the impact of cyber on crisis stability negligible if not inclined towards peace. In addition, the civilian nature of digital capabilities and the ways in which these capabilities undergird national economies make significant cyber attacks in crises unlikely to occur. These scholars argue that states will restrain their use of significant cyber attacks and therefore mitigate the potential for inadvertent escalation through the use of cyber operations.

However, for others the extreme uncertainty, speed of evolving capabilities, and perception of offense dominance increases the potential that cyber will induce conflict.[15] For these scholars, the ubiquitous nature of the digital economy and digitized nature of conventional warfare create de-stabilizing incentives for cyber first strikes that could escalate to armed conflict.[16] Fundamentally, these arguments posit that the extreme uncertainty of cyber effects and dependencies increases the risk for inadvertent escalation due to cyber operations.

---

[13] Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: Rand Corporation, 2012); Lin, "Escalation Dynamics and Conflict Termination in Cyberspace"; John Stone, "Cyber War Will Take Place!." *Journal of Strategic Studies* 36, no. 1 (2013): 101-108; Gartzke, "The myth of cyberwar: bringing war in cyberspace back down to Earth"; Rid, "Cyber war will not take place."

[14] Lindsay, "Stuxnet and the limits of cyber warfare." Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction."

[15] David Gompert and Martin Libicki, "Cyber Warfare and Sino-American Instability," Survival 56, no.4 (2014): 7-22; Adam Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no.3 (2012).

[16] Jacquelyn Schneider, "Digitally Enabled Warfare: the Capability-Vulnerability Paradox," *Center for a New American Security*, August 29, 2016: https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox.

Methodology

In order to examine these conflicting hypotheses about cyber and crisis stability, I use data from a U.S. Department of Defense wargame. The game, called the Deterrence and Escalation Game in Review (DEGRE), is conducted annually with a sample of U.S. foreign policy decision-makers at the United States Naval War College. It is sponsored by U.S. Strategic Command and takes place over four days. For this research, I have drawn data from wargames conducted from 2011 to 2016. The use of wargaming in social science is experiencing a period of relative resurgence (this was a somewhat common practice in the early part of the twentieth century) and so a discussion about the merits and limitations of wargaming for international relations research is timely and important.

What is a wargame? Peter Perla, a lifetime wargamer at the Center for Naval Analysis and a trained social scientist presents the most accepted definition which is that, "a wargame is a warfare model or simulation whose operation does not involve the activities of actual military forces, and whose sequence of events affects and is, in turn, affected by the decisions made by players representing the opposing sides. In the end, a wargame is an exercise in human interaction . . . its forte is the exploration of the role and the potential effects of human decisions."[17] Wargames, as opposed to simulations or probabilistic models of operational research, examine the processes of warfare and do not present quantitative analyses of military effectiveness. As Perla explains, "wargames are tools for gaining insights into the dynamics of warfare. They can help players come to a

[17] Peter Perla, *The Art of Wargaming* (Annapolis: Naval Institute Press, 1990, pg. 164).

more complete understanding of the sources and motivations underlying the decisions made . . . wargames are best used to investigate processes."[18]

Wargames are explorations of human behavior when placed in a notional crisis or war scenario. The focus on human behavior makes the analogy of wargames and experimental research intuitive. Wargaming, however, is not an experiment, though it does have some experimental qualities. Like an experiment, wargames are tools to examine behaviors. They are also designed to test behavior when placed in certain constraints. However, experiments are designed specifically to deduce a causal effect. As such, special emphasis is placed in experimental design on controlling for confounding variables. Subjects of experiments are carefully randomized and alternatively provided with either control or treatment scenarios. Unlike experiments, wargames are usually one-off iterations (the wargame in this research is an exception to this rule). Because wargames are generally designed to exercise decision-making in complexity, they are rarely built to control for a specific variable. Finally, samples are generally not randomized and also are not divided into both a control and treatment group. These differences between wargaming and experiments have important implications for social science.

Most importantly, the non-experimental design of most wargames creates significant limitations both for determining causal effects and generalizing inferences beyond the single wargame iteration. This is for a number reasons. First, wargames are generally conducted with a small sample of individuals and are not usually repeatable or reproducible. For instance, they are usually played with specific countries in mind and

[18] Ibid, pg. 9.

therefore are also highly contingent on contextual biases. Secondly, wargames tradeoff between simplicity and accuracy. Simplicity helps wargame designers better understand the variables that influence players' decisions and wargame outcomes. However, with simplicity comes a loss of accuracy, particularly when playing the very complex game of war. Not only are players less invested in the outcomes of the games when there is less accuracy, but also the outcomes and behaviors are less indicative of a true decision in war.

Despite these limitations, wargaming provides a host of benefits to security researchers. And, in fact, many of both the limitations and the benefits of wargaming are similar to field experimentation in which scientists trade control and randomization for realism in both the environment and the participants.[19] Perhaps the most obvious benefit of wargaming is the sample that is generally used to play the games. One of the fundamental problems with using experiments in international relations is the difficulty in generating an appropriate sample that may replicate the kind of decision-making that occurs between nation states.[20] Critics have rightly pointed at the inability for undergraduates, the primary sample of experiments in international relations, to simulate an experienced foreign policy decision-maker. Additionally, experiments conducted in a lab have difficulty reproducing the stress and high stakes of foreign policy decisions. Wargames provide at least a partial solution for both those problems. Frances McHugh, former Department Chair of the U.S. Naval War College gaming department notes, "by explicitly allowing human decisions that are made under the press of time and on the

[19] Alex Mintz, Yi Yang, and Rose McDermott. "Experimental approaches to international relations." *International Studies Quarterly* 55, no. 2 (2011): 493-501.
[20] Alex Mintz, Steven B. Redd, and Arnold Vedlitz. "Can we generalize from student experiments to the real world in political science, military affairs, and international relations?." *Journal of Conflict Resolution* 50, no. 5 (2006): 757-776.

basis of imperfect or incomplete information to influence the course of events, and by incorporating the capricious effects of randomness and 'luck,' wargaming comes closer than any other form of intellectual exercise to illuminating the dynamics of warfare . . . the 'unquantifiable' factors."[21]

By using the same decision-makers that are vested with decisions in actual crises and conflicts, the behaviors of wargame participants are inherently more valid than student-generated experiments. Also, unlike undergraduates who are asked to play games for monetary compensation, wargame participants are generally significantly invested in the outcomes of the games (whether for institutional, personal, or professional reasons) and are placed under similar decision-making constraints as actual foreign policy decision-makers. As Perla and McGrady argue, "games give players active responsibility for their decisions, similar to what they would experience in the real world, and force them to bear many of the same consequences of those decisions, both positive and negative."[22]

