Cyber Operations and Nuclear Stability: Networked Instability?

Jacquelyn Schneider

Texas National Security Review 9, no. 2 (Spring 2026) | © 2026 by Jacquelyn Schneider | DOI: 10.1353/tns.00033

The digital transformation of nuclear forces made modern nuclear forces more effective but potentially introduced strategic cyber vulnerabilities. Despite warnings about the cyber threats to nuclear stability, our understandings of when and why cyber operations create nuclear instability are rife with contradictory suppositions. Does entanglement create interdependence that stabilizes crisis dyads, or destabilizing pathways to inadvertent nuclear war? Do uncertainties about cyber vulnerabilities within nuclear command, control, and communications lead to a security dilemma that incentivizes preemptive nuclear use? Or does the uncertainty about how cyber operations create effects and vulnerabilities create incentives for restraint? This paper argues that current literature overlooks a foundational element of cyber and strategic stability: how the structure of networks determines the feasibility and effectiveness of cyber operations. By shifting the focus toward the intersection of network architecture and nuclear use, this piece argues that highly centralized information-processing or command nodes, which increase a network's efficiency, can create incentives for deliberate nuclear escalation. Second, entanglement and network complexity increase the potential for inadvertent escalation or accidental nuclear use. Third, cyberattacks that exploit trust in data to degrade decision-making are the most dangerous for escalation risk.

Over the last half-century, nuclear forces have embarked on a digital transformation. The advent of the microprocessor has made nuclear weapons more precise and controllable, new sensors have turned launch warnings into a big data challenge, and digital networks have shifted the flow of information from space to ground into a matter of milliseconds.[1] In the past, command, control, weapons guidance, and intelligence warnings existed on floppy disks and analog processors; in today's world, nuclear inventories are equipped with precision guidance, networked intelligence and surveillance, and control by digital code. The United States led these efforts, embarking on a revolutionary digital modernization of its nuclear arsenal, command, and control—investing billions to transform US nuclear capability.[2]

But even as nations have invested in digital technologies for nuclear weapons, they have also developed cyber capabilities to attack these technologies, turning digital modernization from a capability into a vulnerability. In fact, it was the potential vulnerability of nuclear command and control in the fictional movie *Wargames* that led President Ronald Reagan to initiate the first cyber vulnerability study within the US Department of Defense.[3] Despite Reagan's

1 Donald A. MacKenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (MIT Press, 1993).

2 Jake Hecla, Rebecca Krentz-We, and Andrew Reddie, "The Next Generation NC3 Enterprise: Opportunities and Challenges," *Journal of Science Policy and Governance* 14, no. 2 (2019); David Deptula, William LaPlante, and Robert Haddick, *Modernizing US Nuclear Command, Control, and Communications* (Mitchell Institute for Aerospace Studies, 2019); Jeffrey Larsen, "Nuclear Command, Control, and Communications: US Country Profile," NAPSNet Special Reports, August 22, 2019, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-control-and-communications-us-country-profile/.

3 Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (Simon and Schuster, 2016).

recognition of cyber threat thirty years ago, the cyber threat to US nuclear capabilities has not been resolved. Instead, cyber capabilities have proliferated and become more normalized within countries' military and foreign power arsenal—from attacks on nuclear development facilities,[4] to electric grids,[5] and even to cyberattacks on cutting-edge weapons technology.[6] Meanwhile, analyses of cyber operations' threat to nuclear stability warn that not only are nuclear powers' capabilities hackable, but also the potential for these hacks could cause dangerous instability.[7] As Stoutland and Pitts-Kiefer warn: "Cyber threats to nuclear weapons systems increase the risk of use as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and could undermine confidence in the nuclear deterrent, affecting strategic stability."[8]

Despite warnings about the cyber threat to nuclear stability, our understandings of when and why cyber operations create nuclear instability are inchoate at best and misguided at worst. Far too much of the literature on cyber operations and nuclear instability is based on unfounded hypotheses about both the extent of cyber capabilities and how nuclear decision-makers might respond to these threats. This speculation leaves a burgeoning literature on cyberspace and nuclear stability that is rife with contradictory suppositions. For instance, does entanglement create interdependence that stabilizes crisis dyads,[9] or does entanglement create destabilizing pathways to inadvertent nuclear war?[10] Do uncertainties about cyber vulnerabilities within nuclear command, control, and communications (NC3) lead to a security dilemma that incentivizes preemptive nuclear use?[11] Or does the uncertainty about how cyber operations create effects and vulnerabilities actually make it a stabilizing force?[12]

What most of the work on cyberspace and nuclear stability has overlooked—despite the growth of digitally dependent and networked nuclear forces—is how the structure of networks impacts the technical feasibility of cyber operations and, ultimately, their effect on nuclear use. This omission is remarkable—especially given that modern military campaigns and nuclear strategies are explicitly tied to information networks. It is even more remarkable because the way a network is built—how centralized or decentralized, what dependencies exist, its complexity versus simplicity, its entanglement with conventional or civilian resources, and how, ultimately, it degrades—explains the probability of achieving a cyber access for attackers, as well as the potential scope of the effects of cyber exploitation.

Despite warnings about the cyber threat to nuclear stability, our understandings of when and why cyber operations create nuclear instability are inchoate at best and misguided at worst.

This article introduces novel arguments about cyber operations and nuclear stability, focusing on how network characteristics explain what types of cyberattacks are more likely to create destabilizing effects. I find, first, that highly centralized information-processing or command nodes, which increase a network's efficiency,

4 Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

5 Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction," *Wired*, September 12, 2019, https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

6 Sue Halpern, "How Cyber Weapons Are Changing the Landscape of Modern Warfare," *The New Yorker*, July 18, 2019, https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

7 Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* (Chatham House, 2018); Bruce G. Blair, "Why Our Nuclear Weapons Can Be Hacked," *The New York Times*, March 14, 2017; David C. Gompert and Martin Libicki, "Cyber War and Nuclear Peace," *Survival* 61 no. 4 (2019): 45–62, https://www.tandfonline.com/doi/full/10.1080/00396338.2019.1637122; Page Stoutland and Samantha Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age," *Nuclear Threat Initiative*, 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf; Geoffrey Ingersoll, "Defense Science Board Warns of 'Existential Cyber Attack,'" *Business Insider*, March 6, 2013, https://www.businessinsider.com/cyber-exploits-turn-weapons-on-us-2013-3.

8 Stoutland and Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age."

9 Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (2015): 7–47.

10 James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018): 56–99; James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (2020): 133–49.

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

12 Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81; Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation," *International Organization* 77, no. 3 (2023): 633–67.

can create incentives for deliberate nuclear escalation. Second, entanglement and network complexity increase the potential for inadvertent escalation or accidental nuclear use. Third, cyberattacks that exploit trust in data to degrade decision-making are the most dangerous for escalation risk.

The exploration begins with an introduction to three pathways toward instability: deliberate escalation, inadvertent escalation, and accidental use. Second, I examine the expected effect of cyber operations on each. Third, I introduce network structures and the characteristics that differentiate networks from one another, which I use to explore hypotheses about how different networks create destabilizing or stabilizing effects on nuclear dynamics. I examine these hypotheses with respect to the parts of a nuclear system: (1) intelligence, surveillance, and reconnaissance; (2) weapons platforms; and (3) command and control. Finally, I conclude with implications for nuclear stability and policy recommendations to decrease the threat of cyber operations to nuclear stability.

