Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation

Jacquelyn Schneider,[a]* Benjamin Schechter,[b] and Rachael Shaffer[b]

[a]Hoover Institution, Stanford University, Stanford, CA, USA
[b]Naval War College, Newport, RI, USA
*Corresponding author. Email: jacquelyn.schneider@stanford.edu

Abstract How do emerging technologies affect nuclear stability? In this paper, we use a quasi-experimental cyber-nuclear wargame with 580 players to explore three hypotheses about emerging technologies and nuclear stability: (1) technological uncertainty leads to preemption and escalation; (2) technological uncertainty leads to restraint; and (3) technological certainty leads to escalation through aggressive counterforce campaigns. The wargames suggest that uncertainty and fear about cyber vulnerabilities create no immediate incentives for preemptive nuclear use. The greater danger to strategic stability lies in how overconfidence in cyber exploits incentivizes more aggressive counterforce campaigns and, secondarily, how vulnerabilities encourage predelegation or automation. Both of these effects suggest worrisome relationships between cyber exploits and inadvertent nuclear use on one hand and cyber vulnerabilities and accidental nuclear use on the other hand. Together, these findings reveal the complicated relationship between pathways to escalation and strategic stability, highlighting the role that confidence and perhaps-misplaced certainty—versus uncertainty and fear—play in strategic stability.

In the 1983 movie *WarGames,* a curious teenager with a penchant for computer games accidently hacks into a US nuclear weapons command and control system, bringing the United States and the Soviet Union to the brink of thermonuclear war. The movie inspired Ronald Reagan to conduct a major review of digital vulnerabilities in the United States' nuclear command, control, and communications (NC3) and ultimately led to the first major warning about cyber operations and nuclear stability.[1] The subsequent National Security Decision Directive, published in 1984, cautioned that "recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services … Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges … The technology

1. Kaplan 2016.

International Organization 77, Summer 2023, pp. 633–67

doi:10.1017/S0020818323000115

to exploit these electronic systems is widespread and is used extensively by foreign nations."[2]

Despite the early warning, almost thirty years later states have doubled down on digital technologies within their NC3. Most notably, the United States embarked on a major nuclear modernization effort in 2017, with over USD 77 billion devoted to replacing legacy analog systems with state-of-the-art digital computing and communications technologies.[3] This modernization is a top priority for US strategic decision makers, who testified that NC3 digitization is essential for the United States' nuclear deterrence.[4] The NC3 modernization was also a centerpiece of the 2018 National Defense Strategy and Nuclear Posture Review, which both heralded the modernization of the NC3 as key pillars of effective US nuclear deterrence.[5]

Implicit in this testimony and in the US defense strategies is an assumption about NC3 and stability: that the benefits of digital components will outweigh the risk of novel cyber vulnerabilities. This is a remarkable assumption because, in a field with little agreement, a majority of scholarship on cybersecurity and nuclear stability argues that cyber vulnerabilities in the NC3 are the most dangerous implications of the digital revolution.[6] Further, most of the strategic-stability literature about NC3 argues that vulnerabilities in command and control both increase incentives for first strike and decrease states' ability to control nuclear escalation once nuclear war begins.[7] Even the Nuclear Posture Review warns that "the NC3 system is now subject to challenges from both aging system components and new, growing twenty-first century threats. Of particular concern are expanding threats in space and cyberspace."[8]

So why pursue digital modernization of the nuclear arsenal if the cyber risks are so high? Here is where a scholarly puzzle converges with real-world application because underlying all of these decisions about digital modernization is a question about how emerging technologies impact strategic stability. Do these technologies increase uncertainty and the risk of escalation? Does their novelty lead to restraint and deterrence? Or might the introduction of new technologies create asymmetries of certainty that push an overconfident state to adopt dangerous nuclear force postures?

While the cyber-nuclear literature might largely agree that cyber creates dangerous incentives for nuclear use, it cannot yet answer these larger questions about pathways from technology to instability. Are some pathways more likely than others? How will decision makers frame the threat (and promise) of cyberspace during nuclear crises? Answering these questions is difficult. In a world of emerging and prolific cyber

2. National Security Decision Directive 145, National Policy on Telecommunications and Automated Information Systems Security,1984.
3. Government Accountability Office 2017; Hyten 2017.
4. Deptula, La Plante, and Haddick 2019; House Armed Services Committee 2017.
5. Department of Defense 2018a, 2018b.
6. Acton 2020; Bracken 2016; Futter 2016, 2018; Gartzke and Lindsay 2017; Lindsay 2020.
7. Blair 1984; Bracken 1983; Carter, Steinbruner, and Zraket 1987.
8. Department of Defense 2018b.

threats, there is still no large-*N* database of cases of cyber exploits or vulnerabilities of NC3 to analyze, nor do we necessarily have the technical data to assess the probability or scope of successful (likely highly classified) cyber attacks against the United States' or adversaries' NC3. What we can do, however, is try to understand how humans may react, given assumptions about cyber technology and NC3, to the threat of cyber attacks against NC3. Are there generalizable reactions that can help us understand the impact of this emerging technology on strategic stability?

Normally this would be an almost impossible question to answer. The data simply do not exist, and the dominant synthetic-data-generation methods can struggle with external validity, especially for high-stakes scenarios. However, recent innovations in experimental wargaming have introduced a novel opportunity to understand human reactions to rare and dangerous scenarios. We therefore turned to this methodology to explore the impact of cyber capabilities on nuclear decision making, placing players in two crises (one of low intensity and one of higher intensity) between comparable nuclear states and varying only their cyber vulnerabilities and exploits within NC3.[9]

After running the game with 115 teams and 580 players, we find it is not uncertainty and fear about cyber vulnerabilities that create the most dangerous incentives for nuclear use. Instead, it is overconfidence produced by the cyber exploit that incentivizes the riskiest behaviors, including aggressive counterforce campaigns and nuclear alerts. Counterintuitively, it is players' confidence in their ability to mitigate cyber vulnerabilities by predelegating nuclear use to a lower level of command or relying on automation to launch nuclear weapons that increases the danger of accidental or inadvertent nuclear use. Together, these findings reveal the complicated relationship between emerging technologies and nuclear use, highlighting the role of confidence and perhaps-misplaced certainty—versus uncertainty and fear—in strategic stability.

This exploration first introduces theories of strategic stability and emerging technology, outlining how foundational assumptions about uncertainty drive opposing hypotheses about how technologies like cyber impact strategic stability. We then describe the quasi-experimental method and wargame design before exploring the findings from the data for both cyber operations and nuclear use. Finally, we explore what the game reveals about strategic stability writ large and the impact of cyber operations on nuclear stability, and conclude with recommendations for further research on escalation, the use of wargames, and implications for current cyber and nuclear policy.

9. We define a cyber vulnerability as a flaw in software code, network configuration, or network access that allows an intruder to access networks, software, or hardware to manipulate, destroy, or deny access to information or system control. This could include vulnerabilities in software code, back doors in hardware, Wi-Fi access vulnerability, and so on. Conversely, we define a cyber exploit as a cyber capability that takes advantage of a cyber vulnerability to manipulate, destroy, or deny access to information or system control. More generally for our game design, one can think of a cyber vulnerability as a weakness in the ability to defend, and an exploit as a weapon to attack vulnerabilities.

Strategic Stability and Emerging Technology: Certainty versus Uncertainty

The impact on conflict of emerging technology, or systems that may have been invented and integrated into militaries but not yet used extensively in conflict, is a foundational puzzle of international relations. Do new technologies lead to escalation and nuclear use?[10] Do they create incentives for deterrence and restraint?[11] Or are they merely an intervening variable to larger issues of strategy or politics?[12] While the matter is still hotly contested, decades of debate reveal that one foundational assumption fissures the field: how uncertainty affects the likelihood of nuclear use or arms races. Some scholars have argued that technological uncertainty creates strategic instability, while others look at that same uncertainty and argue that emerging technologies can create restraint and deterrence. And for a third group of scholars, it is certainty (often misplaced) in emerging technologies that has the most dangerous implications for strategic stability.

For those who believe that uncertainty creates incentives for instability,[13] emerging technologies are more likely to lead to nuclear use when they create uncertainty about regime intentions,[14] capabilities,[15] or the overall balance of power.[16] This technological uncertainty leads to security dilemmas,[17] arms races,[18] cults of the offensive,[19] and asymmetries of information[20]—all of which increase the incentives for nuclear use.

This happens in a few ways. First, technological uncertainty increases the chance of preemptive nuclear use by creating the fear that first movers will win a conflict.[21] The best illustration of this for strategic stability is the survivability of a second-strike arsenal. If a state believes that a first mover would decimate its ability to launch a nuclear response, it may be incentivized to launch preemptively. Further, in the quest to maintain deterrence in the midst of a first mover advantage, states have incentives to adopt first strike policies and aggressive nuclear force postures.[22] Vulnerabilities in NC3 could be especially dangerous for a state worried about assured control to launch a second (or even first) strike. Practitioners at the dawn of the information age, faced with the uncertainty around emerging threats like

10. Gottemoeller 2021; Johnson 2020; Sherwood-Randall 2020.
11. Cox and Williams 2021.
12. Kroenig 2021; Lieber 2008; Talmadge 2019.
13. Blainey 1998; Booth and Wheeler 2008; Copeland 2000; Powell 2002; Schelling 1980; Waltz 1959.
14. Glaser 1997.
15. Glaser and Kaufmann 1998.
16. Mearsheimer 2001.
17. Jervis 1976; Quester 2002.
18. Glaser 2000; Richardson 1960.
19. Snyder 1989.
20. Debs and Monteiro 2014; Fearon 1995; Reiter 2003; .
21. Jervis 1976; Van Evera 1998.
22. Cunningham and Fravel 2015; Nitze 1976

electronic warfare, wrote pointedly about their concern that threats to NC3 from emerging technologies could create incentives for preemptive strike. As Ashton Carter warned, "faced with alarming analyses, the superpower command systems can come to fear their vulnerability so much that they take seriously the need to strike first."[23]

Technological uncertainty also increases the chance of inadvertent or accidental escalation by incentivizing states to build dangerous offense-dominant weapons, campaigns, and force postures.[24] Famously, Jervis argued that uncertainty about whether a weapon was designed for offensive or defensive campaigns could led to security dilemmas in which even status quo states could find themselves at war.[25] Here—as opposed to the logics of preemption—the danger of uncertainty is how states hedge their nuclear vulnerabilities, with nuclear alert, predelegation of launch authority, or automation, which then increases the chance of inadvertent or accidental escalation to nuclear use.[26] In this pathway from technological uncertainty to nuclear use, states' attempts to mitigate uncertainty about vulnerabilities may ease the pressure for preemptive use of nuclear weapons (warned of earlier), but at the expense of safety and control.

Not surprisingly, the application of these theories of technological uncertainty and escalation to the cyber domain predicts instability with greater incentives for nuclear use.[27] Scholars point to uncertainty about cyber attribution, effects, and offense–defense differentiation to paint a warning for future nuclear conflict.[28] A strong focus in this conversation is how cyber uncertainty creates incentives for preemption and early nuclear use,[29] largely building on assumptions from the larger literature about how uncertainty creates fear and an impetus for action. As a 2021 Carnegie Endowment paper concluded, "Cyber-attacks against a nuclear command and control system would expose the attacked state to significant pressure to escalate conflict and even use nuclear weapons before its nuclear capabilities are compromised."[30] Secondarily, the cyber-nuclear literature also warns of inadvertent and accidental nuclear use driven by the uncertainty that cyber operations may create about targeting, early warning, and control of nuclear forces.[31]

But while the cyber-nuclear literature may lean heavily on assumptions about uncertainty's central role in provoking nuclear war, uncertainty is often what states make of it. Indeed, scholars examining how states respond to uncertainty suggest

23. Carter, Steinbruner, and Zraket 1987, 556.
24. Herrmann and Fischerkeller 1995.
25. Jervis 1976.
26. Blair 2011; Johnson 2020; Posen 1982; Sagan 1985.
27. Futter 2018; Wan, Kastelic, and Krabill 2021.
28. Buchanan 2016; Buchanan and Cunningham 2020; Gompert and Libicki 2014, 2015, 2019; Healey and Jervis 2020; Schneider 2017.
29. Acton 2020; Lin 2021.
30. Levite et al. 2021.
31. Cimbala 1999, 2017; Gartzke and Lindsay 2017; Klare 2019; Lindsay 2019; Stoutland and Pitts-Kiefer 2018; Unal and Lewis 2018.

that some theories of conflict may be overly deterministic about the impact of uncertainty on war.[32] A rich literature explores how both context and individual-level variables interact with uncertainty to mediate its impact on war onset.[33] And other scholars question the assumption that uncertainty necessarily leads to war[34]—providing theoretical and empirical evidence for the role of certainty (as opposed to uncertainty) in strategic instability.