For this research, I use the Naval War College's Deterrence and Escalation Game and Review (DEGRE) to examine cyber and crisis stability. DEGRE is conducted once a year and is designed to examine the "strategic impact of nuclear weapons proliferation, deterrence, employment, and escalation and its implications on U.S. plans, policy, and force structure." Its players come from U.S. think tanks, government departments, and academia and include both current and former high-level policy makers. The vast majority of players (approximately 25-30) are placed on a "blue" team in which they play

[21] Francis McHugh. *Fundamentals of Wargaming* (Newport: United States Naval War College, 1966, pg. 9).
[22] Peter P. Perla and E. D. McGrady. "Why wargaming works." *Naval War College Review* 64, no. 3 (2011): 113.

the role of U.S. government positions from Commander in Chief to Department of Treasury, Secretary of State, Secretary of Defense, and subordinate combatant commands. A secondary set of players (approximately 15-20) with subject matter expertise is placed on the "red" team to simulate a notional adversary. The game takes place over a week, starting the players in a crisis scenario and then letting the play evolve with decisions made by each team in six rounds of play. The wargame is considered a free-form game in which umpires serve only to arbitrate the net effects of decisions made between red and blue teams and not to induce an effect.

DEGRE is a particularly useful wargame for studying cyber and crisis stability because of some unique qualities of the game. First, DEGRE is a crisis game in which cyber may be played as a tool but is not the subject of the game. Therefore, the wargame shows behaviors towards cyber embedded within larger conventional military operations and other whole of government tools (diplomacy, sanctions, trade, etc.). The integration of cyber within this larger scenario is a more accurate gauge of decision-makers' perceptions of cyber than a cyber-only game because it introduces trade-offs between the usage of cyber and other conventional operations. This enables the analysis of the interaction between the use of cyber and subsequent or preceding uses of conventional or non-military options. Secondly, DEGRE does not dictate the play of the game. Instead, arbitration (i.e. the umpires of the game) serves only to adjudicate the result of the interaction of each side's move and not to decide outcomes. Therefore, the outcomes of the game are tied more closely to the behaviors of the players than the design of the game, which makes DEGRE less likely to introduce systematic bias through game design. Additionally, DEGRE uses an elite sample for its game from top current and

former government officials. And finally, DEGRE has been played for six years using the same play format. Even though the notional crisis scenarios as well as the players vary in many of the years, the iterative play of the game allows for longitudinal analysis, increases the sample size, and can help control for scenario-based intervening variables. Further, in all six years of analysis the same individual played the cyber subject matter expert; this individual's play was remarkably consistent throughout the games and therefore provides a useful control throughout the wargames.

There are two large limitations to using DEGRE for this analysis. First, with the exception of two years that ran the same scenarios, the scenarios change each year. Therefore, significant effort must be devoted in the analysis of the data to determine what role scenario variables play in any changes over the years. Perhaps a larger limitation is that the game is played at a Top Secret classification level. Many of the details about the scenarios and the players are masked, which impact the transparency of the research method. I have tried to work around this by providing generalizable characteristics, vice specific scenarios or capabilities.

In the data section below, I detail when contextual variables were similar and when they varied as well as significant changes in play structure, sample, and blue team lead. The variance of these variables, while affecting the ability to generalize patterns over time, also provides a mechanism to better understand motivating factors that determine cyber behavior. If cyber play vis-à-vis escalation changes with the context, the sample or the blue team lead, then that provides insight into how balance of power, personality traits, and organizational biases may impact U.S. use of cyber in a crisis situation. However, if we see consistencies in play despite changes in context, sample,

etc., then that provides evidence for enduring behaviors that may transcend changes in administration, etc. It is important to note that I will not be analyzing red play for insights on cyber and crisis stability. While red team members are generally subject matter experts in an adversary, they are at best a representation of U.S. perception of the adversary and so cannot provide insights into true "red" perceptions about cyber and crisis stability.

Data from DEGRE is generated in a variety of ways. First, an end of game report is created that details major moves of the game, lessons learned, and outcomes. Secondly, transcripts of player conversations are taken in both the red and blue cells during move discussions. These transcripts detail the decision-making process and capture conversations between players about the adversary, their potential courses of action, and their decision-making about future actions.[23] In addition, in two of the games, post-move surveys ask players specifically about perceptions of escalation. This survey data was analyzed in concert with the transcripts of conversations. Finally, a move summary provides the list of actions taken by both blue and red, at what point in the game the actions were taken, and to what effect.

Hypotheses

For the U.S. foreign-policy decision-makers that participate in DEGRE, the wargaming data allows me to examine a series of questions: do perceptions about the

[23] These transcripts are generated by two to three "ethnographers" (military officers provided with some training on data acquisition methods) positioned on opposite sides of the room. Because these are not trained social scientists and because there are physical limitations towards what conversations these individuals are able to hear, there is some variance in the reporting. I have compiled the cyber-relevant data from the transcripts and cross-referenced between the ethnographer reports. Any potential inconsistencies were discarded.

effects of cyber operations on crisis escalation impact decisions to utilize cyber operations at different phases of crises? At what point in crises do decision-makers choose to use cyber operations? What are their perceptions of the escalatory effects of cyber operations (especially vis-à-vis other potential actions)? Conversely, how does blue respond to red cyber operations? Does red cyber play lead to escalation on the part of blue? These questions lead to two categories of hypotheses: 1) "blue" hypotheses about how blue perceives itself and the actions it takes against red and 2) "red" hypotheses about how blue perceives red cyber actions against blue. Evidence for these hypotheses is derived both from the sequence of moves as well as transcripts and surveys about the decisions in the wargame.

"Blue" Hypotheses: Perceptions of the Effect of Blue's Actions

The first set of hypotheses explores how blue believes its own use of cyber operations will impact the adversary's escalation calculus. Evidence for these hypotheses are derived from discussions about action, and not necessarily from the move itself. For instance, if blue decided to conduct a cyber attack did they think it would lead to escalation? Were there conversations about not using particular cyber operations because of fears of escalation?

Hypothesis 1: Blue perceives blue cyber operations will lead to crisis escalation.

Hypothesis 2: Blue perceives blue cyber operations lead to crisis de-escalation.

Hypothesis 3: Blue perceives cyber operations have no effect on crisis escalation.