Nuclear Stability—Deliberate Escalation, Inadvertent Escalation, and Accidental Use

While stability as a concept—the idea that a state of existence is more or less likely to change—has played a prominent role in crisis literature,[13] nuclear literature is more likely to discuss escalation, accidents, or even proliferation. Nuclear stability is best understood as whether the chance of nuclear use is more or less likely to occur. There are multiple pathways by which cyber operation might undermine nuclear stability: deliberate escalation, inadvertent escalation, and accidents.

Deliberate escalation,[14] or the use of nuclear weapons "carried out for instrumental reasons," occurs when "a combatant deliberately increases the intensity or scope of an operation to gain advantage or avoid defeat."[15] States may choose to deliberately use nuclear weapons for a variety of reasons, most notably to coerce states (either to de-escalate or to create a new bargaining solution) or to preemptively win in a nuclear conflict. Perhaps the most straightforward explanation for deliberate use is that states believe they need to use nuclear weapons to win a conventional war in which they are asymmetrically disadvantaged.[16] This view was, for example, the dominant US strategy throughout much of the Cold War, when estimates for conventional warfare in Europe suggested that, without US nuclear use, the Soviets would quickly overrun NATO forces.[17] Deliberate use of nuclear weapons may also occur as an act of coercion when a decision-maker believes that the use of nuclear weapons signals resolve that then either coerces adversary states to change course on a previous foreign policy decision or deters them from subsequent escalation. The key factor in deliberate escalation to nuclear use—as opposed to inadvertent escalation (discussed below)—is that the use of nuclear weapons is a deliberate part of the state's strategy, not an outcome resorted to because of the unforeseen repercussions of an otherwise conventional strategy.

Inadvertent escalation,[18] in contrast, is the use of nuclear weapons "arising out of the normal conduct of intense conventional conflict. . . . It is neither a purposeful act of policy nor an accident. . . . [It] is rather the unintended consequence of a decision to fight a conventional war."[19] Inadvertent nuclear use is most likely to occur when states misperceive conventional attacks as precursors for a nuclear

13 Robert Jervis, "Arms Control, Stability, and Causes of War," *Political Science Quarterly* 108, no. 2 (1993): 239–53; Robert Powell, "Crisis Stability in the Nuclear Age," *American Political Science Review* 83, no. 1 (1989): 61–76; Steven J. Brams and D. Marc Kilgour, "Threat Escalation and Crisis Stability: A Game-Theoretic Analysis," *American Political Science Review* 81, no. 3 (1987): 833–50; Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War," *Journal of Strategic Studies* 42, no. 6 (2019): 727–35.

14 Keir A. Lieber and Daryl G. Press, "Coercive Nuclear Campaigns in the 21st Century: Understanding Adversary Incentives and Options for Nuclear Escalation," PASCC, Naval Postgraduate School, report number 2013–001, March 2013, https://apps.dtic.mil/sti/pdfs/ADA585975.pdf; Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton University Press, 2014); Herman Kahn, *On Escalation: Metaphors and Scenarios*, vol. 1 (Transaction Publishers, 2009); Karl P. Mueller, Jasen J. Castillo, Forrest E. Morgan, Negeen Pegahi, and Brian Rosen, *Striking First: Preemptive and Preventive Attack in US National Security Policy* (RAND Corporation, 2006); Robert Jervis, "Why Nuclear Superiority Doesn't Matter," *Political Science Quarterly* 94, no. 4 (Winter 1979/80): 628–29.

15 Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (RAND Corporation, 2008), xii.

16 Tyler Bowen, "Threading the Needle: The Logic of Conventional Coercion in Nuclear Crises," *Texas National Security Review* 9, no. 1 (2025): 28–51.

17 Consider also the reverse: Russia's contemporary incentives to use nuclear weapons. See Kristen Ven Bruusgaard, "Russian Nuclear Strategy and Conventional Inferiority," *Journal of Strategic Studies* 44, no. 1 (2021): 3–35.

18 Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Cornell University Press, 1991); Anthony M. Barrett, Seth D. Baum, and Kelly Hostetler, "Analyzing and Reducing the Risks of Inadvertent Nuclear War Between the United States and Russia," *Science & Global Security* 21, no. 2 (2013): 106–33; Barry Nalebuff, "Brinkmanship and Nuclear Deterrence: The Neutrality of Escalation," *Conflict Management and Peace Science* 9, no. 2 (1986): 19–30.

19 Barry R. Posen, "Inadvertent Nuclear War? Escalation and NATO's Northern Flank," *International Security* 7, no. 2 (1982): 29–30.

counterforce attack or when a conventional counterforce attack threatens a nuclear strike capability. Caitlin Talmadge points to factors—like dual-capable weapons and intermingled command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)—that increase the risk of inadvertent escalation between the US and China.[20] Relatedly, nuclear security expert James Acton argues that the entanglement of conventional and nuclear networks increases the chance that states misperceive conventional attacks as threats or intention to undermine an adversary's nuclear capability.[21] Inadvertent escalation is therefore almost always tied to misperceptions within conventional conflict, which are intimately related to uncertainties created by weapons, command structures, and doctrines that make it difficult to differentiate between nuclear and conventional forces.

Most analyses on cyber operations and nuclear stability conclude that cyber operations make nuclear use more likely.

Finally, a third pathway to nuclear instability involves accidents[22] or unintentional uses of nuclear weapons. For example, work by political scientist Scott Sagan examines how pre-delegation of nuclear command, alert status, organizational interests, and baseline safety considerations may make states more or less likely to accidentally use nuclear weapons.[23] Unlike the other two pathways to nuclear use, which involve intentional (if not always deliberate) decisions to use nuclear weapons, accidental use occurs when states have not made a choice to use nuclear weapons. Instead, perhaps because of a misunderstood order or a failed safety mechanism, nuclear use occurs unintentionally. Pathways to accidental use can almost always be traced to organizational decisions that maximize risk, perhaps due to organizational cultures or increased tensions between nations.

Cyber Operations and Nuclear Stability: State of the Literature

Existing literature on cyber operations and nuclear stability can generally be divided into two sets of arguments: one rooted in theories of nuclear stability, and the other in the empirical precedents of cyber and crisis stability. In the first camp, scholars argue that cyber operations create incentives for nuclear instability—either because they create windows of preemption for deliberate escalation (as entanglement increases incentives for inadvertent escalation), or because cyber operations increase the chance of accidental use. A second camp, which focuses on cyber and crisis stability, argues that cyber operations can create stabilizing incentives, the logic of which might be extended into the nuclear realm. These scholars examine empirical precedents of cyber use and find little evidence for escalation from cyber operations. They point to the increased bargaining space created by cyber operations, the lack of emotional reaction to cyberattacks, and the interdependence of civilian and military cyber resources as factors that generate restraint.