Mitzen and Schweller provide one of the most direct responses to theories that assume uncertainty drives conflict, presenting an alternative model of misplaced certainty and war in which overconfidence (often driven by a yearning for certainty in dangerous situations) creates pathways to both preemption and inadvertent escalation.[35] Altman applies a similar argument to military campaign assessments, arguing there are cognitive and organizational incentives for false optimism about the success of military campaigns.[36] Meanwhile, explorations of individual foreign policy decision making provide evidence that personality traits and risk proclivities shape how leaders deal with uncertainty in crisis decisions, with those more prone to cognitive closure and risk acceptance more likely to use military force earlier in a crisis.[37] Perhaps most compellingly, evidence from wargames suggests that war onset is determined more by individuals' overconfidence, willingness, and desire to create certainty through aggression than by any fear created by uncertainty.[38] Johnson explains that this trait, overconfidence, evolved as a means of survival, suggesting that the path from misplaced certainty to war has strong and powerful roots in humans.[39] He links this evolutionary trait to a Rubicon theory of war onset in which overconfidence can induce a state to move from status quo restrainers to attackers.[40] For these theories, emerging technology is not necessarily dangerous to nuclear stability when it makes states uncertain about victory, but when it imparts confidence or certainty for more aggressive campaigns, whether that be nuclear use or counterforce initiatives.

These alternative theories about uncertainty and conflict could explain a significant empirical puzzle about cyber and escalation that has divided the scholarly community. Despite the dominance of hypotheses linking cyber with escalation, a burgeoning literature suggests cyber operations are not only *not* destabilizing, but in some instances can create incentives for restraint. Across case studies, experiments, and wargames this work finds little or no evidence of cyber operations increasing

32. See also Rathbun 2007 for a useful explanation of how different approaches in international relations understand uncertainty.
33. Friedman 2019; Jervis 1976; Lebow, and Stein 1989; Mercer 2005; Rosati 2000.
34. Bas and Schub 2016; Mitzen and Schweller 2011.
35. Mitzen and Schweller 2011.
36. Altman 2015.
37. Lebow 2020; Macdonald and Schneider 2017.
38. Johnson et al. 2006; McDermott, Cowden, and Koopman 2002.
39. Johnson 2004.
40. Johnson and Tierney 2011.

violence within crises.[41] Meanwhile, more theoretical work in this vein questions previous hypotheses about uncertainty and the offensive nature of cyberspace. It argues that cyberspace is not as offensively dominated as previously believed and that the uncertainty that does exist might incentivize restraint instead of escalation.[42]

While this literature throws doubt on theories that link cyber uncertainty with escalation, it does find evidence of misplaced certainty and overconfidence. Experiments and content analysis find a tendency to overestimate cyber capabilities, even while underestimating cyber vulnerabilities.[43] This overconfidence in cyber capabilities, especially against nuclear networks, could (as Carter described in 1987) "encourage deliberate, direct attack intended to achieve purely military rather than politico-diplomatic objectives."[44] Gartzke and Lindsay explain this logic as a cyber commitment problem in which there is "a logical possibility for creating a window of opportunity for using particular cyber operations. . . . It would be important to exploit this fleeting advantage via other credible military threats (e.g., forces mobilized on visible alert or deployed into the crisis area) before the window closes."[45] The cyber commitment problem becomes most dangerous when incentives to use cyber exploits create the impetus for otherwise risky counterforce strategies paired with conventional capabilities like air, missile, or naval attacks on nuclear arsenals.[46]

Together, these theories of uncertainty (and certainty), technology, and war lead to three competing hypotheses about cyber operations and nuclear use. The first, drawing from assumptions that link uncertainty with war, predicts that cyber vulnerabilities create fear, which leads to preemptive nuclear use and tactics that minimize the vulnerability of first strike at the expense of safety and control. This includes nuclear alert, predelegation, and automation. The second hypothesis is that uncertainty creates incentives for deterrence and restraint, suggesting that uncertainty about cyber effects and vulnerabilities leads to cyber restraint against an enemy's NC3, decreases incentives for states to use their nuclear arsenal, and ultimately decreases the willingness of states to commit to risky campaigns against nuclear adversaries. The third hypothesis focuses on misplaced certainty, suggesting that misplaced certainty in cyber capabilities incentivizes cyber attacks against nuclear networks and engenders an overconfidence that could also lead to counterforce campaigns in other domains.

41. Gomez and Whyte 2021; Jensen and Valeriano 2019; Kostyuk and Wayne 2020; Kreps and Schneider 2019; Lindsay 2013; Schneider 2017; Valeriano, Jensen, and Maness 2018; Valeriano and Maness 2015.

42. Borghard and Lonergan 2017, Gartzke 2013; Kaminska 2021; 2019; Lindsay 2013; Nye 2017; Slayton 2017.

43. Gomez and White 2021; Kreps and Schneider 2019; Lawson 2019.

44. Carter, Steinbruner, and Zraket 1987, 7.

45. Gartzke and Lindsay 2017, 44–45.

46. Clary and Narang 2019; Lieber and Press 2017; Long and Green 2015; Talmadge 2017.

Wargame Design

To test these hypotheses about cyber and nuclear stability, we developed a quasi-experimental wargame. Wargames are useful mechanisms with which to study crisis decision making, and in particular to look at the impact of emerging technologies on nuclear use.[47] First, like survey experiments, games and the use of hypothetical scenarios let us collect data on incidents that are rare, have bad data, or look to the future. Similarly, games and experiments are particularly useful methodologies to look at decision making and human behaviors—both important variables in crisis stability. Games go beyond survey experiments, however, both in the use of groups in some games and in the ability to immerse players in the game environment for an extended period. Together, these characteristics make games an extraordinarily useful methodological alternative to historical case studies, big data, or even survey experiments because they may provide greater external validity and novel data for rare or future events.[48]

These advantages make wargaming ideal as a way to address our research question. First, decisions about cyber operations and nuclear events are both rare and highly classified. This means that case studies and large-*N* databases are both extremely limited and potentially biased toward public events. Further, because our hypotheses are about how humans react to certainty and uncertainty in high-stakes scenarios, other behavioral synthetic data generation methods (like surveys or lab experiments) may struggle with external (or ecological) validity.[49] While there is debate about how immersive and externally valid games can be, features of games like multi-hour durations, deliberative discussions, and rich scenarios create the conditions for a more immersive environment than surveys. Schelling, for example, recounts that games were so immersive that participants began to see the game as "either real or as one that could be real."[50] This immersion also helps build rich qualitative data through narratives written into response plans, facilitator notes, and transcripts—all of which help us understand the "why" behind game outcomes, which is especially useful for evaluating hypotheses about the motivations behind human behaviors. Finally, groups used as decision-making units in wargames can more accurately represent the important mediating role of advisors and group dynamics in complicated decisions like cyber or nuclear use.[51]

47. Lin-Greenberg, Pauly, and Schneider 2022; Pauly 2018; Reddie et al. 2018; Schechter, Schneider, and Shaffer 2021.

48. Lin-Greenberg, Pauly, and Schneider 2022.

49. Ibid.

50. Department of Defense 1966, D3. Indeed, comparing scenario comprehension questions between a virtual iteration of this wargame and an identical survey treatment, 97.5 percent of wargame participants answered correctly while only 73 percent of survey treatment respondents did.

51. Haney 2002; Redd 2002.

Game Design

The game is designed to look at how two independent variables, having a cyber exploit in an adversary's NC3 and having a cyber vulnerability in your own NC3, affect a dependent variable, strategic stability.[52] In this game we use a narrow scope for strategic stability (or crisis stability), which is defined by Acton as "the absence of incentives to use nuclear weapons first."[53] We operationalize it as not only binary use of nuclear weapons but also whether teams put forces on nuclear alert, predelegated authority, used automated systems, or launched counterforce campaigns. We hypothesize that uncertainty and overconfidence explain how our independent variables affect strategic stability, so we introduce uncertainty within our cyber exploit and vulnerability treatments and use group- and individual-level data to trace uncertainty and certainty to decisions about nuclear weapons, cyber use, and campaign strategies.

Given our research question, we sought to design a wargame that allowed us to control for our variables of interest while creating an immersive and engaging experience that would induce players to behave as closely as possible to how they might in a real crisis. The wargame, which includes two related but independent scenarios—one of low intensity and one of high intensity[54]—pits two strictly comparable states (Our State and Other State) against each other over a contested territory (Gray Region). Teams play a notional cabinet for Our State and are randomly assigned to one of four treatment groups, which vary as to whether teams have cyber exploits and/or cyber vulnerabilities.

Condition 1 is our full treatment. These players are given both an exploit into the adversary's NC3 and a vulnerability in their own NC3 (Table 1). Condition 2 is the first of our asymmetric treatments: the group is given an exploit into the adversary's NC3 and told they have no vulnerability in their own NC3. The third group and second asymmetric treatment gives the team a vulnerability in their own NC3 but no exploit into the adversary's NC3. The fourth group is a control group; they have neither an exploit nor a vulnerability. This allows us to control for differences in crisis outcomes based on the cyber treatment.

According to our first hypothesis, that uncertainty and fear about cyber vulnerabilities lead to nuclear preemption, we would expect that the asymmetric vulnerability group, followed by our full treatment group, would be the most likely to use nuclear weapons, go on nuclear alert, and predelegate launch authority. The logic here is that

52. For more in-depth exploration of game design choices, see Schechter, Schneider, and Shaffer 2021.
53. Acton 2013, 117.
54. We chose to play one-sided, one-move games to allow control and ease of iteration across time. While we were concerned initially that playing a one-move game would lead players to take one-off actions that would not be representative of a true emerging crisis, players' extensive use of "if-then" comments in their response plan (if Other State does this, then we would do that) mitigated some of that concern. Further, when asked in the first scenario why they had not used cyber exploits, many of the players responded that they were reserving them for later use, implying that they were internalizing a multi-move decision-making process instead of the single move we presented them in the game.

uncertainty about the vulnerability would create fear about second strike survival and therefore incentivize early use of nuclear weapons. In contrast, our second hypothesis, that uncertainty about cyber operations creates incentives for restraint and deterrence, suggests that the groups with the cyber vulnerability will be less likely to use nuclear weapons than our control group or exploit-only group. Finally, the hypothesis about misplaced certainty suggests that it is the exploit that drives differences in our groups—with exploit groups not only more likely to use the capabilities but also the most likely to use nuclear weapons and launch counterforce campaigns.

TABLE 1. *Treatment groups*

	NC3 vulnerability	No NC3 vulnerability
Adversary NC3 access/exploit	Full treatment group	Asymmetric group 1
No adversary NC3 access/exploit	Asymmetric group 2	Control group

Playing both scenarios in the game takes about three hours. All players are given an initial scenario brief and instructions about how to complete the response plan. Players are then divided into their separate teams to discuss the scenario and their response.[55] Teams are made up of four to six players who are randomly assigned to work together in a rough approximation of a national security cabinet. They are asked to choose roles among themselves, including head of state, minister of defense, minister of state, economic advisor, intelligence advisor, and national security advisor (if there are six). They are then given separate but identical pamphlets with the information from the initial brief as well as details about the economy, military, and cyber capabilities of both Our State and Other State. Teams fill out a response plan for each of the scenarios and take individual surveys after each of the scenario turns are completed. There is no adjudication or opponent for teams between or after the scenarios, which allowed us to directly compare game outcomes across iterations. Players are told that scenario 2, while being thematically an extension of scenario 1, is not contingent on the actions they took in scenario 1.