"Red" Hypotheses: Effect of Red's Actions on Blue

The second set of hypotheses explores action—how did blue respond to the adversary's cyber operations? Did the blue players take any actions specifically to respond to red cyber activity? What kind of actions and were there any conversations about the bleu team's perceptions of escalation in these retaliatory strategies?

Hypothesis 4: Blue takes cyber action in response to red cyber operation.

Hypothesis 5: Blue takes conventional kinetic action in response to red cyber operation.

Hypothesis 6: Blue takes nuclear action in response to red cyber operation.

Hypothesis 7: Blue takes diplomatic or economic action in response to red cyber operation.

Hypothesis 8: Blue takes no action in response to red cyber operation.

These hypotheses examine how cyber is utilized in the game, but the games also provide insight into the motivation behind these cyber behaviors. In other words, cyber play within the first set of hypotheses act as a dependent variable on escalation and crisis stability. However, the variance of games over time provides insight into cyber operations as a dependent variable—what drives the cyber play of U.S. decision-makers in the DEGRE wargame?

This leads to a second set of hypotheses which test five "schools" of explanations for cyber behavior in crises: organizational, capability, situational context, individual personality, and cognitive. If cyber play varies according to the departmental distribution within the gaming sample (i.e. department of defense or geographic command players vs.

department of state), then there may be evidence that organizational identities will be important drivers of U.S. cyber operations in crises. If, on the other hand, cyber operations within the game vary based on the evolution of capabilities over time, then the increased institutional capacity of U.S. cyber tools within its military would impact the future use of cyber operations. Alternatively, if cyber play varies based on the wargame's context than that would provide evidence that cyber's role in crisis stability will be based primarily on situational variables such as balance of power or geography. Additionally, play that is dominated by the personality of the blue team lead would provide evidence of the importance of Presidential personalities in determining cyber operations in crises. And, finally, analysis of the text and patterns of behavior that occur across all these scenarios might suggest that there are patterns of cognitive or cultural biases that impact the use of cyber operations in crises.

Motivation Hypotheses:

Hypothesis 9: Organizational variables explain blue cyber operations.

Hypothesis 10: Capability variables explain blue cyber operations.

Hypothesis 11: Situational context variables explain blue cyber operations.

Hypothesis 12: Individual personality variables explain blue cyber operations.

Hypothesis 13: Cognitive variables explain blue cyber operations

Data

Summary of Wargames and Cyber Activity

	Context	Blue Lead	Blue Highest Level Cyber	Blue Actions Before Cyber Attack	Red Highest Level Cyber	Actions in Response to Red Cyber
2011	Land war, Near-peer Adversary	Female, State Dept	Cyber attack against conventional military operations	Conventional military force and nuclear alert	Cyber attacks on conventional military targets	None
2012	Naval war, Near-peer Adversary	Male, Former Military	Cyber attacks against strategic command and control	None	No red cyber attacks	NA
2013	Naval war, Near-peer Adversary	Male, State Dept	Reversible virtual cyber attack on military capability	Conventional military force	Cyber attacks on military C2 nodes and critical infrastructure	None
2014	Land war, Asymmetric Adversary	Male, Policy	Cyber attack against offensive cyber capabilities	Conventional military force and nuclear alert	Cyber attacks on allied nuclear facilities	None
2015	Land war, Near-peer Adversary	Female, Policy	Information Operations	Conventional military force and nuclear alert	Cyber attacks on allied economic system, conventional military targets	None
2016	Land war, Near-peer Adversary	Male, Policy	Cyber attack on dual-use target that is reversible and covert	Conventional military force and economic sanctions	Cyber attacks on mainland blue power	Economic sanctions

Table 3. Summary of Wargames and Cyber Activity

Below I summarize the cyber play from the DEGRE wargames conducted from 2011 to 2016. A few notes about the terminology are required. First, I will use cyber attack, cyber network attack, and offensive cyber operations interchangeably. Over the course of these wargames, the official Department of Defense terminology on cyber attack vs. offensive cyber operations changed. In this analysis, I understand them to be the same and will be specific about the type of cyber operations conducted if there could

be a confusion between cyber network attack and offensive cyber operations. For instance, I use the term cyber-led information operations as separate from "cyber attack." Additionally, in order to protect sensitive information, I have generalized all armed conflict with weapons in the air, space, naval, and land domains as conventional conflict and further lump all potential nuclear activity into nuclear conflict. Finally, I will generally refer to players and the teams as "blue" (sample of U.S. decision-makers), "red" (adversaries), and "green" (allies). In these wargames, U.S. experts play the role of red and green. As such, I will not focus on their actions and instead on the reaction of blue to red and green activities.

Wargame 2011:

Wargame 2011 involved a land war scenario with a near-peer adversary. A female Department of State representative led the blue team. This was one of the first times that cyber was integrated in DEGRE and was the most rudimentary cyber play of the six wargames that I examined. Cyber was modeled very similarly to conventional capabilities. Unlike later games where there was extensive discussion about accesses, authorities, and current capabilities, wargames in 2011 and 2012 did not replicate institutional and capacity variables. One cyber token was generally equal to one conventional token. Without questions about capacity and institutional authorities, one would expect that cyber play would be very similar to conventional capabilities.

However, that was not how the blue team played cyber in the wargame. Instead, cyber capabilities were viewed as special and qualitatively different than their conventional counterparts. Throughout the game, players discussed the escalatory nature

of cyber and these perceptions of escalation caused them to curtail almost all cyber operations—to include network defense and network exploitation—until after conventional conflict had broken out and nuclear forces were placed on alert. At this point, once they no longer viewed cyber as more escalatory than other conventional or nuclear actions, the players became frustrated that the remaining cyber options could not substitute effectively for what was now deemed more escalatory and damaging physical attacks.

In post-move surveys, the players were explicit about how this fear of escalation from operations in cyberspace led to decisions to curtail cyber operations. In numerous survey responses and in discussions during the wargame, blue players repeatedly questioned whether the use of cyber—to include both cyber network exploitation and cyber attacks—would lead to a nuclear response by the adversary. This concern went beyond escalation from cyber attacks and included the use of cyber network exploitation to obtain accesses into adversary networks. As the blue team ethnographer noted, "Blue Lead argued that the adversary would know about this [network exploitation] . . . many questions grew including deep discussions into exploitation. Rail lines could be affected and viewed as hostile vice de-escalating." Debates about escalation continued after conventional conflict begun as the team discussed targeting strategic command and control with cyber attacks. Once again, concerns about escalation curtailed the use of cyber operations and all on the team decided that attacks against strategic command and control would necessitate full-scale nuclear war.