Most analyses on cyber operations and nuclear stability conclude that cyber operations make nuclear use *more* likely. The potential pathways to nuclear use, however, vary across these accounts. For some scholars, cyber operations incentivize nuclear use because they create windows of preemption or vulnerability that induce deliberate escalation.[24] According to this logic, states may grow so alarmed by the vulnerability of their NC3 that they no longer trust their second-strike capability

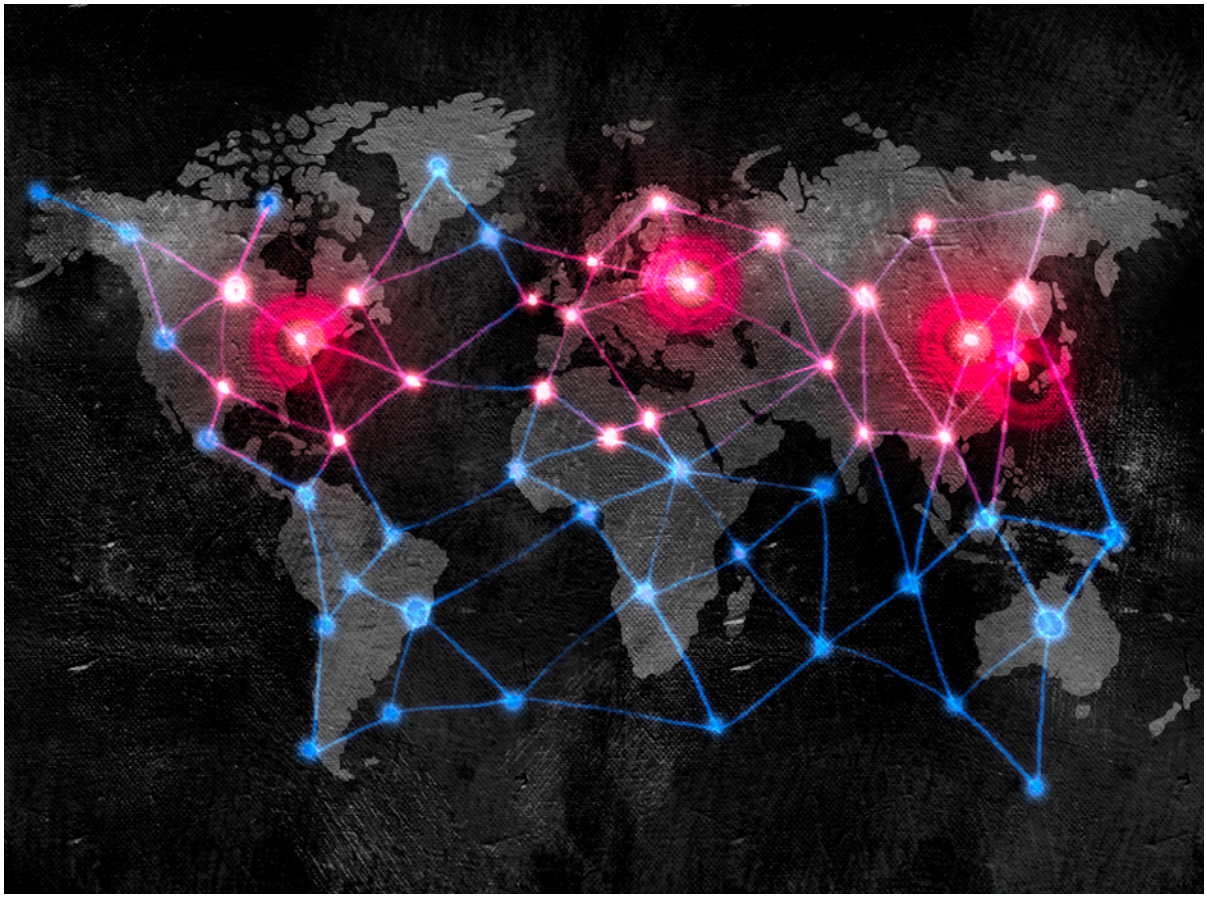
20 Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (2017): 50–92.

21 James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018): 56–99.

22 Bruce G. Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Brookings Institution Press, 1989); Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton University Press, 1995); Peter D. Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Cornell University Press, 1992).

23 Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton University Press, 1995); Scott D. Sagan, "Nuclear Alerts and Crisis Management," *International Security* 9, no. 4 (1985): 99–139; Richard N. Lebow, *Nuclear Crisis Management: A Dangerous Illusion* (Cornell University Press, 2019); Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton University Press, 1990); Scott D. Sagan, "The Perils of Proliferation: Organization Theory, Deterrence Theory, and the Spread of Nuclear Weapons," *International Security* 18, no. 4 (1994): 66–107.

24 Greg Austin and Pavel Sharikov, "Pre-Emption Is Victory: Aggravated Nuclear Instability of the Information Age," *The Nonproliferation Review* 23, nos. 5–6 (2016): 691–704, https://doi.org/10.1080/10736700.2017.1346834; Bruce G. Blair, "Why Our Nuclear Weapons Can Be Hacked," *The New York Times,* March 14, 2017; David C. Gompert and Martin Libicki, "Cyber War and Nuclear Peace," *Survival* 61, no. 4 (2019): 45–62, https://doi.org/10.1080/00396338.2019.1637122; Stephen J. Cimbala, "Nuclear Crisis Management and 'Cyberwar': Phishing for Trouble?," *Strategic Studies Quarterly* 5, no. 1 (2011): 117–31; Steve Fetter and Jaganath Sankaran, "Emerging Technologies and Challenges to Nuclear Stability," *Journal of Strategic Studies* 48, no. 2 (2025): 252–96; Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Georgetown University Press, 2018); Paul Bracken, "The Cyber Threat to Nuclear Stability," *Orbis* 60, no. 2 (2016): 188–203.



or their situational awareness to head off a limited nuclear attack, which leads them to launch preemptive nuclear strikes. This dynamic becomes even more dangerous when one side is already asymmetrically disadvantaged in either conventional or nuclear domains. A burgeoning nuclear state like North Korea, for example, would require only a small nudge about the vulnerability of commanding or controlling their nuclear forces to induce a preemptive use of nuclear weapons. Indeed, North Korea's 2022 nuclear law specifically threatens a preemptive nuclear war if a "fatal military attack against important strategic objects" is "judged to be on the horizon" or if it is necessary to take "the initiative in war."[25] Similar arguments within the cyber and crisis stability literature point to the offensive nature of cyberspace and the paradox of digital dependencies to identify escalation pressures from cyber operations.[26] Pathways to deliberate nuclear use are most likely when states have a strong belief that their ability to control nuclear forces is under threat and when significant nuclear asymmetries exist between states in a nuclear dyad.

Deliberate pathways from cyber operations to nuclear use are generally about creating certainty, whereas inadvertent pathways to nuclear use are about the effects of uncertainty on inducements for nuclear use. Many of the pessimistic arguments focus on inadvertent pathways—whether because of the entanglement of conventional and nuclear forces, false warnings, or manipulation of data.[27] These arguments suggest, for example, that cyber operations could cause inadvertent nuclear use because they increase the fog of war about states'

25 "Law on DPRKs Policy on Nuclear Forces Promulgated," *KCNA*, September 8, 2022, https://kcnawatch.org/newstream/1662687258-950776986/law-on-dprks-policy-on-nuclear-forces-promulgated/.

26 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press, 2016); David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* 56, no. 4 (2014): 7–22; Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," *Journal of Strategic Studies* 42, no. 6 (2019): 841–63.