The Scenario

The scenario presented to players involves two neighboring peer adversaries, Our State and Other State, which contest territory in the Gray Region.[56] Both states

55. In some games, teams convened in separate rooms. In others, teams were in the same room but at separate tables. We noted no difference in the outcomes based on whether they were in separate rooms or in one room. We also didn't observe any collaboration or crosstalk between teams when they were in the same room.

56. In developing the scenarios, we opted for abstractions—from the country names to the simplified geography and order of battle—for two reasons. First, our sample included a significant number of current and former government practitioners, and we wanted them to be comfortable that they weren't

have nuclear capability (a triad of delivery platforms), a strong military, and an advanced economy. Allies are not overtly included in the scenario, though the scenario brief and background information mention the UN Security Council. The crisis begins when Other State foments an uprising in the Gray Region, a semi-autonomous region within the territorial boundaries of Our State that includes a large population of individuals ethnically Other State (Figure 1). Other State security forces are spotted in the Gray Region, while Other State mobilizes its land and naval assets and announces: "In defense of our brothers and sisters in Gray Region, we have acted decisively. … The Gray Region is now under Other State rule … We will use any means to protect our territory, including the nuclear option."

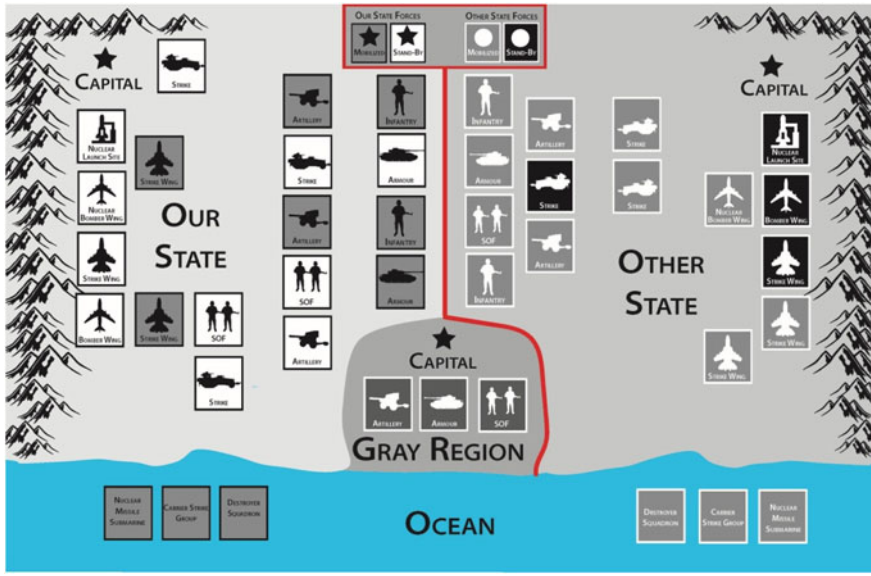

FIGURE 1. *Scenario 1 situation map (not to scale)*

Scenario 2 picks up at the end of scenario 1 with a significant escalation of violence and threat (Figure 2). Other State invades Our State and mobilizes nuclear forces. Players are told that Other State is considering the "preemptive use of nuclear

revealing classified or sensitive information about their country. Second, we are looking for generalizable behavior across a wide variety of potential scenarios, so we wanted to reduce the risk that players would be biased by a particular scenario. To confirm that they were not imputing one particular scenario, and therefore inserting systemic bias, the survey said, "Our game was based on a hypothetical scenario, but often players refer back to one country when playing. Did you think back to a particular country when playing your country?" To this, 59 percent said yes, but there was no pattern between game iterations and specific real-world scenarios, and players mentioned a wide array of places (among them India/Pakistan, Kuwait/Middle East, Crimea/Russia, North Korea, Germany, China, and Venezuela).

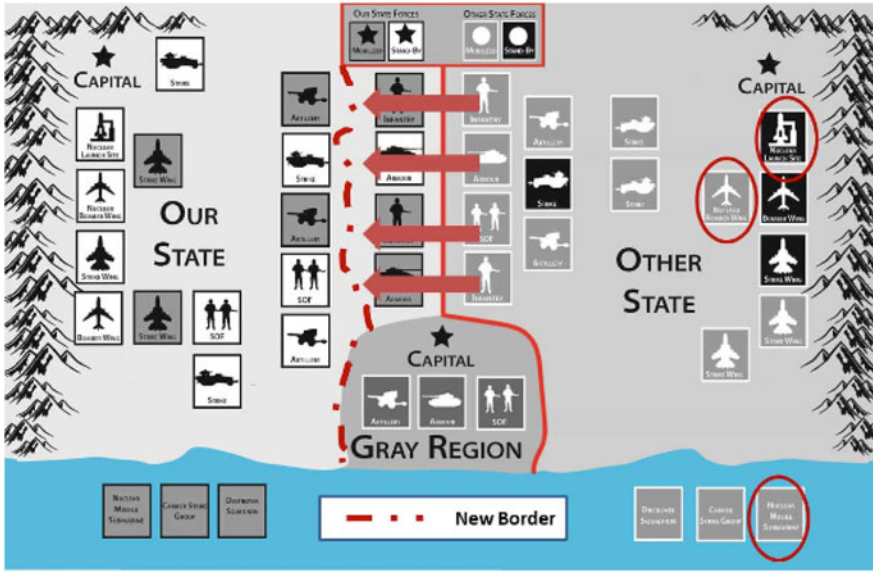

FIGURE 2. *Scenario 2 situation map (not to scale)*

weapons." By varying the intensity of these two scenarios, the game is able to explore how cyber vulnerabilities and exploits affect incentives for nuclear use in two distinct phases of crisis escalation.

The Treatment

Teams received two handouts representing their treatment after the collective scenario brief (see the online supplement for the facilitator guide and details about game facilitation). One slide detailed whether they had a cyber exploit, and the other detailed whether they had a vulnerability. Every team received both handouts, regardless of whether or not they had the exploit or the vulnerability.

Players with the exploit treatment were told that they had "a new cyber exploit/access to attack Other State's NC3" (Figure 3). The "exploit has a high probability of success," "cuts off Other State's ability to launch nuclear attacks; effective for an undetermined amount of time; relatively covert, but full attribution may be possible in the long run," and it is "unclear how long this exploit/access against NC3 will exist." To make the exploit and vulnerability treatments as symmetrical as possible, the vulnerability treatment uses nearly identical language: "intel reports Other State has a cyber exploit/access against Our State's NC3; Other State assesses the NC3 cyber attack would have a high probability of success; cuts off Our State's ability to launch nuclear attacks; effective for an undetermined amount of time; relatively covert, but attribution may be possible in the long run," and it is "unclear how to

mitigate the NC3 vulnerability." Teams without these treatments were told either that they had "no access to Other State's NC3" or that there was "no vulnerability within Our State's NC3."

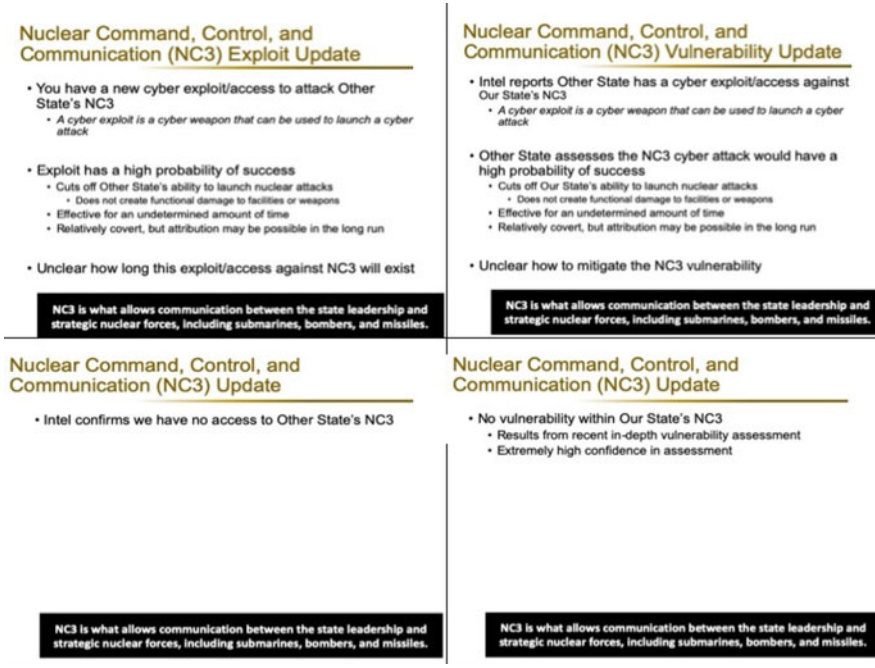

FIGURE 3. *Treatment examples*

Both the access/exploit treatment and the vulnerability treatment were designed to evoke a highly effective cyber tool (in fact, this kind of capability is unlikely unless a state built a highly centralized NC3 with very few redundancies). Empirical work has found that cyber operations rarely have an effect on behaviors.[57] We wanted a treatment that biased against these findings so that, if we still found no effect from cyber operations even with an extremely significant exploit and vulnerability, then we would be able to say that *even if* cyber could create large effects, it still would not play a large role in the crisis dynamics. If we designed the treatment in the other direction, with limited effectiveness or vulnerability, then we wouldn't be able to rule out whether cyber would have mattered if it had been able to create more significant effects. We are therefore simulating the worst-case scenario—again, gaming has the advantage of being able to generate synthetic data about even rare circumstances.

57. Gomez and Whyte 2021; Kostyuk and Wayne 2020; Kostyuk and Zhukov 2019; Kreps and Schneider 2019; Valeriano, Jensen, and Maness 2018.

Despite the bias toward a significant cyber capability/vulnerability, we still believed that unique characteristics about cyber operations (uncertainty about effectiveness, uncertainty about how long the effect or the access would last, uncertainty about where the vulnerability exists) mattered to these decisions and integrated those characteristics into the treatment. Therefore, players had to deal with inherent uncertainty for both the cyber vulnerability and the cyber exploit as they debated whether and how to use and respond to the cyber treatments.

The Sample

The International Crisis Wargame was played in eleven different locations and twelve different iterations, including the Naval War College, Thailand, the Harvard Belfer Center, Norway, Argentina, Sandia National Labs, Tufts University, the Naval Postgraduate School, MIT, Stanford University, and a virtual interface.[58] A total of 580 players have taken part (Table 2).[59] Of those players, 71 percent listed themselves as Americans and 29 percent as other nationalities.[60] Similarly, the participants skewed male, with about 73 percent identifying as male and 27 percent as female. Players spanned the age spectrum, with 19 percent under thirty, 25 percent between thirty and thirty-nine, 28 percent forty to forty-nine, 17 percent fifty to fifty-nine, and 11 percent over sixty years old. Expertise was also heterogeneous, with 37 percent having private industry or military experience, 27 percent government experience, 27 percent academic experience, and 13 percent NGO experience. Most (56%) identified as a senior professional, with fifteen or more years of

58. We advertise the game as a generic "international crisis" wargame to mitigate potential bias toward the use of cyber operations. In some cases, players were attracted to the game by advertisements that discussed the impact of new technologies (including cyber) on crisis stability. The Naval War College, Belfer Center, and NPS games were conducted with students, consulate members, private-sector leaders, and US cyber and nuclear policy experts. Games played in Norway and Argentina were conducted after a Naval War College alumni event, so the participants were predominantly naval officers. The game played in Thailand (scenario 1 only) was conducted as the last event of a Track 2 event with Indian and Pakistani experts. The Sandia game was conducted in conjunction with the Project on Nuclear Issues; players were technical nuclear experts from Sandia or early-career nuclear-policy personnel. Game iterations at Tufts University and MIT included graduate students from the international relations and business schools. The Stanford game included Silicon Valley technologists as well as policy experts and diplomats in the Bay Area. Finally, users of the virtual interface brought all levels of expertise, from student to former head of state.