This discussion displays a few assumptions about cyber and escalation. First, despite the difficulty of attribution, players assumed that adversaries would have

knowledge not only of blue's cyber attacks, but also of the team's cyber network exploitation. Secondly, the players created an equivalency between cyber and nuclear attack—any cyber attack would necessarily lead to a nuclear response. The solution to these assumptions was not to use cyber operations until much later in the conflict—at which point, the capabilities were not able to create the same sort of kinetic effect that the players were able to produce with much more certainty from conventional capabilities. In addition, only after conventional conflict was underway were cyber information operations authorized, but even then the concern for escalation limited the scope and tactics of these information operations. Cyber players had to demonstrate to the blue team lead that any information operations taken via cyber means would be reversible so that there would be no potential permanent damage against civilian networks and capabilities.

This concern about escalation appears to have played some part in the blue players' response to red cyber attacks on conventional military capabilities. While the red team took offensive cyber operations prior to the blue team and before they launched conventional military strikes, the blue team did not view believe these red cyber attacks warranted a response—in the cyber of physical domains. This was partly because the blue team viewed a cyber tit for tat as potentially dangerous. As the defense lead player explained, "I did not feel any of the cyber attacks raised to the level where retaliation was needed and/or warranted! It was not risking nuclear war!" Note the cognitive dissonance in this explanation. The cyber attacks were not worrisome enough to warrant response. This was an observation that was held throughout the game by most of the players. As one argued in discussion, "cyber-attacks although annoying do not appear crippling."

Despite the fact that these attacks were considered annoying and below the level of retaliation, the players were concerned that any response would necessarily go nuclear. Therefore, the players were both deterred from responding because of a belief that any cyber act would go nuclear, but also didn't need to be deterred because they didn't feel cyber warranted any response.

Wargame 2012:

Wargame 2012 involved a naval war scenario with a near-peer adversary. A male former military official led the blue team. The design of cyber play within the game was more robust than in 2011 in that the type of targets and effects were more explicit. However, as in 2011, cyber was generally not played with significant institutional or capacity limitations.

Wargame 2012 saw the largest cyber play than in any other DEGRE game before or since. It was also the most escalatory game that has been played in DEGRE in the recent history of the wargame. Cyber operations were a primary line of effort from move one and cyber attacks on missile command and control were authorized prior to conventional force employment. In fact, the use of conventional power was placed in reserve to be contingent on the success of cyber attacks to degrade the enemy's ability to conventionally respond to U.S. operations. As the blue team lead directed, "don't get the air expeditionary and tanking assets in place too early—until cyber effort has been effective." Those initial cyber moves were not just designed as a combined arms operation to maximize military effectiveness. Instead, cyber attacks were envisioned as a

signal to the adversary of U.S. will and capability, that "you don't want to go to war with us." The blue team lead believed that by demonstrating cyber capability, the blue team would be able to convince the red team to de-escalate the crisis. The perception by the blue team was that blue was just as vulnerable (if not more) as the red team to early cyber attacks on command and control. Therefore, the blue team needed to take the initiative and conduct the first strike in order to ensure that blue was able to maintain its advantage in cyberspace while also cutting off the opponent's ability to later mass and control conventional forces.

After pursuing these cyber attacks on the adversary's military command and control, the blue leader then pursued horizontal cyber escalation and attacked red's primary-civilian use cyber infrastructure in order to decrease the opponent's economic ability to support war. Finally, as the crisis escalated to a naval blockade, the blue team lead advocated the use of cyber attacks against opponent nuclear weapons as well as concentrated cyber-led information operation campaigns. The greatest debate—in terms of escalation—about the use of cyber was actually in reference to the information operation campaign and the use of cyber to impact domestic populations.

In wargame 2012, red was unable to conduct any cyber attacks and so there was no response by blue to red operations. However, discussion by the blue team indicated that they would be willing to escalate cyber attacks and conventional attacks to red cyber attacks on blue command and control. In fact, blue considered their cyber vulnerabilities as so existential that they could not wait to respond to the cyber attack and therefore had to pre-emptively strike red's ability to conduct both cyber and kinetic attacks against blue command and control.

Wargame 2013:

Wargame 2013 involved a naval war scenario with a near-peer adversary. A male former Department of State Representative led the blue team. The design of cyber play within the game included greater flexibility in target choice as well as greater fidelity of the cyber planning/targeting process than in the 2011 and 2012 games.

The 2013 wargame saw a large emphasis on deterring adversary cyber operations as well as the use of cyber operations as a signaling tool. Combined, these concerns about deterring adversaries while also signaling from cyberspace led to cautious use of offensive cyber operations and computer network exploitation. The focus on deterrence seemed to stem from the perception that the blue team was uniquely vulnerable both to attacks and to effects on its national economy based on these attacks. As the blue team lead commented at the onset of the game, "consider the economic impact of cyber ops to blue and global economy. Deterrence is key . . . be noisy in defense of homeland and computer network defense/computer network exploitation." As with 2011, the players were more comfortable committing conventional forces and physical effects than they were with conducting cyber attacks and consequently offensive cyber was not played in the game until after sizeable conventional escalation, to include deployment of large forces to the area, air to air engagement, and a naval blockade. These cyber attacks that blue played were against military targets and were limited (by direction of the blue team lead) to reversible and virtual attacks.

The players started the game with an initial objective of deterring adversary cyber attacks through the use of declaratory deterrence policies. This focus on deterrence also led the players to question whether or not blue cyber network exploitation would create incentives for the adversary to conduct a preemptive cyber strike. Consequently, strict rules of engagement—to include no network exploitation of strategic command and control and limited military command and control—were placed on computer network exploitation with the assumption that these activities would be detected and would be interpreted as signals of the United States' desire to escalate the crisis. At one point in the game, in the midst of a naval blockade, the blue team's cyber operations were detected as it conducted exploitation of networks related to the adversary's conventional maritime operations. Despite the fact that shots had already been fired between vessels, the gameplayers were very concerned that the detection of their cyber exploit (not attack) would inadvertently escalate the conflict. In that same move, 20 adversary aircraft were shot down. However, exit surveys suggested that the majority of the blue players believed that the discovery of the cyber exploit was potentially the most escalatory action that occurred in the move (the red team did not make any statement or conduct any operation in response to this cyber action).