27 Stephen J. Cimbala, "Accidental/Inadvertent Nuclear War and Information Warfare," *Armed Forces & Society* 25, no. 4 (Summer 1999): 653–75; Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* (Chatham House, 2018); Erik Gartzke and Jon Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017): 37–48; Jon R. Lindsay, "Cyber Operations and Nuclear Weapons," *Tech4GS Special Reports*, June 20, 2019, https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-global-overview.html; Stoutland and Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age*.

intentions and willingness to escalate. Acton argues that nuclear-conventional entanglement "could lead to escalation because both sides in a US-Chinese or US-Russian conflict could have strong incentives to attack the adversary's dual-use C3I [command, control, communications, and information] capabilities to undermine its nonnuclear operations. As a result, over the course of a conventional war, the nuclear C3I systems of one or both of the belligerents could become severely degraded. It is, therefore, not just US nonnuclear strikes against China or Russia that could prove escalatory; Chinese or Russian strikes against American C3I assets could also—a possibility that scholars have scarcely considered since the end of the Cold War."[28] While deliberate escalation is most likely to occur when cyber operations affect control, inadvertent escalation is most likely when attacks degrade situational awareness.

At its most basic, network structure is simply the shape of relationships (edges or links) between nodes (vertices).

Finally, cyber operations may lead to nuclear use if they increase the chance of accidents. Cyber operations that affect the targeting or communications capability of nuclear weapons increase the chance of accidental nuclear use. This type of use is more likely to occur when states are at high alert and have pre-delegated command, placed nuclear forces on alert, or paired nuclear weapons with their associated platforms. The threat of cyber operations could induce these kinds of high alert and inherently risky nuclear activities, thus creating more potential for accidents. As political scientist Stephen Cimbala describes the phenomenon of introducing cyber operations to nuclear stability: "The problem of valid warning and appropriate response is complicated by the tight coupling of sensors, assessment centers, and response systems. Certain high technology organizations are especially prone . . . to normal accidents."[29]

Despite the overwhelming literature presenting the destabilizing effects of cyber operations on nuclear use, literature on cyberspace and crisis stability is largely optimistic about the effect that cyber operations have on otherwise dangerous crises. Empirical work analyzing large-N cyber cases,[30] cyber operations within conventional wars,[31] cyber operations in war games,[32] and survey experiments on responses to cyber operations[33] all suggest that cyber operations do not correlate with more violent crises; rather, these operations can (in some cases) stabilize crises. Social scientists who specialize in cybersecurity offer a variety of rationales for this otherwise puzzling lack of reaction from cyber operations. Jon Lindsay notes the ephemeral physical effects of cyber operations like Stuxnet,[34] while Erik Gartzke similarly argues that this limited physical nature of most cyber effects relegates cyber operations to bit roles in nuclear stability politics.[35] This finding could be because, as Erica Borghard and Shawn Lonergan argue, the difficulties in creating and maintaining cyber exploits make cyber operations cumbersome tools for coercion.[36] Alternatively, as Sarah Kreps and I conclude, cyber operations may not create the same kind of emotional saliences as other, more overt forms of state power. [37] Or it could be, as both Lindsay and Joseph Nye suggest,

28 James Acton, "Escalation Through Entanglement," 58.

29 Stephen J. Cimbala, "Accidental/Inadvertent Nuclear War and Information Warfare," *Armed Forces & Society* 25, no. 4 (Summer 1999): 661.

30 Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015); Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018).

31 Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* 63, no. 2 (2019): 317–47.

32 Benjamin Jensen and Brandon Valeriano, "Cyber Escalation Dynamics: Results from War Game Experiments International Studies Association," *Annual Meeting Panel: War Gaming and Simulations in International Conflict, March 27, 2019* (2019); Jacquelyn Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict" (PhD diss., The George Washington University, 2017); Jacquelyn Schneider, "Cyber Attacks on Critical Infrastructure: Insights from Wargaming," *War on the Rocks*, July 26, 2017, https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/.

33 Nadiya Kostyuk and Carly Wayne, "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public," *Journal of Global Security Studies* (2020); Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019): tyz007.

34 Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

35 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73.

36 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81; Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45.

37 Kreps and Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains."

that cyber operations may actually create interdependencies between civilian and national security targets that incentivize restraint.[38]

Network Structure and Hypotheses

How can we reconcile these competing hypotheses? A missing intervening variable— network structure—may help explain these seeming contradictions. As Albert-László Barabási (one of the first network scientists) notes: "We cannot interpret a system's behavior without fully accounting for the structure of the network behind it."[39]

What is network structure? At its most basic, network structure is simply the shape of relationships (edges or links) between nodes (vertices). Each node is characterized by its degree, or the number of links it has to other nodes. Nodes with multiple degrees represent hubs. Sometimes hubs cluster together in components, linked by a bridge. At other times nodes are more evenly dispersed and multiple paths exist between nodes. The number of paths between nodes determine whether a network is dense or sparse, and the availability of pathways to move between these nodes is determined by "rules of the road" and whether lines are directed (one-way) or undirected (both ways).[40] Choices about nodes and paths lead to networks that are hierarchical or decentralized, robust or precarious, or controlled or diffuse.

According to percolation theory, networks with a high density of small nodes and multiple pathways are inherently resilient. For example, the internet, full of small nodes and multidirectional linkages, can withstand the random removal of an extraordinary amount of nodes before it decomposes and loses its ability to function.[41] In contrast, networks with larger nodes and limited pathways have much lower critical thresholds and will therefore degrade with far fewer node or pathway removals. That quality means that, for centralized networks characterized by limited pathways and large hubs, even isolated attacks can have devastating cascading effects to the network's integrity. In contrast, dense and small-node networks with multiple pathways between nodes are the most resilient to attack.

Centralized networks may be less resilient than their decentralized counterparts, but there are trade-offs that can make these types of networks appealing. Though centralized networks are more likely to degrade in catastrophic ways, they also offer more efficiency and control. Dense networks, like the internet, are designed for collaboration and diffusion. They are inherently resilient, but these network models are not necessarily ideal for the control of private information—like the command and control of nuclear weapons. Even networks that are both diffuse and controlled, like blockchain, often sacrifice efficiency and speed. In an ideal world, we would always build networks that are resilient, efficient, and controlled. These "perfect networks," however, are complex and often expensive to build and administer. There are, therefore, legitimate reasons why a state might choose a centralized and sparse nuclear network despite heightened vulnerability to outsider attacks.

These choices—about how networks privilege resiliency over efficiency, control, or cost—help explain when and why cyber threats impact nuclear stability. Applying network theory to arguments about escalation leads to a series of hypotheses about when and why cyber threats create incentives for nuclear use (see table 1).

Table 1. Network theory and nuclear use

	Large, sparse nodes with limited pathways	Small, dense nodes with multiple pathways
Entangled components	Highest chance of inadvertent nuclear use	Highest chance of accidental nuclear use
Separate components	Highest chance of deliberate nuclear use	Most resilient to cyberattack—but least efficient and most expensive

38 Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (2015): 7–47; Nye, "Deterrence and Dissuasion in Cyberspace," 44–71.