59. Players were asked to provide consent before participating in the game—using a signed paper form for in-person games, and a similar online form filled out during registration for the virtual game. Participants were told they were taking part in a research study and that at any time they could stop participation or choose not to answer the survey or crisis response plan questionnaire. All data from participants were kept confidential, and no identifying information was collected. Participants were not compensated monetarily for their time (this was included in the consent form), but the research team provided refreshments throughout the experience. In many cases, the games occurred within a larger event that participants were paid (by the host institution or their own institution) to attend.

60. Non-American participation from Argentina, Barbados, Brazil, Bulgaria, Canada, Chile, Colombia, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, Greece, Germany, Guyana, Haiti, India, Jamaica, Japan, Netherlands, Norway, Oman, Pakistan, Peru, Poland, Portugal, Romania, Spain, St. Vincent and the Grenadines, Sweden, Taiwan, Ukraine, United Kingdom, and Uruguay.

TABLE 2. *Game iterations by location and date*

Location	*Date*	*Players*	*Groups*
Bangkok*	10 May 2018	18	3
Naval Postgraduate School*	5 September 2018	15	3
Naval War College*	16 November 2018	59	14
Harvard Belfer Center	7 December 2018	13	2
Naval War College	18 December 2018	9	2
Bergen, Norway	11 April 2019	27	5
Sandia National Laboratory	10 July 2019	51	11
Naval War College	21 August 2019	62	13
Argentina	29 August 2019	57	12
MIT	7 January 2020	81	14
Tufts	24 January 2020	36	7
Stanford	5 March 2020	77	15
Virtual	27 May 2020	75	16

*Groups played only scenario 1.

experience; 26 percent as mid-level, and 18 percent as student or entry level. Looking more granularly at specific experience, 15 percent identified themselves as either a technical or policy cyber expert, and 16 percent identified with similar nuclear expertise (see the online supplement for a breakdown of demographic variables).

Data Collection

Data were collected in the game in three ways. The primary method of outcome measurement was the response plan, written by each group collectively (Figure 4). They described their overall plan, chose their response actions (from a preset list of sixteen possible actions), and then described their end state and prioritized objectives. The crisis response plan collected data on the outcome variable, but surveys—the second form of data collection—were used to measure individual behaviors and motivations behind response plans. Finally, facilitator and plenary notes were used in some games to capture group dynamics, conversations within the game, and lessons learned from players.

Based on our game design, what evidence would support or disprove the three hypotheses about technology and strategic stability? First, for the hypothesis that uncertainty leads to preemption, we would expect teams with cyber vulnerabilities to be more likely to launch nuclear weapons or place them in their response plan. We would expect also that teams with vulnerability are more likely to predelegate control, automate, and place forces on nuclear alert. In the survey and the response plan, we would expect players to explain their choices by discussing the uncertainty of controlling their nuclear forces given the adversary's cyber exploit and uncertainty about solving the vulnerability. Alternatively, if (per the second hypothesis) cyber uncertainty leads to restraint and deterrence, we would expect teams with vulnerability not to use nuclear weapons and teams with both the vulnerability and the exploit to restrain their own use of NC3 exploits. These teams would also be

Response Plan

Describe your Overall Response Plan/Course of Action:

Select Response Actions (check all that apply):

___Diplomacy
___Economic Punishment
___Economic Incentives
___Cyber Attack on Civilian Targets
___Cyber Attack on Military Targets
___Cyber Attack on Nuclear C3
___Information Operations
___Conduct Intelligence
___Invade Territory
___Mobilize Forces
___Fortify Defenses
___Nuclear Alert
___Air Attack
___Maritime Attack
___Nuclear Attack
___Special Forces Operations

Describe your Response Plan's desired end state:

Below are potential objectives of your Response Plan. Please rank these objectives in order of their importance to your plan (1 is the most important). Cross out objectives that are not a factor in your plan:

____ Re-take territory
____ Deter/defend against further conventional attack
____ Deter nuclear attack
____ Ensure survival of regime
____ Defend the homeland
____ Find a peaceful end state
____ Ensure international support
____ Other: _____

FIGURE 4. *Response plan form*

less likely to take risky counterforce strategies, and in surveys they would provide evidence that they were uncertain of both their vulnerabilities and their cyber capabilities. Finally, if decisions are driven instead by misplaced certainty (per the third hypothesis), we would expect the cyber exploit to correlate with nuclear use, as well as campaigns of counterforce, and potentially even nuclear alert and predelegation to support those campaigns. Teams would be more likely to use the cyber exploit, with evidence from surveys that players were confident of their cyber capabilities.

Game Campaign Strategies

What did two years of wargames across 580 players and 115 games reveal about emerging technologies and strategic stability? What was the effect of NC3 cyber exploits and vulnerabilities on nuclear use? How did having and responding to these cyber threats affect the crisis response options that players crafted? What differences did we see between our low-intensity scenario 1 and the higher-intensity scenario 2? Finally, what role did uncertainty play in our game?

First, looking at crisis response plans across both scenarios, we noticed patterns of behavior regardless of treatment condition. In particular, in scenario 1, teams were most likely to rely on diplomacy and sanctions while using the military for defensive or hedging means, such as mobilizing forces (instead of launching a counter-attack), fortifying defenses, conducting intelligence and information operations, and to a somewhat lesser extent conducting special forces operations. Many of these games (though not most) also included cyber attacks on civilian (30%) and military targets (40%), as well as nuclear alert (33%). No team in scenario 1 chose to launch a nuclear attack.

Player behavior in scenario 1 generally reflected hedging, or restraint. In describing their desired end state, players often used phrases like "return to status quo"[61] or "deescalating tension,"[62] all while "garnering international support."[63] In surveys, players used similar language, explaining that they developed crisis strategies with the intent to "return to status quo,"[64] while focusing on "non-escalation, give diplomacy a chance"[65] and "immediate conflict de-escalation and invocation of international pressure/intervention."[66] Players in the first scenario generally believed that, despite the Other State invasion, the crisis could be managed without significant use of military force. For example, one team explained that they intended to "recapture control of grey zone principally through economic and political pressure while ensuring that other state cannot coerce us or dominate us militarily."[67]

In this attempt to manage the crisis and avoid escalation, teams focused on information strategies and controlling narratives to garner international support. Players said they "needed international support" and to "increase outreach to international community."[68] In their crisis response plans, one team said that they aimed to "create leverage over Other State by having a stronger narrative. 'Other State intentionally escalated the situation in Gray Region through organizing a riot.' We set up a campaign of diplomatic pressure, isolate and drain them economically. Military we are merely posturing defensively along the border, we are not (yet) hitting back."[69] All of these actions were below the use of force, aiming to deter further aggression, control escalation to more violent uses of conventional military power, and avoid nuclear use. As one player explained in the survey, the team developed their strategy "looking to engage in peaceful/diplomatic discussions first."[70] Another team wrote that their desired end state included "retaking Gray Region and returning it to

61. Almost a quarter of scenario 1 response plans used the exact term "status quo." Only three teams suggested that they might use the crisis to change the status quo to advantage Our State.
62. 29AUG1921H, scenario 1.
63. Thirty percent of the crisis response plans for scenario 1 mentioned international support.
64. 07DEC1811A6, survey.
65. 07DEC1811A7, survey.
66. 16NOV1811A4, survey.
67. 16NOV1831G, scenario 1.
68. 10JUL1912D4, survey.
69. 27MAY2021K, scenario 1.
70. 21AUG1921E5, survey.

autonomy without us escalating the conflict, avoiding nuclear especially."[71] Interestingly, many of the responses also discussed the role of a port in the Gray Zone and its importance to their desired end state. This is remarkable, given that this port is only mentioned in the players' briefing booklets and is not briefed or highlighted.[72]

As expected, strategies changed in the second scenario. Teams transitioned from hedging strategies to more active measures, including maritime (78%) and air attacks (85%), special forces operations (88%), and increases in cyber attacks on military, civilian, and NC3 targets. As one player explained, "We choose to leverage conventional strikes to alter the balance of power if possible."[73] But despite the overall trend toward more active measures, most games still featured some restraint, with only a minority of games (37%) including a counter-invasion of territory. And while nuclear alert increased to 81 percent of the scenario 2 games, only 9 percent featured the use of nuclear weapons. As in scenario 1, teams focused on returning to the status quo, but with a stronger focus on avoiding nuclear use. This sentiment was best illustrated by one of the groups in the August 2019 Naval War College iteration, who wrote in their crisis response plan that they wanted to "defend and take back homeland (inclusive of Gray Region) while reducing loses to civilian lives and military personnel without nuclear impact."[74] Players also explicitly identified this desire in surveys. When asked why they chose not to use nuclear weapons in the second scenario, they responded that they "wanted to avoid nuclear use if possible,"[75] "avoid nuclear war at all cost,"[76] and "avoid catastrophic losses and deaths."[77]

Only a minority of teams wanted to change the status quo territorial borders. Few sought either to surrender Gray Region territory or to use the crisis as an opportunity to take Other State territory. Across these desired end states, however, there was a focus on counterforce efforts to disable Other State's ability to use nuclear weapons. Both team response plans and individual surveys spoke often about this desire to destroy the adversary's first strike capability. For example, in one survey, an individual wrote that they intended to use their cross-domain conventional and nuclear capabilities to "create opening to destroy nuclear capabilities."[78] While cyber attacks on NC3 were the preferred option for these counterforce attempts, groups also discussed special operations attacks and air strikes (Figure 5).

71. 07JAN2031G, scenario 1.
72. This focus on the port was especially noticeable with our American players, who struggled to understand why a state might be willing to go to war over a semi-autonomous region if it did not include a strategic asset.
73. 27MAY2042B1, survey.
74. 21AUG1922F, scenario 2.
75. 10JUL1912K3, survey.
76. 05MAR2042O5, survey.
77. 05MAR2012D2, survey.
78. 24JAN2022C3, survey.

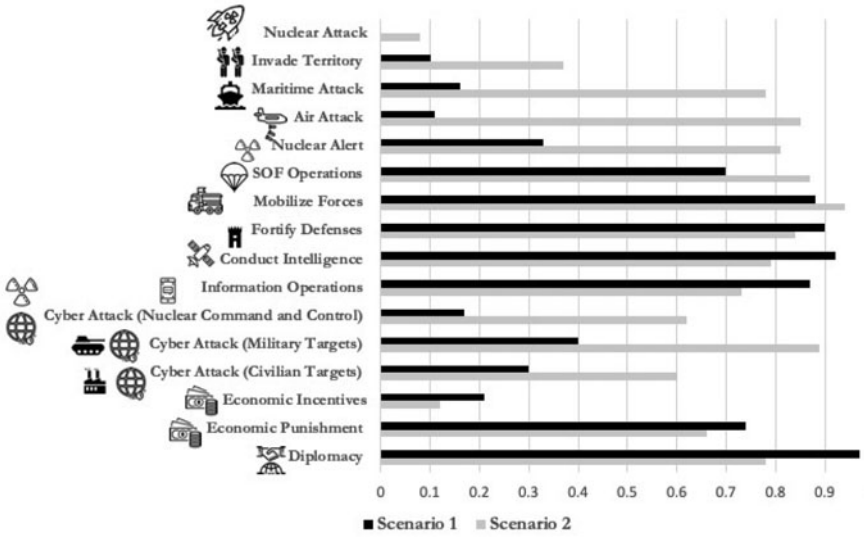

FIGURE 5. *Frequency of use of various means in games*

Nuclear Use

The discussion so far looked at outcomes across groups, but were our treatment and control groups more likely to opt for nuclear alert or nuclear use? Secondarily, did teams with the NC3 exploit use it? And how did having both the exploit and the vulnerability affect these dynamics?