This concern with escalation even after the exchange of conventional fire was especially prevalent in discussions about cyber attacks that might impact civilians. At one point after the exchange of fire and loss of life, a conversation occurred between the blue team lead and the cyber lead. The cyber lead was trying to advocate for the use of cyber attacks against targets that affected both military and civilian logistics. The blue lead was emphatic that cyber options, especially those against trains and power grids,

were off the table. In frustration, the blue lead told cyber to look into a lower range of options and voiced a concern that cyber was "outpacing the kinetic efforts."

In general, the blue team was more comfortable conducting cyber deception that affected the adversary's ability to control and influence its population, than strictly offensive cyber operations. They saw the deception operations as comfortably deniable and reversible, and therefore a less escalatory use of cyber operations than cyber attacks. However, to complicate decision making about these deception operations, the blue team thought of these deception operations more as an effort to signal than as an asymmetric influence operation. Therefore, the cyber operations were designed to signal potential capability and will while not at the same time signaling aggression or the willingness to escalate. As can be expected, the red team failed to understand this elegant distinction.

In terms of the blue team's response to red cyber actions, there was limited if any response. In the 2013 wargame, red undertook significant cyber play including attacks on blue command and control nodes as well as attacks on allied economic markets. Both of these actions were taken before conventional fire in the initial moves of the game. In both of these cases, as well as the case of cyber attacks on conventional blue forces after the naval blockade, the blue team viewed the cyber attacks as less escalatory than other kinetic options and therefore believed it was not worth response. The ethnographer captured some of this dynamics on day one in a conversation between the cyber lead and the blue team lead "cyber briefs that the adversary has conducted 'very escalatory' destruction of blue homeland nodes. Blue lead says, 'we need to have a discussion about how we treat cyber attacks vice kinetic attacks.' Cyber feels this is nearly kinetic, like bombing a command and control tower. Blue lead says it is different psychologically."

Blue lead's distinction about the psychological difference between cyber and kinetic was evident later in the game as well when blue vessels came under attack. As the message came in, the navy lead reported that "blue combined surface groups are under attack." The room appeared ready to escalate and then the navy lead corrected, "according to the commander in the region, it was only a cyber attack." The team chose not to respond.

Wargame 2014

Wargame 2014 involved a land war scenario with an asymmetric adversary. A male policy leader led the blue team. The design of cyber play was consistent with the game played in 2013. Like the wargames in 2011 and 2013, the 2014 iteration showed cautious use of offensive cyber operations. There was a focus on deterring cyber operations consistent with behavior in 2013 and a concern about escalation to the nuclear realm by offensive cyber operations taken both by blue and by allies. Similarly, the blue team was concerned about the signaling effects of computer network exploitation. This concern was so strong that it affected not only the use of cyber exploitation to achieve access but also the use of cyber exploitation for traditional intelligence operations. At one point in the beginning of the game, a blue player cautioned the team, "they're ready to shoot. Without provoking them we need to use cyber ability to locate them." The concern was that even being in the adversary's networks would be enough to start a conflict. A comment later by the defense lead in blue showed this assumption that cyber attacks could lead to nuclear escalation when he noted, "not a lot of strategic force mobilization [by red]. That will depend on whether red sees cyber and bomber

movement by blue." The blue defense lead was—probably subconsciously—creating an equivalency between cyber operations and the use of airborne nuclear assets. He believed that either could instigate the movement of the adversary's nuclear forces. Note also that he didn't define what kind of cyber operations would be equivalent with nuclear bombers, but that broadly "cyber operations" of all flavors could have the same tailored effect as the movement of a nuclear bomber.

Due to these concerns, the blue team focused on cyber defense until after conventional military operations had commenced and blue nuclear forces had been put on alert. Cyber attacks taken by blue at that time were limited in scope to tit for tat attacks against the adversary's cyber offensive capabilities. These were taken with great reticence. As one team member cajoled, "maybe we can take away some of their capabilities by taking out some of their cyber in a defensive way." Even the perception of being offensive in cyber—even within a conventional conflict—was very concerning for the blue team.

The wargame in 2014 also demonstrated responses to red cyber activity that were consistent with play from all previous wargames. Despite significant attacks—to include a cyber attack that created physical effects on an allied nuclear facility—the blue team did not believe that the red cyber attacks warranted escalation. Even after significant allied pressure in response to a red cyber attack on the allied nuclear facility, the blue team warned of caution and the potential for escalation. As the blue team lead concluded, "we have to strike something soon. But . . . tell country Y we are preparing option to respond to country X's provocation but we are also delaying these responses in order to allow ceasefire discussions to continue. We have continued to show caution,

doing forensic on cyber attack." Interestingly, during this same period in the game conventional forces remained in place and continued low scale violence. In addition, this commentary reveals a dissonance in which the blue team was concerned that their exploitation activities would be caught and attributed and escalates to nuclear war, but when nuclear plants were attacked, the difficulty in attribution caused blue to take no response.

Wargame 2015

Wargame 2015 involved a land war scenario with a near-peer adversary. A female policy leader led the blue team. The design of cyber play was consistent with the game played in 2013 and 2014. The cyber play in the 2015 wargame was once again characterized by escalation concerns about cyberspace activity. Not only was there significant discussion about the use of cyber network exploitation, cyber-led information operations, and cyber attacks before conventional conflict, but even the deployment of a defensive cyber protection team to a foreign ally was questioned. Additionally, as the conflict escalated and shots were fired, significant debate still occurred about the escalatory nature of cyber operations taken in conjunction with other military operations. And while the ability to conduct offensive operations against military targets became less likely to succeed (due to the loss of access during the wargame), the blue team was still concerned with the signaling created by the use of the cyber than the ability to create military effects. They were willing to sacrifice military effectiveness in cyberspace for the perception of greater stability. Consequently, throughout the wargame the blue team

placed significant restrictions on cyber operations and required that any attacks or information operations conducted through cyberspace would be non-attributable and reversible. This was consistent both pre and post conflict initiation.

The wargame in 2015 continued many of the nuclear equivalencies of earlier wargames, but the discussion about escalation to nuclear use was rich and articulated some of the logics of how cyber might lead to inadvertent escalation. In particular, there was a discussion that occurred early in the wargame about conducting a variety of cyber network exploitations. At one point, cyber asked the blue team lead if they would be authorized to conduct cyber network exploitation of the adversary's strategic command and control. She responded, "prep for the environment is fine," but iterated the concern that any move to action on these accesses would be centrally controlled at the presidential level. The defense lead echoed concerns about the authorization to achieve accesses, warning: "there are certain things there we will have to watch very carefully. We will have to be very careful about their nuclear redlines . . . wouldn't want to worry them too much. Can we limit it to accesses and not worry Country x that their nuclear deterrent is held at risk?" The blue team lead affirmed these concerns and ended the conversation with, "I think it would hit our redlines. We would have to talk through these logics."