39 Albert-László Barabási and Marton Pósfai, *Network Science* (Cambridge University Press, 2016), 3.

40 Barabási and Pósfai, *Network Science*; Mark Newman, *Networks*, 2nd ed. (Oxford University Press, 2018).

41 Albert-László Barabási and Eric Bonabeau, "Scale-Free Networks," *Scientific American* 288, no. 5 (2003): 60–69; Albert-László Barabási, *Linked: The New Science of Networks* (Perseus Publishing, 2002), 409–10; Jeff Ash and David Newth, "Optimizing Complex Networks for Resilience Against Cascading Failure," *Physica A: Statistical Mechanics and Its Applications* 380 (2007): 673–83; Morton E. O'Kelly, "Network Hub Structure and Resilience," *Networks and Spatial Economics* 15, no. 2 (2015): 235–51; Prasanna Gai, Andrew Haldane, and Sujit Kapadia, "Complexity, Concentration and Contagion," *Journal of Monetary Economics* 58, no. 5 (2011): 453–70.

First, cyber operations are most likely to create incentives for deliberate escalation to nuclear use when nuclear networks are optimized for efficiency and control, featuring large, dense hubs and limited pathways between hubs. The more certain attackers are about the ability to create long-term, pervasive effects across a nuclear network, the more likely they are to deliberately escalate as part of a strategy to gain first-move advantage. Further, these incentives for deliberate escalation increase when states keep their nuclear and conventional networks separate, because attacking states are more certain about which network they are targeting.

In contrast, the more complicated and diffuse networks become, the less certain attacking states can be that a cyberattack on nuclear networks will cause significant or prolonged damage. This scenario decreases the incentives for deliberate escalation, but increases the chance of inadvertent or accidental nuclear use. That effect occurs because, whereas the pathway from cyber operations through networks to deliberate nuclear use is about certainty, pathways to inadvertent escalation and accidental use are a product of uncertainty. Networks create uncertainty about the effectiveness of cyberattacks by creating duplicative nodes, redundant pathways, and dual-direction linkages. These structures make attackers less certain about the scope of their attacks, but they may also make users of the network less certain about how vulnerable they are to attacks. Uncertainty about vulnerabilities can create either complacency or anxiety, which decreases the pressure for deliberative escalation, but may also leave users surprised by unintended or unexpected effects of cyberattacks.

This uncertainty, created by network structure, leads to two distinct dynamics. On one hand, uncertainty created by the entanglement of nuclear and conventional networks can lead to inadvertent escalation if entangled nodes, perhaps misperceived as part of conventional warfighting networks, are attacked in what a state might have thought to be a scoped cyberattack. The degradation of the node, on the other hand, could inadvertently pressure a vulnerable nuclear force to escalate in response or, in a worst case, cause accidental nuclear effects. As nodes become more prolific and networks denser, however, there is less chance that the entanglement creates a highly lucrative target during conventional warfare. And while this doesn't nullify the risk of inadvertent or accidental escalation, more diffuse and smaller node networks are less likely to suffer from catastrophic entanglement issues. Therefore, central hubs with entangled components are most likely to suffer from inadvertent nuclear use, while entangled but smaller and more prolific node networks are most likely to create the kinds of complexities that lead to accidental use. Entanglement, as a result, does not always create incentives for nuclear use—though it may increase complexity in an unintentional way.

Cyber Operations and Nuclear Networks

Understanding how these hypotheses apply to modern nuclear capabilities requires examining multiple components of a nuclear arsenal: (1) intelligence, surveillance, and reconnaissance capabilities, (2) nuclear weapons delivery platforms and warheads, and (3) command and control. Each of these components relies on different network structures with unique implications for cyberattacks and nuclear stability. Are these networks made up of large, sparse nodes with limited pathways or small, dense nodes with multiple pathways? Are they entangled with conventional capabilities? Finally, this section explores how cyber operations might create effects within these networks as well as how technically feasible it might be for cyber operations to exploit these vulnerabilities.

Intelligence, Surveillance, and Reconnaissance Networks

Nuclear stability is intimately tied to networks of intelligence, surveillance, and reconnaissance (ISR). Overhead satellites take images of fixed and mobile nuclear sites, generate signals intelligence (SIGINT) on weapons and communications, and provide tactical warning of launches.[42] Meanwhile, airborne platforms provide both long-distance imagery and SIGINT as well as submarine tracking, post-nuclear launch attribution operations, and real-time video capabilities. These suites of overhead and airborne platforms are complemented by ground-based SIGINT collection sites as well as underwater and surface sensors to monitor underwater activity. Finally, technical collection efforts are aided by human intelligence on nuclear decision-making, personnel movements, and special information about hidden technologies.[43]

In the past, tactical and strategic nuclear warning were relatively disconnected networks made up

42 "The SIGINT Satellite Story," National Reconnaissance Office, 1994, https://www.governmentattic.org/19docs/NRO-SIGINTsatStory_1994u.pdf; "Defense Support Program Satellites," https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/2197774/defense-support-program-satellites/; "SBIRS," https://www.lockheedmartin.com/en-us/products/sbirs.html.

43 Kenneth J. Hintz, *Sensor Management in ISR* (Artech House, 2020); Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, *Managing Nuclear Operations* (Brookings Institution Press, 1987); John A. Gentry and Joseph S. Gordon, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Georgetown University Press, 2019).

of scarce platforms. For most of the nuclear age, strategic missile-launch warning relied on a few scarce satellites.[44] The scarcity of these strategic assets also meant that the most valuable sensors rarely performed both a nuclear and a conventional warning mission. This was an inefficient, sparse, unentangled network. While the destruction of a few intelligence platforms in this network would have devastating consequences to nuclear warning (and therefore increased incentives for deliberate escalation), few components were entangled with conventional assets (and therefore posed less risk of inadvertent escalation or accidental targeting).[45]

With the digitization of technology, however, packets of digital information flow freely between sensors, collection sites, and command centers. Instead of nuclear warning being reliant on a few platforms linked together by vulnerable bridges and reporting back to one hub, the modern ISR network is diffuse, with many components and multiple, significantly larger nodes for processing and distribution. These processing and distribution centers are increasingly centralized (both geographically and virtually), as standardized and consolidated datasets from these sensors enable the analysis of extraordinary amounts of data by using machine learning (ML) and artificial intelligence (AI).[46]

The ability to perform big data analytics on conventional and nuclear early-warning sensors increases the situational awareness of states seeking indications of imminent nuclear use, and potentially makes it easier to target both mobile and fixed nuclear launch sites. The diffusion of sensors in the modern NC3 makes cyberattacks on any one sensor far less debilitating than would have been the case in the more platform-reliant pre-digital nuclear world. Additionally, the integration of AI and ML techniques on this data can help maintain situational awareness even when some sensors are out of commission, allowing for a graceful degradation of nuclear warning.[47] However, digitally advanced states like the US—in their quest to create this very resilient and smart network of sensors—entangle conventional and nuclear assets. Intelligence sensors, now able to pass digital packets of information instead of analog or physical film, are increasingly used to collect for both strategic and conventional mission sets. Moreover, processing, exploitation, and distribution centers are agnostic to the focus of the sensors and instead process vast quantities of data and then pass on relevant warning indicators to strategic consumers. Both the entanglement of these sensors and their processing capability increase the amount of data that states can use for nuclear warning and conventional warfighting, which has a side effect of increasing resiliency against attacks on sensor platforms.

The diffusion of sensors in the modern NC3 makes cyberattacks on any one sensor far less debilitating than would have been the case in the more platform-reliant pre-digital nuclear world.