In scenario 1, no team chose nuclear attack, regardless of treatment (Figure 6). However, we did see variance in teams that chose to put forces on nuclear alert. Groups with a cyber exploit were more likely to do so; 38 percent of our groups with both an exploit and a vulnerability chose to, and 41 percent of the exploit-only groups did. This is in contrast to our control and vulnerability groups, with 28 percent of the teams in both these groups electing to put forces on nuclear alert. Thus, contrary to hypotheses that might link cyber vulnerabilities with fear and nuclear alert, in our games it was the cyber exploits that had a larger effect on nuclear alert decisions.

This relationship between cyber exploits and nuclear instability continued in the second scenario (Figure 7). Teams given just the vulnerability were the least likely to put their forces on nuclear alert, while almost 90 percent of the teams with exploits did. The group most likely to use nuclear weapons in the second scenario was the exploit-and-no-vulnerability group (21%); the only other group to use nuclear weapons was the full treatment group with both the exploit and vulnerability (11%). No teams without an exploit used nuclear weapons.

But why would the exploit be more important than the vulnerability to both nuclear alert and nuclear use? Hypotheses about technology and uncertainty would suggest that perceptions of vulnerability lead states to either increase their nuclear readiness

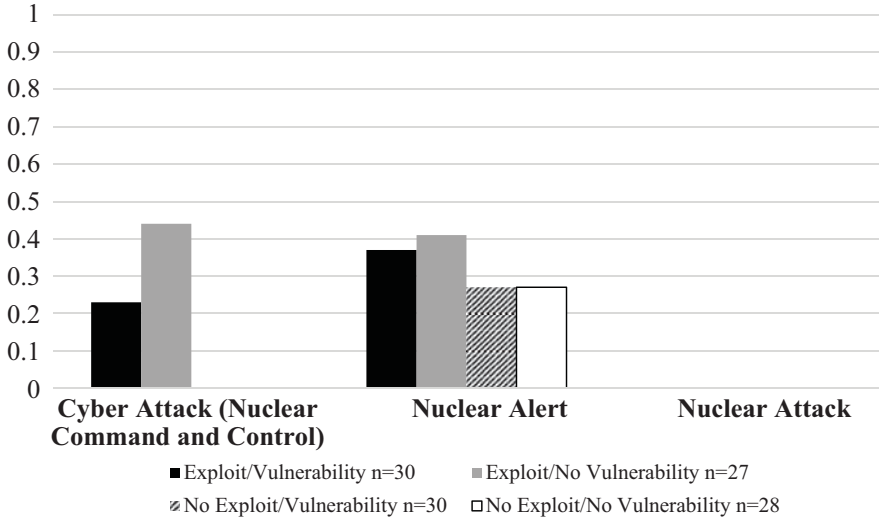

FIGURE 6. *Propensity to use cyber or nuclear options, scenario 1*

or preemptively use nuclear weapons. However, in our game, windows of vulnerability had little impact on preemptive nuclear use and a complicated relationship with nuclear readiness. Indeed, when we asked the players with a cyber vulnerability how it affected what means they used during the game, many indicated that it

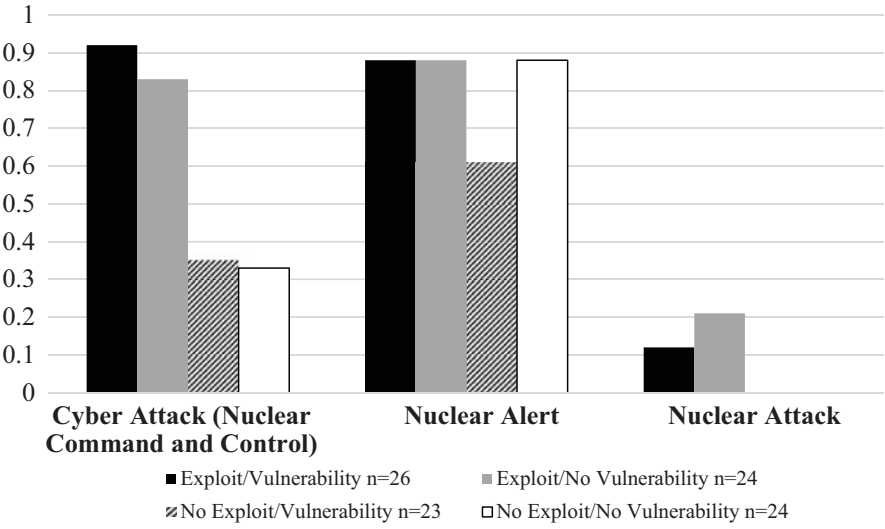

FIGURE 7. *Propensity to use cyber or nuclear options, scenario 2*

restrained their nuclear use—evidence for the second (uncertainty and restraint) hypothesis. This was especially the case for groups with a vulnerability and no exploit. Across both scenarios, many of the players in those groups (60% in the first scenario and 48% in the second scenario) believed that cyber vulnerability led to greater nuclear restraint. For example, one asymmetric vulnerability team noted in their response plan that they must "avoid nuclear war if possible as they have access to our C3, but we can't access theirs."[79] This was a sentiment we found echoed in the players' surveys, in which players explained they chose not to use their nuclear weapons because they "thought NC3 might be compromised."[80] Another player explained that "we didn't think we'd be able to with their cyber exploit,"[81] and most succinctly, a player reported that there were "doubts on [whether] our nuclear deterrence was real."[82]

In contrast, almost none of the response plans indicated that the vulnerability incentivized nuclear use. No crisis response plan tied a team's decision to use nuclear weapons with fear about cyber vulnerabilities. Only a single group with a vulnerability had a majority of players indicate in their surveys that the vulnerability incentivized nuclear use. However, this group had an exploit as well, which the majority of the team also said influenced decisions for nuclear use. Simply put, for the teams given cyber vulnerabilities, uncertainty mattered. But it didn't create preemption or escalation. Instead, it created incentives for restraint.

While cyber vulnerabilities did not create incentives for preemption, they did have a more insidious effect on nuclear stability. To negate the vulnerability, many teams decided to turn to predelegation of nuclear use to lower levels of command, or even to automate nuclear use. Latent within the crisis response plans we found evidence that players were willing to sacrifice safety and control to limit the potential effect of the NC3 vulnerabilities on second strike. Remarkably, players were willing to remove the human from the loop, substituting the uncertainty about the extent of cyber vulnerabilities within NC3 with a (perhaps misplaced) certainty in autonomous nuclear launch decisions. Further, teams suggested that this automation or predelegation could be a deterrent signal, designed to decrease the adversary's confidence in their own NC3 cyber exploit. For example, one team explained that they would "emphasize dead hand orders to our strategic nuclear forces; emphasize preemption is a way of getting them killed as well."[83] Another asymmetric vulnerability team wrote that they would "protect our NC3 by disabling to bring to an autonomous level."[84] Perhaps most alarmingly, one of the full treatment groups in scenario 1 predelegated nuclear use to lower echelons, and charged these commanders with launching a nuclear retaliation in the case of either nuclear attack or an attack on

79. 27MAY2032P, scenario 2.
80. 27MAY2012M5, survey.
81. 10JUL1932G3, survey.
82. 07JAN2032H3, survey.
83. 27MAY2032D, scenario 2.
84. 27MAY2032I, scenario 2.

NC3. The group wrote that they planned to "separate part of our nuclear deterrence from our NC3 system by delegating authority to lower level commanders to mount a nuclear retaliation to either a nuclear attack or successful attack on our NC3, inform Other State of this."[85]

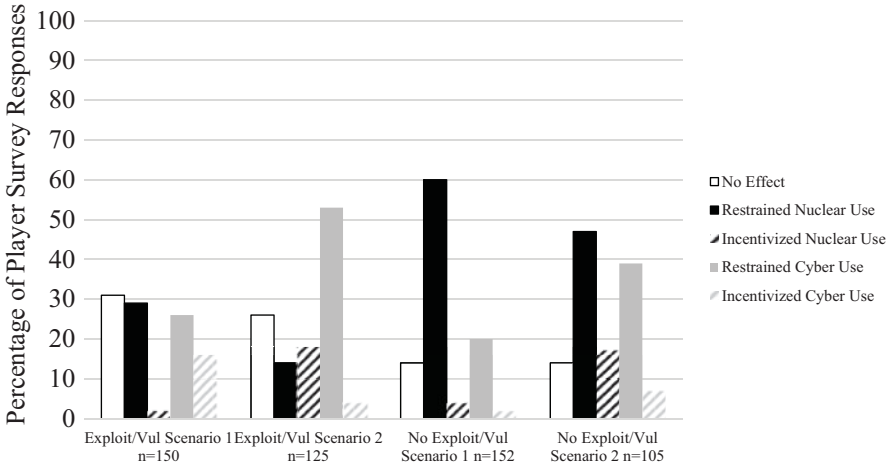

FIGURE 8. *Responses to "What role did having an NC3 vulnerability play in your response plan?"*

The role of the cyber vulnerability, versus the exploit, becomes more apparent when looking at survey responses from players asked what role having an NC3 vulnerability played in their response plan (Figure 8). For the teams with no exploit, the vulnerability overwhelmingly incentivized nuclear restraint; almost 60 percent of the teams in the first scenario answered that the vulnerability led to nuclear restraint. Even in scenario 2, most reported that vulnerability incentivized restraint, whether nuclear or cyber. In contrast, teams with the vulnerability and the exploit were less likely to say that the vulnerability led to nuclear restraint, though it did restrain cyber use (especially in scenario 2). When it came to restraint, the vulnerability was more important than the exploit.

Cyber Exploit Use

If cyber vulnerabilities aren't driving nuclear use in these games, what role are the exploits playing? One of the most interesting findings of this game series is how many teams chose to use the NC3 cyber exploit—suggesting that players viewed

85. 16NOV1811E, scenario 1.

their capabilities quite differently from their vulnerabilities. They may have been uncertain about their own vulnerabilities, leading to restraint, but they were perhaps overconfident in their cyber capabilities, with dangerous implications for strategic stability.

In scenario 1, 45 percent of the teams with the exploit and no vulnerability chose to use their cyber weapons. By the second scenario, 82 percent of the asymmetric exploit groups chose to use their cyber exploit; 92 percent of the exploit/vulnerability groups did the same. Most remarkably, the exploit was so popular in the second scenario that a little over 30 percent of the groups that were *not* given a NC3 cyber exploit treatment added the cyber-NC3 exploit into their crisis response plan—many making it a linchpin of the plan. This is all the more fascinating because those who wrote in a NC3 exploit were given no details in the order of battle about the ability or extent of any potential cyber weapon against nuclear targets. Therefore, they were bringing into the game their own beliefs about cyber exploit effectiveness—beliefs that seemed to skew toward overconfidence.

Why was the exploit used so much in the game? For some teams, it countered the NC3 vulnerability. For example, one team with both the exploit and the vulnerability explained they used the exploit because of a concern about their NC3 vulnerability, writing in their crisis plan, "We must assume our NC3 system is compromised; therefore, we will use cyber attack against Other State NC3 to buy time in preventing nuclear attack."[86] When we asked players in the survey why they used the exploit, one explained they were motivated by "concern that Other State was about to launch nuclear attack, not deterred by Our State nuclear capability."[87] Indeed, many of the dual treatment groups suggested that they felt pressure to use their exploit because of the vulnerability—explaining, for instance, that they needed to "conduct cyber attack on NC3 and military C2 to gain advantage."[88] This is a remarkable finding for cyber deterrence, suggesting that (especially in high-stakes scenarios) the threat of cyber vulnerabilities may not be powerful enough to deter cyber attacks.[89]

But deciding to use the exploit was more than just a response to the vulnerability; it was also a covetable counterforce option and a new foreign policy tool for teams to exercise. Often, teams with the exploit viewed the cyber weapon as both a signaling mechanism and a useful counterforce option. As one asymmetric vulnerability exploit team explained, "We are going with the cyber attacks on nuclear C3. Try to keep undercover, but our goal is to show we can defend ourselves."[90] Given that Our State and Other State were otherwise symmetrical, the inclusion of the cyber exploit appeared to tip the perceived balance of power in the crisis for many of the

86. 27MAY2012M, scenario 2.
87. 10JUL1912B2, survey.
88. 10JUL1912K, scenario 2; 07DEC1812A, scenario 2; 11APR1912A, scenario 2; 11APR1912C, scenario 2; 10JUL1912D, scenario 2; 10JUL1912K, scenario 2.
89. For more on the general cyber use within the game, see Schneider, Schechter, and Shaffer 2022.
90. 07DEC1821B, scenario 1.

teams. This made the cyber exploit a more credible and useful signaling tool and incentivized more assertive counterforce strategies (especially in scenario 2).