The debate in the 2015 wargame also highlighted the players' perception that cyber attacks that affected domestic populations would lead to nuclear war. This concern was not just about cyber attacks that created virtual or physical effects, but also cyber-driven information operations. In fact, the concern that social influence operations conducted via cyber would go nuclear led information operations to be conducted after kinetic action (air strikes and special operations forces). In a conversation about whether

or not to use cyber operations in conjunction with conventional operations, concerns about effects on American citizens curtailed the use of cyber attacks to aid the operation:

> *Cyber: We should look at cyber attacks on conventional military targets . . .*
>
> *Blue lead: What are the pros and cons of doing an operationally significant cyber cut? And doing a demonstration of that capability?*
>
> *Cyber: We could do a demonstration of that capability for instance on a dual-use system in the adversary's homeland.*
>
> *Intel lead: Those are good ideas but you need to communicate to American that there could be dead Americans*
>
> *Cyber: If we demonstrate, they could demonstrate on American targets.*

Curtailing cyber operations due to civilian impact seems to be a product of two competing concerns. One is the belief that the American homeland is more vulnerable to cyber attacks than other nations. The other concern is that the high premium placed on not affecting civilians biases decision-makers towards operations with known effects. Decision-makers are more confident that they can limit war with a 500 lb. bomb than a cyber-led information operation. Taken together, these concern create a strong perception that cyber operations that affect domestic populations are both dangerous for Americans and dangerous for nuclear war. A revealing conversation at the end of the wargame in 2015 sheds light on these perceptions:

> *Defense lead: I'm looking for categories of cyber and when in the timeline you would implement them. Social networks would be very early in the conflict.*
>
> *Cyber: We wouldn't do that in phase 0; very loathsome to do that in peacetime.*
>
> *Defense lead: Social early but not before phase 1. At the other end is the power, financial, and transport.*
>
> *Cyber: We need to do that early in phase 2. We are loathe to do that in cyberspace because it affects civilians . . .*

Defense lead: I liken this to the use of WMD. Is there another category between social and these large political targets?[24]

Finally, as in all the previous wargames, the blue team in 2015 did not view red cyber attacks as grounds for escalation. In fact, after a successful red attack against an allied economic system, allies specifically requested a tit for tat cyber operation. The blue team demurred and instead supported continued sanctions against red.

Wargame 2016

Wargame 2016 played the same land war scenario with a near-peer adversary as in 2015. As such, changes in cyber play between the two are of particular interest. A male policy leader led the blue team. The design of cyber play was consistent with the game played in 2013, 2014, and 2015.

The 2016 wargame saw increased focus on proactive defensive measures, hardening, resiliency, and the use of cyber protection teams pre-emptively to mitigate vulnerabilities. Additionally, leaders were more comfortable with computer network exploitation for access than in previous years; however, reluctance to use cyber attacks remained with extreme emphasis placed on reversibility and "scoping" cyber attacks

[2424] The phases of conflict that the players refer to in this discussion is a planning framework used by the U.S. Department of Defense. The phase construct separates warfare into six phases. Phase 0- shaping, Phase 1: deterring, Phase 2- seizing the initiative, Phase 3-dominating, Phase 4- stabilizing, and Phase V- enabling civil authority. Though not explicitly tied to the law of armed conflict, the general assumption is that war begins in phase 2 and therefore the authority to conduct most armed operations is delegated to the geographic combatant command at that point. Prior to that time, hostilities will be highly controlled by peacetime or crisis rules of engagement. For a brief overview of the phasing construct, see Lauren Fish, "Painting by Numbers: A history of the U.S. Military's Phasing Construct," *War on the Rocks*, November 1, 2016: http://warontherocks.com/2016/11/painting-by-numbers-a-history-of-the-u-s-militarys-phasing-construct/.

away from civilians and adversary leadership (this was despite the use of economic sanctions that directly targeted adversary leadership and had implications for civilians). Once conventional operations were under way, there was a general support for cyber attacks that affected military capabilities, though there were still concerns that some cyber operations even after conventional force would lead to escalation. Therefore, rules of engagement about non-attribution curtailed many cyber operations. For instance, at one point cyber lead suggested an operation that would gain access to the supply chain and distribution of materials for nuclear and conventional war fighting. The blue lead, who was otherwise risk acceptant with his use of conventional force, declined to use the cyber operation arguing that "the risk of attribution is too high to move forward with this option." Finally, the wargame in 2016 saw a continued adherence to an unofficial norm of non-attack against strategic command and control, to include exploits that could be misinterpreted at as an imminent attack.

Like the previous years' wargames, blue did not escalate after any red cyber activity to include attacks on the blue homeland. On day three, after the employment of conventional forces and loss of life on both sides, a cyber attack was conducted on mainland blue that led to the loss of power that affected large blue civilian populations. A conversation about the response led to the decision not to escalate, including not using cyber operations in response.

Discussion

Cyber Escalation ladders

2011	2012	2013	2014	2015	2016
Computer network defense	Computer network attacks against military C2	Computer network defense	Computer network defense	Computer network defense	Computer network defense
Conventional conflict	Conventional conflict and nuclear alert	Conventional conflict and nuclear alert	Conventional Conflict	Conventional Conflict	Cyber network exploitation for future attack
Cyber attacks against military + dual-use targets	Computer network attacks against economic targets	Cyber-led information operations	Nuclear alert	Cyber-led information operations	Conventional conflict and nuclear alert
Cyber-led information operations	Nuclear and cyber attacks against strategic command and control	Cyber attack, reversible on military target	Cyber attack against adversary cyber offensive capabilities		Cyber attack on military target, reversible and covert
Nuclear conflict	Cyber-led information operations				Cyber attack on dual-use target and Cyber-led information operations

Table 4. Cyber Escalation Ladders

Patterns of Play

With the exception of 2012 (which I will discuss further in the motivations section below), all the other wargames showed a strong belief that cyber operations would escalate crises, potentially even to nuclear war. These perceptions of escalation were so strong that they significantly curtailed the blue use of cyber attacks, cyber network exploitation, and often cyber-led information operations. Additionally, fears about escalation led to tight rules of engagement for the cyber attacks that were utilized, including requirements for non-attribution and reversibility. These beliefs about

escalation were unique from their conventional counterparts and across all the wargames players commented about the special nature of cyber. While cyber operations were often conflated with nuclear or space, they were never conflated with tanks, aircraft, or ships.