The new digital ISR networks for both early warning of nuclear threats and nuclear targeting are composed of diffuse, decentralized sensor networks that are far more resilient to attacks on any one node than previous analog ones. However, the reliance on hubs for data processing and exploitation can create new centralized vulnerabilities, even as the networks promise better efficiency and overall situational awareness for both early warning and targeting.[48] Meanwhile, the entanglement of both sensors and processing nodes means that digital ISR networks are characterized by uncertainty about the separation between conventional and nuclear missions.

What does this new digital ISR network mean for cyber operations and nuclear stability? Where is the network most vulnerable and what types of cyber operations are most likely to succeed? Finally, how do those vulnerabilities and potential effects lead to deliberate, inadvertent, or accidental pathways to nuclear use?

44 Curtis Peebles, *High Frontier: The United States Air Force and the Military Space Program* (Air Force History and Museums Program, 1997).

45 Acton, "Escalation Through Entanglement."

46 Mark Kempf, *Distributed Common Ground System—Navy Increment 2 (DCGS-N Inc 2)* (US Navy, 2016); Brandon L. Van Orden, *The Role of a Data Manager in the Successful Employment of the Distributed Common Ground System—Army (DCGS-A)* (Army Command and General Staff College, 2014); Jon A. Kimminau, *A Culminating Point for Air Force Intelligence, Surveillance, and Reconnaissance* (Air Force Deputy Chief of Staff, Intelligence, Surveillance & Reconnaissance, 2012); Sherrill Lingel, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li A. Zhang, and David Blancett, *Joint All Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications* (RAND Corporation, 2020).

47 Patty Welsh, "Using AI to Improve Intelligence Gathering," *Air Force Material Command*, May 18, 2020, https://www.afmc.af.mil/News/Article-Display/Article/2190029/using-ai-to-improve-intelligence-gathering/.

48 There are potentially technical solutions to this centralization vulnerability, including creating digital twins and hybrid clouds. The trade-off is potentially cost and complexity.

Perhaps the bluntest use of cyber operations is in cyberattacks, or cyber operations that destroy data or physical capability, on the sensors themselves—whether they are satellites, airborne reconnaissance, or ground SIGINT collection sites. Because these platforms are so diffuse and the networks so dense, successful cyberattacks on sensors will likely have little impact on the overall resiliency of the sensor network.[49] These attacks would have to render a large proportion of the sensors inoperable to generate significant impact on the network. If platforms are diffuse and varied, it is unlikely that cyberattacks could find success with multiple platforms at the same time.[50] Doing so would require multiple unique exploits and multiple unique accesses, making cyber success in creating significant impacts to the ISR network exponentially more difficult. Even the manipulation of information via cyber operations would struggle to affect the overall network of these operations that target one or a handful of sensor platforms. Because big data and multiple sensors allow processing to identify and discard erroneous data,[51] it would, theoretically, be very difficult to alter a common operating picture or overall situational awareness by manipulating information from separate platforms. Finally, entanglement with conventional platforms increases the chance that nuclear sensors might be targeted inadvertently, but it does not decrease the difficulty that cyberattacks would have in creating meaningful effects when those attacks are solely against cyber platforms within ISR networks.

While cyberattacks on platforms are both difficult and unlikely to create the kind of systemic effects that would make the three pathways to nuclear use more likely, cyberattacks on intelligence hubs (processing and distribution facilities, command centers, and so forth) may be more destabilizing. Indeed, migration to the cloud creates large database centers that consolidate entire inventories of nuclear knowledge.[52] The centralization of these intelligence data hubs—which makes the network so resilient and able to gracefully survive multiple attacks on platforms—also creates valuable and vulnerable nodes for cyberattack, giving incentives for both deliberate and inadvertent escalation. In particular, given an ISR network with few and highly centralized hubs, successful cyberattacks against these intelligence hubs could enable blinding preemptive nuclear attacks with significant ramifications for secure second strike. Without secure second strike, states may have to lean forward with more nuclear alerts and pre-delegation of authorities and capabilities to deployed weapons platforms. This approach in turn creates increased risk of accidental nuclear use. Finally, the entanglement of both conventional and nuclear ISR networks within these hubs makes these facilities enticing targets for even limited conventional conflict. Whereas attacks on entangled sensor platforms were unlikely to create systemic effects that would lead to escalation, the centralization and density of these intelligence nodes makes the pathways to inadvertent escalation from conventional attacks on these facilities far more likely.

How likely is it that cyberattacks could create blinding effects against ISR nodes? There are a few plausible and therefore dangerous vectors. The first vector is using cyberattacks to create physical restrictions to the use of a facility—for example, attacking electrical infrastructure, HVAC, physical hard drives,[53] or even security so that people would be unable to access the facility. While these types of exploits and accesses could be within the capabilities of the most competent state actors in cyberspace, they are unlikely to have long-term effects on the ability to use the facility. Most of these vulnerabilities should have manual backups or physical alternatives (like a generator). Attackers using this cyber vector would have to know that the exploit was extremely time sensitive and therefore the window of opportunity for preemptive strike must be quite small. This effect means that this vector is unlikely to create pathways to inadvertent nuclear use, but may increase the pressure for deliberate nuclear use. The second potential vector is through the networks that come in and out of the facility—encrypted radio-frequency (RF) communications, fiber-optic cabling, and satellite up and down links. Each of these links creates physical (as well as virtual) challenges for cyberattackers, many of which require physical access to one of these modes of transmission. While not impossible, once again these would be very difficult accesses for states to achieve.[54]

49 The exception here is if there are intelligence assets that provide sole-source early warning (for example, if there were a limited number of assets able to photograph a launch site or detect thermal emissions from a launch).

50 Investment in a large quantity of sensors from one vendor, however, could create systemic vulnerabilities across different intelligence missions.

51 R. H. Hariri, E. M. Fredericks, and K. M. Bowers, "Uncertainty in Big Data Analytics: Survey, Opportunities, and Challenges," *Journal of Big Data* 6, no. 44 (2019), https://doi.org/10.1186/s40537-019-0206-3.

52 Jacquelyn Schneider, "JEDI: Outlook for Stability Uncertain as Pentagon Migrates to the Cloud," *Bulletin of the Atomic Scientists*, June 21, 2018, https://thebulletin.org/2018/06/jedi-outlook-for-stability-uncertain-as-pentagon-migrates-to-the-cloud/.

53 Christian Vasquez and Elias Groll, "Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault," *Cyberscoop*, August 10, 2023, https://cyberscoop.com/viasat-ka-sat-hack-black-hat/; https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

54 Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *Wired*, March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/; Pierluigi Paganini, "Kevin Mitnick Explains How to Hack Fiber Optic and Steal Sensitive Data," *Security Affairs*, June 22, 2015, https://securityaffairs.com/wordpress/37987/hacking/kevin-mitnick-hack-fiber-optic.html.