Many respondents explained that they chose to use the cyber exploit because it represented a "less escalatory option." This seems to support suggestions in other cyber literature that cyber operations are viewed differently than conventional military options and are therefore more likely to be used to increase the bargaining space and foreign policy options in crises. Players seemed to believe that cyber operations were less escalatory than other options, particularly because they were considered less visible or more covert. Many teams rationalized that cyber attacks on NC3 might not be attributable (or at least were less likely to be attributed than other means). For example, one team used their NC3 exploit, but stipulated that it was "covert."[91] Other teams lumped cyber exploits against NC3 with special operations counterforce missions, perhaps signaling a belief that these operations were similarly less escalatory than air strikes, maritime strikes, or invasions of territory.[92]

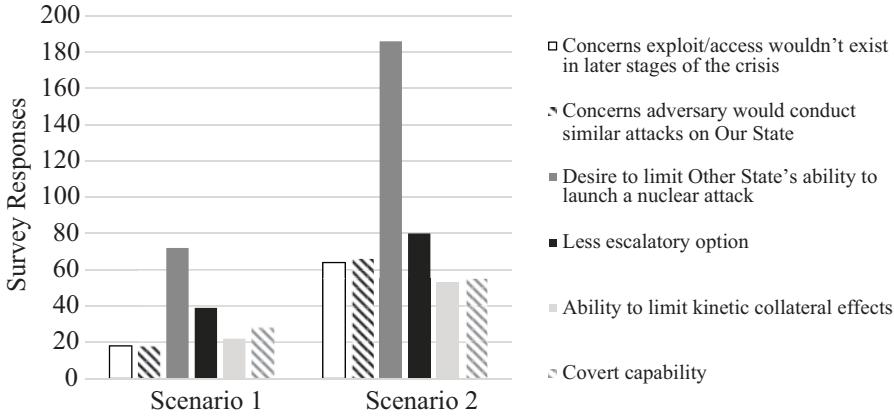

FIGURE 9. *Responses to "Why did you use your NC3 exploit?"*

Most importantly for the overall crisis outcomes, the cyber exploit appeared to embolden counterforce initiatives, especially for the asymmetric exploit groups. In fact, when we asked players why they chose to use the exploit, the dominant response in both scenarios was that it was part of a counterforce strategy, a "desire to limit Other State's ability to launch a nuclear attack." When we coded response plans for either cross-domain or cyber counterforce efforts, we found that forty-three teams explicitly discussed counterforce campaigns in the written description of

91. 07JAN2022D, scenario 2.
92. 05MAR202B, scenario 1 and 2.

their crisis response plan for scenario 2.[93] Of those forty-three teams, twenty discussed using the cyber NC3 exploit to counter Other State's nuclear strike capability; nineteen used it with a complementary cross-domain counterforce campaign. Only four said they would conduct cross-domain counterforce against Other State without the cyber exploit, and none of these had been given the NC3 cyber exploit in the game setup. This evidence points to Gartzke and Lindsay's cyber commitment problem and suggests that one of the primary dangers of cyber exploits for nuclear stability is that they create incentives for offensive campaigns in other domains.

This remarkable relationship between the cyber exploit and cross-domain counterforce campaigns was evident throughout the crisis response plans coded for counterforce. For example, one team with an asymmetric exploit treatment said that their crisis response plan in scenario 2 involved "cyber attack on nuclear C3 and come out to them. Give them three hours to move back and leave the territory. Communications to the world that we are pressuring Other State to hold the invasion or else we are going to move with the nuclear attack."[94] Other teams explicitly linked the cyber exploit to counterforce campaigns in other domains, sometimes also pairing these cyber attacks on the NC3 with cyber attacks on military and civilian infrastructure. For instance, an asymmetric exploit team developed a crisis response plan that would "employ NC3 cyber attack, use conventional attacks to destroy Other Country's nuclear weapons, then retake lost territory and compel Other Country to surrender."[95] Another asymmetric group proposed "cyber attack on N3 combined with air strike on their nuclear capabilities," while also hedging by placing their forces on "nuclear alert."[96] Indeed, in these asymmetric exploit plans, alert seems to be an attempt to prepare for potential adversary retaliation after the emboldened counterforce campaign. One team said they would "(1) Alert nuclear forces to reduce vulnerability to preemption but do not initiate nuclear employment (2) trigger exploit to pressure them."[97]

Part of why exploits may have led to greater use of counterforce campaigns (or even nuclear use in some groups) is that players tended to believe in the efficacy of the cyber exploit (while sometimes downplaying the vulnerability).[98] It is extraordinary how much confidence players had in this cyber exploit (especially given that the cyber exploit treatment used the same uncertainty language as the vulnerability treatment). Nowhere was this more evident than in the crisis response plans of teams that were not given the exploit but still wrote it into their crisis response plan. For example, for scenario 2 one control group (no exploit or vulnerability)

93. More teams used the cyber NC3 exploit in the means section of their crisis response plan, but we coded only the qualitative descriptions of the response plan for explicit counterforce discussions.
94. 07DEC1822B, scenario 2.
95. 29AUG1922B, scenario 2.
96. 11APR1922E, scenario 2.
97. 05MAR202I, scenario 2.
98. Many teams with the vulnerability discussed remediation options in their crisis response plan, including patching or "demonstrating NC3 resilience" (05MAR203C, see also 05MAR203A). This belief that they could mitigate their vulnerability came despite the treatment inject explicitly telling players that they did not know where this vulnerability existed and had no way of remediating it.

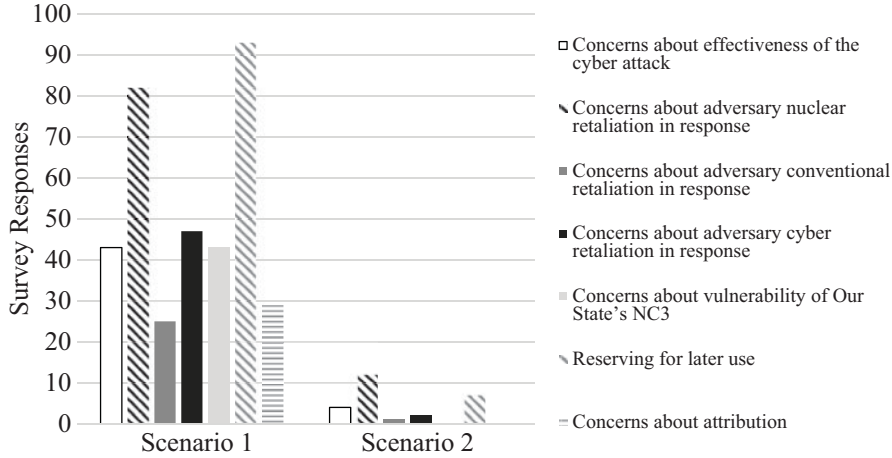

FIGURE 10. *Responses to "Why didn't you use your NC3 exploit?"*

wrote in their crisis response plan that they would "deter nuclear attack by cyber attack on nuclear C3."[99] Another team that had a vulnerability but no exploit centered their whole scenario 2 response plan strategy on exploiting Other State's NC3, proposing to "cut off NC3 and publicly 'announce' that every nuclear site including submarines have [autonomic] authority to launch a retaliation strike in case: (a) we are attacked nuclearly, (b) we lose the war."[100]

That's not to say that cyber exploits were always used. For the minority of teams that chose not to use them, their restraint revealed when and why cyber operations might induce caution for users. While many teams chose to "reserve" the NC3 exploit for scenario 2,[101] many others cited concerns about adversary nuclear retaliation in response (and a desire to use the exploit later in the crisis). As one dual-treatment group explained, despite having a cyber exploit they chose to "maintain Other State's C3 (to avoid unintended effects)."[102] Perceptions of cyber asymmetry also mattered, at least in the first scenario. In scenario 1, the percentage of exploit/vulnerability teams that used the exploit was approximately half the asymmetric group. This large delta suggests that having the vulnerability did create incentives for cyber restraint for some groups. Further, when asked about the impact of the vulnerability on their overall crisis response plan, 23 percent of the exploit/vulnerability group in scenario 1 answered that it restrained their cyber use. Thus, while cyber deterrence

99. 07JAN2042B, scenario 2.
100. 07JAN2032E, scenario 2.
101. 27MAY2011H, scenario 1.
102. 11APR1911B, scenario 1.

failed in high-stakes scenario 2, in scenario 1 cyber vulnerabilities deterred some actors from using the exploit.

Conclusion

Our game-based study suggests that an emerging technology, cyber operations, plays a complicated role in nuclear stability—with implications not only for understanding how cyber operations might affect near-term crises, but also for understanding emerging technology and stability decisions. Cyber weapons are an interesting case with which to explore hypotheses about technology and stability because they are known for their uncertainty. Early work suggested that the uncertainty inherent in cyber technologies would lead to security dilemmas, arms races, and potentially even nuclear use. However, the work described here suggests that cyber uncertainty is what players make of it. The uncertainties of cyber vulnerabilities led not to escalation or preemption (hypothesis 1), but instead to restraint (hypothesis 2). Finally, it was certainty about cyber exploit effectiveness (hypothesis 3)—not uncertainty about cyber vulnerabilities—that led to more aggressive counterforce campaigns, nuclear alert, and even in some cases nuclear use. Where cyber uncertainty was dangerous was when it created incentives for strategies—like predelegation or automation—that replaced safety and control with preemption and escalation.

While nuclear restraint was not a direct focus of the research, it is noteworthy how little nuclear use we saw in the game despite scenarios that put the teams right on the brink of nuclear war. The player surveys and response plans provide evidence that in our sample the nuclear taboo remains strong and limits the tendency toward nuclear preemption. As players in a NC3 vulnerability team explained, "The actual firing of nuclear weapons is a Rubicon we did not want to cross first."[103] In some situations when a player did advocate for nuclear use, they were overruled by their group—as one individual wrote, "overruled and impeached as head of executive for pushing to use nuclear arsenal."[104] Ultimately, the nuclear taboo held in the vast majority of cases, even for asymmetrically vulnerable groups. As one survey respondent mentioned, the players thought about nuclear weapons for "second strike only."[105] The continued evidence for the strength of the nuclear taboo is important for those worried that cyber vulnerabilities might exacerbate the security dilemma and incentivize nuclear first strike.[106]

The implications for cyber and other pathways to nuclear use are less comforting. First, though nuclear experts may have believed the nuclear taboo and other norms of nuclear restraint would easily extend to cyber exploits against NC3, our game demonstrates the strong incentives states have to use cyber exploits against NC3, especially

103. 11APR1912C5.
104. 24JAN2022C4.
105. 18DEC1832A4.
106. Tannenwald 2007.

when they provide an advantage in an otherwise symmetrical fight. Players who used their NC3 exploit included nuclear and cyber experts, as well as lay citizens and students. The pressure to use the exploit only went up as we increased the intensity of the scenario, and even a reciprocal vulnerability could not alleviate the attraction of the NC3 exploit. What is most interesting is the potential overconfidence in the NC3 exploit. Despite similar hedging language regarding the exploit on the one hand and vulnerability to the exploit on the other hand, players tended to overemphasize the capability and underemphasize the vulnerability. This was unexpected for us, and future work should test how changes in the exploit treatment might affect players' willingness to use the exploit. It appeared that cyber operations' being covert, virtual, and perhaps deniable convinced players that this was a low-escalation-risk option, too valuable to leave on the table (especially given the time-sensitive nature of cyber exploits). What this game suggests, at the very least, is that states may value highly effective cyber exploits against NC3 and so will likely attempt to develop the cyber capabilities to attack these systems. If practitioners believe that a norm of restraint regarding cyber attacks on NC3 is important for nuclear stability, they should be aware that it may be difficult to reach.