There are concrete policy implications for these escalation fears, all of which manifested during the five wargames in a surprisingly consistent way. First, intelligence in cyberspace is viewed qualitatively different than other more traditional means of military intelligence collection. Because obtaining access to a network can provide both situational awareness of the enemy's activity and act as a launching point for an attack, blue players were wary about the effects of extensive cyber network exploitation. This fear was present in discussions about network exploitation of civilian or dual-use infrastructure, such as railroads or energy. However, the fear of escalation was especially pronounced when debating whether or not to seek accesses within adversary strategic command and control. Further, because many of these networks serve dual purpose with conventional military command and control, fears of escalation due to nuclear pressures also curtailed significant network exploitation into military command and control.

Interestingly, despite the murky nature of cyber espionage, discussions about the escalatory nature of these activities assumed that the U.S. activities would be attributed. Therefore, any spying the U.S. was doing within cyberspace would necessarily become a signal of intentions to adversaries. This belief that cyber network exploitation would be a credible signal to adversaries created an interesting phenomenon in which the blue teams were both deterred from conducting exploitation because it would signal aggressive intent and also considered cyber espionage a credible and discernible signal of U.S. capabilities that could be used to de-escalate in other domains. Though red team actions

in wargames are generally not useful predictors of actual adversary behaviors, it may be worth noting that the red team never understood these activities as signals and were neither deterred nor driven to escalation based on cyber network exploitation.

Concerns about escalation had significant effects not only on whether to conduct cyber attacks, but also on the character of these attacks: what kinds of targets were most escalatory? What kind of effects? When in the crisis were they considered appropriate? And what impact did these beliefs have on the decisions to utilize cyber-led information operations?

There are four overarching categories of cyber targets that were debated in these wargames: military targets, dual-use targets, civilian targets, and nuclear targets. Based on the fear of escalation, the first target of choice in the wargames was military capabilities—even better if those military capabilities were the adversaries' offensive cyber operations. When the debate came to dual-use targets (i.e. energy, transportation, or communication), there was extreme reticence to conduct cyber attacks and pure civilian as well as nuclear targets were completely off the table. These decisions were driven by escalation and not by capability because the commentary suggests that military targets were not necessarily the easiest to attack or the ones that would make the greatest effect. Dual-use and civilian targets that use SCADA systems and are not controlled by the government are generally the easiest kind of cyber targets; reticence to target these reflects concerns not about capability but about escalation.

Additionally, there was significant discussion about the types of effects that cyber could create that would lead to escalation. With the exception of 2012, every single blue

lead asked cyber to create effects that were virtual and reversible—all while retaining non-attribution. In fact, these leads were quite often willing to trade off the ability to achieve effect in order to create the perception of escalation control. This could be because cyber provides a flexibility in effects that you don't get with a lot of physical weapons. You can't choose whether a bomb physically or virtually destroys its target; even the anti-radiation missiles that are considered non-kill weapons physically destroy a radar. Cyber allows some potentially flexibility that might be appealing for decision makers. Unfortunately, these choices for virtuality and reversibility were often made after conventional force had already been committed so in some ways, while it provided the decision makers more flexibility, they were already committed to more escalatory actions in other domains.

This brings me to the third consideration for cyber attacks: the point in the crisis in which cyber attacks were considered to be least escalatory. Barring 2012, all cyber attacks were conducted after conventional force on force conflict had occurred. In U.S. Department of Defense parlance, the crisis was firmly in Phase 2 (the phase generally associated with armed conflict) before cyber operations were considered non-escalatory. Even virtual attacks were not condoned prior to those conventional actions. This has significant implications for U.S. responses to increasingly persistent use of cyber operations before armed conflict.

Finally, the wargames demonstrated perhaps a uniquely American concern about cyber-led information operations and escalation control. For many of the wargames, these information operations were not used until after cyber attacks on military targets and were used in conjunction with nuclear alert and even nuclear demonstration.

Conversation debating the use of the information operations often equated their effect with nuclear capabilities and implied an existential threat to adversaries. Because of this existential threat, not only were these not used quite often until the end of the crises, but they were not targeted at regime overhaul but instead at decreasing public support for the use of force. These wargames were all conducted prior to the U.S. election in 2016; perceptions about escalation may have changed after the increased focus on Russian led information operations in peacetime.

In general, the fear of escalation due to cyber operations seems to be based on three factors: 1) a perception that the U.S. is more vulnerable to cyber attacks than its adversaries, 2) concerns about the relationship between cyber and nuclear capabilities, and 3) concerns about the domestic implications of cyber attacks. All of these concerns are magnified by the uncertainty ubiquitous in cyber operations. That uncertainty caused individuals to look for analogies in the nuclear realm and exacerbated concerns about collateral damage and escalation. The bounds of possibility with cyber effects are so expansive that it may become easier cognitively for decision-makers to drop a 1000lb bomb than a virtual cyber attack on the same target. Though the chance of a catastrophic effect in cyber is incredibly low, the high uncertainty of the attack means that it can't be ruled out. In many ways, physics and standard intelligence can bound the uncertainty of the 1000lb bomb so that while the net effects are potentially greater than cyber, there is no potential effect at the extremes.

These factors contribute to the lack of response by blue to red cyber actions. Once in 2016 blue responded to a cyber attack with a slight increase in economic sanctions, but otherwise red cyber attacks either didn't reach the threshold of concern or blue couldn't

find a response that they thought was proportional. Additionally, while the blue teams assumed that their cyber operations would be attributed, confusion about attribution seemed to decrease the chance that blue would escalate to red cyber attacks.

Motivations behind cyber play

Minus 2012, the cyber play in all of the wargames was remarkably consistent. Blue was concerned about the escalatory effects of cyber operations so they were generally cautious in their use of cyber network exploitation, cyber attack, and cyber-led information operations. Also consistent was their lack of response to red cyber activity. In no wargame did blue choose to escalate because of a red cyber attack. This is an interesting divergence in behavior. What can explain the motivations behind this seemingly contradictory logic?