The final and perhaps most dangerous vector is not using cyberattacks to impact the ability of these facilities to function, but instead inserting or manipulating data that fundamentally alters situational awareness.[55] Unlike the other vectors that are designed to stop a facility from receiving information or communicating with others, this vector is meant only to confuse or obfuscate. And while access is always a challenge for cyber operations, the development of Radio Frequency Cyber (the use of RF energy to inject cyber exploits)[56] suggests that access will be increasingly available for cyberattackers—especially those who are large collectors of data over wireless transmission mechanisms. Moreover, the algorithms these hubs use to parse the data collected by the platforms are particularly susceptible to this kind of manipulation. As the data and algorithms become more complex and operators have less understanding of the methods behind the algorithm, even small manipulations of information could create cascading trust effects in which operators distrust all information coming into the system.[57] The implication for nuclear stability is that these kinds of cyber information manipulations may be more likely to occur as technical capabilities increase and can make the chance of accidental nuclear use extraordinarily high.

Weapons Networks

ISR networks are not the only ones that matter for nuclear stability and cyber operations. Delivery platforms and nuclear weapons also form networks of nuclear effects. Like ISR, nuclear weapons have changed significantly since the first airborne bombs. For example, the US went from a handful of air-delivered nuclear bombs to a missile force and submarines. Meanwhile, airborne nuclear-delivery platforms both proliferated and became entangled with conventional platforms, making it increasingly difficult for states to differentiate conventional from nuclear platforms. At the same time, the advent of the microprocessor and the onset of digital networks changed the weapons themselves. Today's nuclear weapons are more precise and more dependent on guidance and navigation systems.[58]

Unlike ISR, the digitization of weapons platforms has not necessarily created dense networks characterized by resiliency. Instead, for many countries, the end of the Cold War, in concert with technological innovations that theoretically made platforms more survivable, allowed for sparser networks with fewer nodes and pathways to create nuclear effects. This development happened in a few ways. First, many nuclear states decreased how many nuclear platforms they had in their arsenal. For example, for the US, as nuclear platforms became more technologically exquisite—with stealth, sophisticated radars, and top-of-the-line sensor suites—they also became more expensive, and the weapons-delivery components of the nuclear network became scarcer. Meanwhile, arms-control agreements between the US and the USSR in the 1970s to early 2000s, the dissolution of the USSR, and declining US budgets post–Cold War led to smaller nuclear arsenals. Even though the US and Russia preserved their ability to launch nuclear weapons from the land, sea, and air (the three "legs" of nuclear platforms), both countries post–Cold War also had fewer platforms or warheads within each delivery domain.

If a nuclear state chooses to build a network with fewer platforms, then the loss of a few of these components is more likely to lead to an overall network failure. The resiliency problem posed by a decreasing number of weapons platforms is compounded when the scarcity of many of these platforms makes it useful for platforms to share both nuclear and conventional missions. States may find it hard to justify platforms that are only strategic, especially as the cost of platforms increases, but this comes with direct trade-offs for inadvertent escalation.

If a nuclear state chooses to build a network with fewer platforms, then the loss of a few of these components is more likely to lead to an overall network failure.

In network terms, fewer delivery platforms means fewer nodes. Nuclear states may also choose, however, to simplify networks by relying on fewer domains. For example, both the United Kingdom and France have only two legs of the nuclear triad (submarine and

55 Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, and Dawn Song, "Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning," *arXiv*, 2017, https://arxiv.org/abs/1712.05526.

56 Mark Pomerleau, "US Military to Blend Electronic Warfare with Cyber Capabilities," *C4ISRNET*, April 14, 2021, https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/#:~:text=RF%2Denabled%20cyber%20is%20%E2%80%9Cbecoming,you're%20going%20up%20against.

57 Jacquelyn Schneider, "A World Without Trust: The Insidious Cyberthreat," *Foreign Affairs* 101 (2022): 22.

58 Carter et al., *Managing Nuclear Operations*; Fred Kaplan, *The Bomb: Presidents, Generals, and the Secret History of Nuclear War* (Simon and Schuster, 2020); Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (Columbia University Press, 2007).

aircraft), resulting in networks of nuclear weapons with both fewer platform nodes and fewer nuclear pathways. This situation could simplify control, but it also makes the linkages in these networks less varied and therefore more singularly vulnerable within the nuclear network. If, for example, a state is solely reliant on aircraft for nuclear delivery, then a cyberattack that targets how that aircraft receives orders, navigates, or communicates with the weapon could make an entire network pathway vulnerable. Paradoxically, the more varied the pathways and platforms are for delivering nuclear effects, the less ability there is to control, but also the more resilient the overall network will be from a singular cyberattack.

Nuclear platforms and pathways aren't the only components of nuclear effects networks. The munition itself—whether it be a cruise missile, ballistic missile, or bomb—also impacts the survivability of a nuclear weapons network. Weapons are differentiated by their guidance, kinematics, and lethality. Each of these characteristics can create network vulnerabilities or, alternatively, resilience. For example, the reliance on navigation systems—GPS (US), BeiDou (China), and GLONASS (Russia)—for targeting and guidance or physical components shared across weapons (like semiconductors) may create systemic points of vulnerability across the nuclear network. In contrast, weapons that rely only on on-board navigation may give up precision and control for less off-board vulnerability.

Decisions to simplify control, standardize components, and decrease cost will lead to a nuclear weapons network that is less resilient and less able to gracefully decompose. In contrast, networks with multiple nuclear delivery pathways, as well as diverse platforms, weapons systems, and guidance—all components that might be detrimental to efficiency or safety—mitigate the risk of systemic cyber effects due to cyberattacks. Adversaries will have to develop cyber exploits and accesses unique to each platform, making these cyber operations time-consuming and expensive. Despite the difficulty, platform-specific cyber vulnerabilities that affect an entire domain of nuclear platforms (for example, in the avionics suite, shipborne navigation, or missile silo software controls) would be a tempting cyber exploit for states to develop—one that could incentivize preemption and deliberate nuclear use, especially for states that might otherwise not have a nuclear advantage. Research from war games suggests overconfidence imbued by cyber exploits is especially dangerous when it threatens a state's second-strike arsenal.[59]

What a network lens reveals about cyberattacks and nuclear stability is that the greatest potential for deliberate nuclear use is not a cyberattack on one weapons delivery platform, but a cyberattack on the weapons themselves. This scenario is the most dangerous and most difficult type of cyberattack because it requires infiltrating supply chains for components like semiconductors, which takes many years of planning and orchestration.[60] If a state were to have this kind of persistent access to a vulnerability inside many different weapons, they might be willing to risk a first strike, confident that the opposing state would not have the ability to conduct a second-strike attack.

The danger for cyber operations and nuclear weapons networks is probably less about deliberate escalation to nuclear use, which requires extraordinarily rare and difficult cyber operations to create systemic effects. Instead, a greater concern is inadvertent escalation and accident. Entanglement of scarce platforms makes them lucrative conventional targets and prime candidates for misperception, which could lead to accidental nuclear engagement. The scarcity that makes these weapons platforms such poor cyber targets also means the platforms are more in demand in a conflict and vulnerable to a first strike, driving states to place them on heightened states of alert. In turn, a nuclear platform on alert that is targeted by a cyberattack on its avionics suite, datalinks, or cabling could create confusion and panic in operators. Forced to make a short-order decision about using nuclear weapons, these operators may find themselves in a real-world version of *Wargames*, in which they must decide whether errors are precursors to attack.