The relationship between the exploit (especially without the vulnerability) and more aggressive counterforce campaigns is perhaps the most troubling of our findings for nuclear stability. Buoyed by exploit-induced overconfidence, groups with an asymmetric exploit were more likely to opt for air or maritime counterforce strikes. This is part of a larger incentive structure toward counterforce campaigns which is only exacerbated by perceptions of asymmetric cyber advantages.[107] The ability to temporarily pacify Other State's nuclear capabilities opened a window of opportunity for aggression, a concept explicitly identified in surveys when players spoke of cyber exploits as an "open possibility to disable nuclear forces conventionally."[108] Although eventually overruled by their group, another player proposed to "use cyber to remove their second strike capabilities and overwhelm them with our nuke."[109] This aligns, at least partially, with Lieber and Press, who found that new capabilities make counterforce viable (or appear viable) and nuclear capabilities appear less assured.

Also of concern is the potential relationship between cyber operations and decisions for predelegation and nuclear alert. Teams with the exploits were more likely to go to nuclear alert, probably as a preemptive hedging response related to their more aggressive planned counterforce campaigns. Groups with the asymmetric vulnerability also had incentives to opt for more dangerous nuclear strategies. The most concerning campaign plans were those that discussed automation, a "dead hand," or predelegation in response to cyber vulnerabilities—perhaps best illustrated by one survey explanation of how cyber vulnerabilities affected their crisis response

107. Bowers and Hiim 2021; Clary and Narang 2019; Lieber and Press 2017; Long and Green 2015.
108. 24JAN2022C4.
109. 10JUL1922C5.

plan: that they "incentivized devolution and autonomy of nuclear command. Incentivized de-digitization and movement to analogue NC2."[110] Previous research has concluded that decisions to put forces on nuclear alert or to automate nuclear decision making also increase the chance of accidental or inadvertent escalation to nuclear use, so these choices are concerning for nuclear stability.[111]

While this exploration was scoped to explore the impact of cyber operations on a large population's willingness to use nuclear weapons, the game series suggests a series of contextual extensions of this research on the role of expertise or the impact of balance of power. For example, the International Crisis Wargame Series was played over multiple years and with an extremely heterogeneous sample of 580 participants. Future research could disaggregate this population to examine the role of expertise at a much more granular level. How do different cultures, different types of expertise, and different levels of expertise lead to different outcomes or deliberations within the game series?

We also want to highlight the importance of the design choice to focus on strictly symmetrical states. Our game presented players with a strictly symmetric balance of power, varying only cyber exploits and vulnerabilities into NC3. However, we wondered whether asymmetries in power could impact final outcomes. While we couldn't introduce this as a separate treatment in the game series (due to concerns about iteration and sample size), we included a survey question on how players' crisis response plans would change if the adversary were either more or less capable. In scenario 1, most responses suggested asymmetry would increase incentives for conventional attack, though the number fell in scenario 2. Perhaps most interesting for questions about the use and impact of cyber operations in future crises, across both scenarios and more and less capable adversaries, 40 percent or more of respondents believed that asymmetry would have increased their cyber activity. This suggests that cyber operations are perceived as valuable tools for asymmetric conflict (in both directions). More research should explore how asymmetries would affect the impact of cyber vulnerabilities on nuclear crises.

Methodologically, this paper presents one of the first large-*N* quasi-experimental wargame series. Despite a long history of wargaming in both political science and defense planning, we have very little empirical work on the methodology of wargames—or what makes some games better than others. In the absence of this work, we had to make choices about moves, sides, and abstraction that drew from social-scientific use of experiments. Future work should look at how wargames may differ from pure experiments—including explorations of the impact of immersion, design choices that affect external validity, the role of expertise, and the intervening role of the group on game behaviors and outcomes. We hope that future researchers use wargames not only to shed light on tough empirical questions like

110. 21AUG1932J1.
111. Blair 2011; Sagan 1997; Sagan and Suri 2003.

the impact of nuclear or cyber weapons, but also to refine methodological choices within wargames.

Most importantly, this game series has implications for states' choices about NC3 modernization, nuclear strategy, and cyber operations against nuclear-armed adversaries. As states' NC3 become more digital, more centralized, and more automated it becomes more likely that during crises adversary states will look to NC3 vulnerabilities as an opportunity to shift the balance of power.[112] Our research suggests there is already a tendency toward overconfidence when it comes to offensive cyber capabilities, and if decision makers believe they have a highly effective exploit against NC3, it could increase the chance of both conventional and nuclear counterforce campaigns. Further, some answers to NC3 vulnerabilities—delegating launch authorities, placing platforms on alert, and automating decision making—are prone to dangerous mistakes. This leaves policymakers in the uncomfortable position of restraining their own use of cyber counterforce for the sake of strategic stability, but having to do so without any real ability to verify whether adversaries are upholding the same norms.

Is there a solution? Can nuclear arsenals just go back to the days of the floppy disk? The answer is not to avoid all digital modernization. It is likely impossible for all cyber vulnerabilities to be mitigated. However, states can invest more in resilient network architectures, limiting centralized hubs, distributing nodes, and creating more linkages and pathways between control loci. By making systems less vulnerable to systemic outages, states may be less confident in their offensive capabilities, deeming it too difficult, too expensive, and not beneficial enough to launch cyber attacks. Our research shows that uncertainty in the cyber context creates incentives for restraint, and so investments in defense and resilience for nuclear networks may increase attacker uncertainty to a point that could disincentivize NC3 exploits. Further, states need to have more pointed discussions about the dangers of automation, digital manipulation, and predelegation. Our research demonstrated the lack of shared norms around digital safety and the dangers of cyber overconfidence; states will need to build shared understandings about these accident and inadvertent-escalation dangers, both in digital modernization and in cyber attacks. Finally, so much of the focus on cyber operations and nuclear stability has been on rational impetuses for preemption, but this research shows how subrational decision making and biases can distort beliefs about crises. This is where cyber is most dangerous, and decision makers should be wary of how cyber threats and capabilities might lead to unexpected pathways for nuclear use.

Data Availability Statement

Replication files for this article may be found at <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/KHXMM6>.

112. Schneider 2018.

Supplementary Material

Supplementary material for this article is available at <https://doi.org/10.1017/S0020818323000115>.

References

Acton, James. 2013. Reclaiming Strategic Stability. In *Strategic Stability: Contending Interpretations*, edited by Elbridge A. Colby and Michael S. Gerson, 117–46. US Army War College Press.

Acton, James. 2020. Cyber Warfare and Inadvertent Escalation. *Daedalus* 149 (2):133–49.

Altman, Daniel. 2015. The Strategist's Curse: A Theory of False Optimism as a Cause of War. *Security Studies* 24 (2):284–315.

Bas, Muhammet, and Robert Schub. 2016. How Uncertainty About War Outcomes Affects War Onset. *Journal of Conflict Resolution* 60 (6):1099–128.

Blainey, Geoffrey. 1988. *The Causes of War*. Free Press.

Blair, Bruce G. 1984. *Strategic Command and Control: Redefining the Nuclear Threat*. Brookings Institution.

Blair, Bruce G. 2011. *The Logic of Accidental Nuclear War*. Brookings Institution Press.

Booth, Ken, and Nicholas Wheeler. 2008. *The Security Dilemma: Fear, Cooperation, and Trust in World Politics*. Palgrave Macmillan.

Borghard, Erica, and Shawn Lonergan. 2017. The Logic of Coercion in Cyberspace. *Security Studies* 26 (3):452–81.

Borghard, Erica, and Shawn Lonergan. 2019. Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly* 13 (3):122–45

Bowers, Ian, and Henrik Stålhane Hiim. 2021. Conventional Counterforce Dilemmas: South Korea's Deterrence Strategy and Stability on the Korean Peninsula. *International Security* 45 (3):7–39.

Bracken, Paul. 1983. *The Command and Control of Nuclear Forces*. Yale University Press.

Bracken, Paul. 2016. The Cyber Threat to Nuclear Stability. *Orbis* 60 (2):188–203

Brewer, Gary, and Paul Bracken. 1984. Some Missing Pieces of the C3I Puzzle. *Journal of Conflict Resolution* 28 (3):451–69.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Buchanan, Ben, and Fiona S. Cunningham. 2020. Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis. *Texas National Security Review* 3 (4):54–81.

Carter, Ashton, John Steinbruner, and Charles A. Zraket. 1987. *Managing Nuclear Operations*. Brookings Institution Press.

Cimbala, Stephen. 1999. Accidental/Inadvertent Nuclear War and Information Warfare. *Armed Forces and Society* 25 (4):661–75.

Cimbala, Stephen. 2017. Nuclear Deterrence and Cyber Warfare: Coexistence or Competition? *Defense and Security Analysis* 33 (3):193–208.

Clary, Christopher, and Vipin Narang. 2019. India's Counterforce Temptations: Strategic Dilemmas, Doctrine, and Capabilities. *International Security* 43 (3):7–52.

Copeland, Dale. 2000. *The Origins of Major War*. Cornell University Press.

Cox, Jessica, and Heather Williams. 2021. The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability. *Washington Quarterly* 44 (1):69–85.

Cunningham, Fiona S., and M. Taylor Fravel. 2015. Assuring Assured Retaliation: China's Nuclear Posture and US–China Strategic Stability. *International Security* 40 (2):7–50.

Debs, Alexander, and Nuno P. Monteiro. 2014. Known Unknowns: Power Shifts, Uncertainty, and War. *International Organization* 68 (1):1–31.

Department of Defense. 1966. Final Report of NU I and II-66, Two Interagency Politico-Military Games Played by Officials of the Executive Branch during 1/11–2/8/66. Doc. no. GALE|CK2349234646, US Washington, DC: *Declassified Documents Online*, 28 February.
Department of Defense. 2018a. Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
Department of Defense. 2018b. Nuclear Posture Review, <https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx>.
Deptula, David, William La Plante, and Robert Haddick. 2019. *Modernizing US Nuclear Command Control and Communications*. Mitchell Institute for Aerospace Studies.
Fearon, James. 1995. Rationalist Explanations for War. *International Organization* 49 (3):379–414.
Friedman, Jeffrey. 2019. *War and Chance: Assessing Uncertainty in International Politics*. Oxford University Press.
Futter, Andrew. 2016. War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control. *European Security* 25 (2):163–80.
Futter, Andrew. 2018. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press.
Gartzke, Erik. 2013. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security* 38 (2):41–73.
Gartzke, Erik, and Jon R. Lindsay. 2017. Thermonuclear Cyberwar. *Journal of Cybersecurity* 3 (1):37–48.
Glaser, Charles. 1997. The Security Dilemma Revisited. *World Politics* 50 (1):171–201.
Glaser, Charles. 2000. The Causes and Consequences of Arms Races. *Annual Review of Political Science* 3 (1):251–76.
Glaser, Charles, and Chaim Kaufmann. 1998. What Is the Offense-Defense Balance and Can We Measure It? *International Security* 22 (4):44–82.
Gomez, Miguel Alberto, and Christopher Whyte. 2021. Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly* 65 (4):1137–50.
Gompert, David C., and Martin Libicki. 2014. Cyber Warfare and Sino-American Crisis Instability. *Survival* 56 (4):7–22.
Gompert, David C., and Martin Libicki. 2015. Waging Cyber War the American Way. *Survival* 57 (4):7–28.
Gompert, David C., and Martin Libicki. 2019. Cyber War and Nuclear Peace. *Survival* 61 (4):45–62.
Gottemoeller, Rose. 2021. The Standstill Conundrum: The Advent of Second-Strike Vulnerability and Options to Address It. *Texas National Security Review* 4 (4):115–24.
Government Accountability Office. 2017. Nuclear Command, Control, and Communications: Update on Air Force Oversight Effort and Selected Acquisition Programs, <https://www.gao.gov/products/GAO-17-641R>.
Haney, Patrick J. 2002. *Organizing for Foreign Policy Crises: Presidents, Advisers, and the Management of Decision Making*. University of Michigan Press.
Healey, Jason, and Robert Jervis. 2020. The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review* 3 (4):30–53.
Herrmann, Richard K., and Michael P. Fischerkeller. 1995. Beyond the Enemy Image and Spiral Model: Cognitive–Strategic Research after the Cold War. *International Organization* 49 (3):415–50.
House Armed Services Committee, 115th Congress. 2017. Military Assessment of Nuclear Deterrence Requirements, <https://armedservices.house.gov/legislation/hearings/military-assessment-nuclear-deterrence-requirements>.
Hyten, John E. 2017. An Interview with Gen John E. Hyten, Commander, USSTRATCOM, Conducted 27 July 2017. *Strategic Studies Quarterly* 11 (3):3–9.
Jensen, Benjamin, and Brandon Valeriano. 2019. *Cyber Escalation Dynamics: Results from War Game Experiments*. Presented at the annual International Studies Association conference.
Jervis, Robert. 1976. *Perception and Misperception in International Politics*. Princeton University Press.
Jervis, Robert. 1978. Cooperation Under the Security Dilemma. *World Politics* 30 (2):167–214.
Jervis, Robert, Richard Ned Lebow, and Janice Gross Stein. 1989. *Psychology and Deterrence*. Johns Hopkins University Press.