Previously, I identified five potential hypotheses to explain the motivations for perceptions of escalation due to cyber operations. The consistency of play for five of the six scenarios presents problems for two of the hypotheses. Both capability variables and the situational context varied over the six years the game was played. From 2011 to 2016, the United States stood up Cyber Command and built 120+ cyber mission teams with skills in defense and offensive operations. The design of the game closely followed this evolution of these capabilities and the cyber defensive play became much more robust; cyber protection teams were used as a capability and were forward deployed in 2016 as a part of an overall deterrence package. That represents a pretty substantial change for how computer network defense was conceptualized in both real life and the game. However, we didn't see a difference in offensive play over those six years as capabilities changed. This would suggest that cyber capabilities are not the primary

motivator for decisions to utilize cyber operations. In contrast, what has been consistent over time is U.S. conventional dominance. Therefore, the non-use of cyber operations may not be tied to U.S. cyber capabilities, but it may instead be tied to the fact that the U.S. has so many conventional options in crises. For states that are much more capable than their peers in other domains, the decision to not respond to cyber attacks while at the same time not utilizing cyber attacks may be a gift of power. You can be concerned about the escalatory effects of cyber when you have conventional dominance to fall back on.

Second, over the six years the wargame was played, there were five different scenarios with multiple adversaries in multiple contexts. And yet there was consistent use of cyber operations. The consistency suggests that the situational context was not a driving factor in these cyber decisions. The one year that we did see cyber played differently, 2012, was run the next year with a similar scenario and returned to the play that we had seen previously and that we saw in 2014, 2015, 2016.

That aberration year does, however, lend some credence to the power individual personalities play in the use of cyber operations. Especially because there are few existing or solidified norms of behavior in cyberspace, limited U.S. policies, and almost no empirical precedent, cyber operations are particularly malleable and prone to leadership motivations. This is exacerbated by the fact that authority to conduct cyber operations in the United States is centrally controlled and quite often at the highest levels. That means that whoever is the President will have a large role in how cyber is utilized in crises. Previous research suggests that individual personality of Presidents matter for the

way states fight wars and that this especially important in emerging technologies.[25] Therefore, while 2012 was an "aberration" in cyber play, it does point to the extreme importance of the U.S. President in the role that cyber plays in crises.

The remaining two variables—organizations and cognition can help explain some of the dissonance in the cyber behaviors of the blue teams in five of the six years of wargaming play. First, in terms of organizational influences, the United States' delegation of cyber responsibilities within the Department of Defense has created some institutional legacies for cyber operations. Cyber Command falls under Strategic Command as a sub-unified command. Strategic Command is traditionally the organization that deals with nuclear capabilities and space. They focus on strategic effects and worry about deterrence and escalation control. Because of Cyber Command's position as a sub-unified command of Strategic Command, there may be a false equivalency between the strategic assets and effects of the predominantly nuclear Strategic Command and cyber operations.[26] Throughout the wargames the players associated cyber with nuclear and often claimed that the use of cyber operations would lead to nuclear war. Note that very few of the blue players were experts in the red doctrine and very few used evidence from red statements or behavior to support that assumption. If cyber is a strategic resource like nuclear weapons, then it logically should be used sparingly, late in conflict, and with clear rules of engagement that allow for escalation control.

---

[25] Julia Macdonald and Jacquelyn Schneider, "Presidential Risk Orientation and Force Employment Decisions The Case of Unmanned Weaponry." *Journal of Conflict Resolution* (2015): 0022002715590874.

[26] It is also significant to note that this is a Strategic Command exercise and is staffed with many (but not the majority) Strategic Command employees. This may decrease some of the generalizability of the findings. However, statements by the Obama administration as well as the scope of cyber operations under his administration indicate that these views are prevalent in many parts of the Washington decision-making apparatus.

But if cyber is an operational resource than these limitations to its use are no longer as applicable. The question is how much of the equivalency with nuclear weapons is false. Blue responses to red cyber attacks would suggest that cyber operations do not have the strategic effect that the blue players were concerned about in their debates about escalation. Part of this may be tied intimately with the way we as human beings process uncertainty and the high amount of uncertainty tied to cyber operations. While that uncertainty may create many potential deleterious outcomes from cyber operations (which limits our use), when they are actually conducted the virtual nature of those operations doesn't lend itself to the same fear-inducing crisis behaviors created when physical effects occur. And indeed even when physical effects occur from cyber operations, their second-order nature tempers the fear generated from a cyber attack.

In one of the wargames, the blue team lead commented that he didn't need to respond to a cyber attack because it was psychologically different. This could be a fundamental truth that goes beyond the wargaming players, beyond U.S. foreign-policy decision makers and explains how humans react to technological threats and particularly cyber. Research on fear suggests that human beings process fear in very similar ways across cultures because of hundreds of thousands of years of evolutionary conditioning. However, cyber is a new threat and is not conditioned for response. We are not primed by fear to respond to cyber operations. Therefore, cyber operations are more likely to create another emotional response: anxiety, which in turn tempers reactions to cyber operations and makes us choose risk-averse cyber strategies.[27] As Libicki aptly describes

[27] Jacquelyn Schneider, "Beyond Strictly Material Assessments of Weapons' Effectiveness: Examining the Effect of Fear in Threat Assessment," paper presented at International Studies Association Annual Meeting, February 2014, New Orleans, Louisiana.

it, "cyberwar engenders worry."[28] Worry is very different from fear and may explain the lack of reaction to red cyber attacks and the reluctance to use blue cyber attacks.

Conclusion

These wargames provide some potential insight into the future use of cyber operations in crises and their impact on escalation for the United States. For five of the six wargames, the players were reticent to use cyber operations due to their fears of escalation. At the same time, they chose not to respond to red cyber attacks. These five wargames suggest that cyber operations, if conducted similarly to these wargames, would not lead to escalation. The use of cyber operations by blue teams in five of the six wargames was highly bound—and bound primarily to control escalation. The one wargame where the blue team did utilize offensive cyber operations early and with great effect was also the most escalatory wargame.

Will cyber operations lead to escalation? This research can't answer that, but it can provide evidence that many people within the U.S. decision-maker community are worried that U.S. cyber operations will lead to escalation. Because of that concern, they build policies that centralize control and limit the use of cyber operations prior to armed conflict. But these policies have not matured and the centralized control of these operations mean that Presidential risk proclivities will have a significant impact on how these cyber operations are used in the future.

[28] Martin Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012, pg. 21).

What this research can say is that in none of the wargames did the gameplayers feel a need to respond to cyber attacks—even when these attacks affected civilians on the homeland and even when they caused nuclear fall out in an ally. Future research should be conducted to better understand what motivates the lack of response. How generalizable is it? Is it something that is unique to American decision-makers, or is it something more pervasive that can explain cyber behaviors of adversary states? And if it is more pervasive, then should American decision-makers be more open to using cyber operations earlier in crises?