Johnson, Dominic D.P. 2004. *Overconfidence and War: The Havoc and Glory of Positive Illusions*. Harvard University Press.
Johnson, Dominic D.P., Rose McDermott, Emily S. Barrett, Jonathan Cowden, Richard Wrangham, Matthew H. McIntyre, and Stephen Peter Rosen. 2006. Overconfidence in Wargames: Experimental Evidence on Expectations, Aggression, Gender and Testosterone. *Proceedings of the Royal Society B: Biological Sciences* 273 (1600):2513–20.
Johnson, Dominic D.P., and Dominic Tierney. 2011. The Rubicon Theory of War: How the Path to Conflict Reaches the Point of No Return. *International Security* 36 (1):7–40.
Johnson, James 2020. Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Quarterly* 14 (1):16–39.
Kaminska, Monica. 2021. Restraint Under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks. *Journal of Cybersecurity* 7 (1):tyab008.
Kaplan, Fred. 2016. "WarGames" and Cybersecurity's Debt to a Hollywood Hack. *New York Times*, 19 February.
Klare, Michael T. 2019. Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. *Arms Control Today* 49 (9):6–13.
Kostyuk, Nadiya, and Carly Wayne. 2020. The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies* 6 (2), <https://doi.org/10.1093/jogss/ogz077>.
Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. Invisible Digital Front: Can Cyber-Attacks Shape Battlefield Events? *Journal of Conflict Resolution* 63 (2):317–47.
Kreps, Sarah, and Jacquelyn Schneider. 2019. Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics. *Journal of Cybersecurity* 5 (1):tyz007.
Kroenig, Matthew. 2021. Will Emerging Technology Cause Nuclear War? *Strategic Studies Quarterly* 15 (4):59–73.
Lawson, Sean T. 2019. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge.
Lebow, Richard Ned. 2020. Cognitive Closure and Crisis Politics. In *Between Peace and War*, edited by Richard Ned Lebow, 127–87. Palgrave Macmillan.
Levite, Ariel, George Perkovich, Lyu Jinghua, Lu Chuanying, Li Bin, Fan Yang, and Xu Manshu. 2021. China–US Cyber-Nuclear C3 Stability. Carnegie Endowment for International Peace, 8 April, <https://carnegieendowment.org/2021/04/08/china-u.s.-cyber-nuclear-c3-stability-pub-84182>.
Lieber, Keir. 2008. *War and the Engineers: The Primacy of Politics over Technology*. Cornell University Press.
Lieber, Keir, and Daryl G. Press. 2017. The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *International Security* 41 (4):9–49.
Lin, Herbert. 2021. Cyber Risk Across the US: Nuclear Enterprise. *Texas National Security Review* 4:108–20.
Lin-Greenberg, Erik, Reid Pauly, and Jacquelyn Schneider. 2022. Wargaming for International Relations. *European Journal of International Relations* 28 (1), <https://doi.org/10.1177/13540661211064090>.
Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22 (3):365–404.
Lindsay, Jon. 2019. Cyber Operations and Nuclear Weapons. Tech4GS Special Report, <https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons>.
Lindsay, Jon. 2020. Digital Strangelove: The Cyber Dangers of Nuclear Weapons. *Lawfare* [blog], 12 March, <https://www.lawfareblog.com/digital-strangelove-cyber-dangers-nuclear-weapons>.
Long, Austin, and Brendan Rittenhouse Green. 2015. Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy. *Journal of Strategic Studies* 38 (1-2):38–73.
Macdonald, Julia, and Jacquelyn Schneider. 2017. Presidential Risk Orientation and Force Employment Decisions: The Case of Unmanned Weaponry. *Journal of Conflict Resolution* 61 (3):511–36.
McDermott, Rose, Jonathan Cowden, and Cheryl Koopman. 2002. Framing, Uncertainty, and Hostile Communications in a Crisis Experiment. *Political Psychology* 23 (1):133–49.
Mearsheimer, John. 2001. *The Tragedy of Great Power Politics*. W.W. Norton.
Mercer, Jonathan. 2005. Rationality and Psychology in World Politics. *International Organization* 59 (1):77–106.

Mitzen, Jennifer, and Randall L. Schweller. 2011. Knowing the Unknown Unknowns: Misplaced Certainty and the Onset of War. *Security Studies* 20 (1):2–35.
Nitze, Paul H. 1976. Assuring Strategic Stability in an Era of Détente. *Foreign Affairs* 54 (2):207–32.
Nye, Joseph S., Jr. 2017. Deterrence and Dissuasion in Cyberspace. *International Security* 41 (3):44–71.
Pauly, Reid. 2018. Would US Leaders Push the Button? Wargames and the Sources of Nuclear Restraint. *International Security* 43 (2):151–92.
Posen, Barry R. 1982. Inadvertent Nuclear War? Escalation and NATO's Northern Flank. *International Security* 7 (2):28–54.
Powell, Robert. 2002. Bargaining Theory and International Conflict. *Annual Review of Political Science* 5: 1–30.
Quester, George H. 2002. *Offense and Defense in the International System*. Transaction.
Rathbun, Brian C. 2007. Uncertain About Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in International Relations Theory. *International Studies Quarterly* 51 (3):533–57.
Redd, Steven B. 2002. The Influence of Advisers on Foreign Policy Decision Making: An Experimental Study. *Journal of Conflict Resolution* 46 (3):335–64.
Reddie, Andrew W., Bethany L. Goldblum, Kiran Lakkaraju, Jason Reinhardt, Michael Nacht, and Laura Epifanovskaya. 2018. Next-Generation Wargames. *Science* 362 (6421):1362–64.
Reiter, Dan. 2003. Exploring the Bargaining Model of War. *Perspectives on Politics* 1 (1):27–43.
Richardson, Lewis. 1960. *Arms and Insecurity*. Boxwood Press.
Rosati, Jerel A. 2000. The Power of Human Cognition in the Study of World Politics. *International Studies Review* 2 (3):45–75.
Sagan, Scott D. 1985. Nuclear Alerts and Crisis Management. *International Security* 9 (4):99–139.
Sagan, Scott D. 1997. Proliferation Pessimism and Emerging Nuclear Powers. *International Security* 22 (2):193–202.
Sagan, Scott D., and Jeremi Suri. 2003. The Madman Nuclear Alert: Secrecy, Signaling, and Safety in October 1969. *International Security* 27 (4):150–83.
Schechter, Benjamin, Jacquelyn Schneider, and Rachael Shaffer. 2021. Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming. *Simulation and Gaming* 52 (4), <https://doi.org/10.1177/1046878120987581>.
Schelling, Thomas C. 1980. *The Strategy of Conflict*. Harvard University Press.
Schneider, Jacquelyn. 2017. Cyber-Attacks on Critical Infrastructure: Insights from Wargaming. *War on the Rocks*, 26 July, <https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/>.
Schneider, Jacquelyn. 2018. JEDI: Outlook for Stability Uncertain as Pentagon Migrates to the Cloud. *Bulletin of Atomic Scientists*, 21 June, <https://thebulletin.org/2018/06/jedi-outlook-for-stability-uncertain-as-pentagon-migrates-to-the-cloud/>.
Schneider, Jacquelyn. 2022. Testimony for the US China Commission, <https://www.uscc.gov/sites/default/files/2022-02/Jacquelyn_Schneider_Testimony.pdf>.
Schneider, Jacquelyn, Benjamin Schechter, and Rachael Shaffer. 2022. A Lot of Cyber Fizzle But Not a Lot of Bang: Evidence About the Use of Cyber Operations from Wargames. *Journal of Global Security Studies* 7 (2):ogac005.
Sherwood-Randall, Elizabeth. 2020. The Age of Strategic Instability: How Novel Technologies Disrupt the Nuclear Balance. *Foreign Affairs*, 21 July.
Slayton, Rebecca. 2017. What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security* 41 (3):72–109.
Snyder, Jack. 1989. *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914*. Cornell University Press.
Stoutland, Page, and Samantha Pitts-Kiefer. 2018. *Nuclear Weapons in the New Cyber Age*. Nuclear Threat Initiative.
Taliaferro, Jeffrey. 2001. Realism, Power Shifts, and Major War. *Security Studies* 10(4):145–78.
Talmadge, Caitlin. 2017. Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States. *International Security* 41 (4):50–92.

Talmadge, Caitlin. 2019. Emerging Technology and Intra-war Escalation Risks: Evidence from the Cold War, Implications for Today. *Journal of Strategic Studies* 42 (6):854–87.
Tannenwald, Nina. 2007. *The Nuclear Taboo: The United States and the Non-use of Nuclear Weapons Since 1945*. Cambridge University Press.
Unal, Beyza, and Patricial Lewis. 2018. *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences*. Chatham House.
Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.
Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.
Van Evera, Stephen. 1998. Offense, Defense, and the Causes of War. *International Security* 22 (4):5–43.
Waltz, Kenneth N. 1959. *Man, the State, and War*. Waveland Press.
Wan, Wilfred, Andraz Kastelic, and Eleanor Krabill. 2021. The Cyber-Nuclear Nexus: Interactions and Risks. UNIDIR, <https://www.unidir.org/publication/cyber-nuclear-nexus-interactions-and-risks>.

Authors

Jacquelyn Schneider is a Hoover Fellow and Director of the Wargaming and Crisis Simulation Initiative at the Hoover Institution, Stanford University, CA. She can be reached at Jacquelyn.schneider@stanford.edu.
Benjamin Schechter is a Senior Military Operations Analyst at Systems Planning and Analysis Inc. and a nonresident Research Fellow at the Cyber and Innovation Policy Institute at the US Naval War College in Newport, RI. He can be reached at Bhschecter@gmail.com.
Rachael Shaffer is a contract researcher for the Strategic and Operational Research Department at the US Naval War College in Newport, RI. She can be reached at rachaelmshaffer@gmail.com.

Acknowledgments

We thank the Naval War College, Hoover Institution, Naval Postgraduate School, Tufts University, Georgetown University, Harvard Belfer Center, Sandia National Laboratories, and CSIS for contributing time and participants for this research. We also thank the anonymous reviewers, Erik Lin-Greenberg, Reid Pauly, Peter Dombrowski, Andrew Winner, Andrew Reddie, and members of MIT SSP, Stanford CISAC, and the Middlebury Institute for helpful comments on earlier drafts. Portions of this research were approved under protocol 53626 by Stanford University's Institutional Review Board.

Key Words

Nuclear stability; cyber; wargames; escalation; emerging technology; uncertainty; overconfidence

Date received: March 24, 2022; Date accepted: April 24, 2023