Command, Control, and Communications Networks

Nuclear weapons platforms and ISR networks are linked together by command, control, and communications networks. Initially, NC3 structures were extraordinarily simple: One centralized hub leveraged telephone lines and line-of-sight radio relays to command and control a limited number of weapons platforms. However, weapons platforms and sensors proliferated—as did nuclear-armed states. For modern nuclear states, the simple structures evolved to multiple command nodes, both airborne and dispersed in ground locations. Communications between these control nodes also evolved, as weapons platforms were increasingly remote and as control needed to be quicker. These communications

59 Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation," *International Organization* 77, no. 3 (2023): 633–67.

60 Jordan Robertson and Michael Riley, "The Big Hack," *Bloomberg*, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

proliferated with wireless communications across the frequency spectrum (increasingly digitized and encrypted), relays over the horizon and into space, and domestic and international fiber-optic cabling.[61]

Control nodes—and the limited pathways between these nodes—may be the most difficult and dangerous cyber targets for incentivizing deliberate nuclear use.

Command creates the most important nodes of the nuclear network. In the United States, the national command authority must be able to launch and respond to nuclear attacks. Perversely for network theory, though these nodes are essential to the nuclear network, they are also scarce, have few linkages, and are unidirectional. This situation makes them extraordinarily vulnerable nodes within the network, and their loss risks the failure of the entire network. These vulnerabilities are not novel to the digital world; for decades, nuclear command nodes have been some of the most fragile components of nuclear systems. And while that fragility threatens nuclear control and second-strike capabilities, it is also necessary to ensure that nuclear weapons are not launched by rogue military or political officials. The choice for control, even if it means fragility and vulnerability, is a conscious decision about political use of nuclear weapons, separate from the digital technology that enables command.

While the decision to limit the number of command nodes is not new to the digital age, the ways in which these nodes can be attacked are perhaps novel. The vulnerabilities inherent in command nodes are very similar to the dense and valuable ISR sensor-processing and distribution nodes, though their role in the network is quite different. Command nodes are difficult cyber targets, with access restricted to either physical exploits of fiber-optic cabling on domestic soil or within line-of-sight encrypted intercepts of satellite or RF relays. If a country was able to gain that sort of access, these vulnerabilities would become the near-perfect targets for cyberattacks against nuclear command and control, arguably creating maximum incentives for the deliberate use of nuclear weapons. Command nodes are therefore the most difficult (and least likely to succeed) cyber targets, and the most dangerous vulnerabilities.

Control nodes—and the limited pathways between these nodes—may be the most difficult and dangerous cyber targets for incentivizing deliberate nuclear use. However, vulnerabilities within more diverse communications mechanisms that hold together the entire nuclear system create incentives for both inadvertent and accidental nuclear use. NC3 networks have three types of communication mechanisms, each with its own implications for cyber operations and nuclear use. The first—radio relays—communicate between sensors, airborne platforms, submarine platforms, and within line-of-sight airborne control or centralized ISR nodes. As airborne transmission mechanisms, radio relays are inherently vulnerable to interception, but often encrypted. Manipulation of information within these nodes is dependent both on the physical range of the relay to intercept it, and the ability to decrypt information. The logic of these vulnerabilities is, therefore, very similar to jamming, which requires a cyberattacker to be both overt and within line of sight (and amplitude range) of the target. Because of this physical challenge, it is difficult to insert cyber exploits across a wide variety of RF communications relays.

Despite the inherent physical challenge of targeting relays, it is impossible to say that a state may not be able to innovate a cyber exploit that targeted a relay or inserted manipulated information (for example, deep fakes) within the network. Like the centralized ISR node vulnerabilities discussed above, the most dangerous outcome here is that cyberattacks create confusion within nodes that cascades into distrust for the entire system. This scenario is more likely to occur by manipulating information than by creating virtual or physical destruction with cyberattacks. Therefore, the danger becomes accidental use derived from bad information or panic after the integrity of communications systems cannot be trusted. In addition, the entanglement of some RF communications links with the transmission of conventional warfighting information may make them lucrative targets that could increase chances for inadvertent escalation. The good news for inadvertent escalation dangers is that, so far, the empirical record suggests that individuals are

61 Paul Bracken, *The Command and Control of Nuclear Forces* (Yale University Press, 1985); Ashton B. Carter, "The Command and Control of Nuclear War," *Scientific American* 252, no. 1 (1985): 32–39; John Harvey, "US Nuclear Command and Control for the 21st Century," *Tech4GS Special Reports* (2019): 3; James J. Wirtz and Jeffrey A. Larsen, eds., *Nuclear Command, Control, and Communications: A Primer on US Systems and Future Challenges* (Georgetown University Press, 2022); Charles Glaser, Austin Long, and Brian Radzinsky, eds., *Managing US Nuclear Operations in the 21st Century* (Bloomsbury Publishing USA, 2022).

overly cautious about nuclear false alarms—especially when induced by cyber vulnerabilities.[62]

The second type of communications mechanism is over-the-horizon satellite linkages. These vulnerabilities are very similar to those from RF transmission methods; these linkages operate within the electromagnetic spectrum and pose similar problems of geography in intercepting the transmissions to and from ground satellite transmission sites. Unlike other RF links that may move with the platform (and thus create very difficult targets to intercept), satellite transmissions can be relatively fixed. This quality makes them easier targets for electromagnetic warfare. Therefore, while these vulnerabilities create the same sort of inadvertent and accidental incentives for nuclear use as line-of-sight relays, they are more likely to occur than ground or airborne RF relays.

The third and final type of communication is via cable—either underwater or on land. These mechanisms require physical access and therefore are the most secure methods of transmitting control—especially over domestic territory (underwater sea cables are much more susceptible to access).[63] They are, however, inflexible, and can only work if command is able to access a physical node to conduct the communications.

Conclusion and Implications

The digitization of nuclear systems can lead to more resilient and effective networks for nuclear weapons. However, certain network characteristics—entanglement, limited nodes, and sparse pathways or linkages—can lead to potentially lucrative targets for cyber operations, which in turn has implications for deliberate, inadvertent, and accidental nuclear use. States will have to find a balance between efficiency, control, and resilience as they modernize nuclear arsenals. Network theory should guide those choices.

The good news is that many modern nuclear networks include diffuse overlapping sensors, varied weapons platforms, and unique communication links. All of these characteristics reduce incentives for preemption and deliberate escalation. As states move to centralized information processing or command nodes, however, incentives for deliberate nuclear use due to cyber vulnerabilities increase. Moreover, reliance on similar hardware components or scarce systems for navigation could create systemic vulnerabilities within both platforms and weapons capabilities. While these vulnerabilities may be hard targets for cyber operations (and therefore make such operations less likely to succeed), they are also the most dangerous.

States concerned with incentives for deliberate escalation should therefore either develop multiple redundant or overlapping nodes for ISR and command and control functions (the highest cost but safest option), or pay particular attention to cyber defense and node hardening (a less costly but less safe option). The first option reduces the overall efficiency of the network, but mitigates destabilizing incentives for preemptive nuclear use. The second option optimizes network effectiveness, but with a risky bet that cyber defenders will be able to fend off cyber attackers—a proposition that will be difficult to prove and therefore introduces significant uncertainty in the resiliency of these nodes and the resulting ability of the nuclear enterprise to maintain a credible second-strike capability. Finally, states facing these dilemmas will have to pay special attention to supply-chain vulnerabilities and sole-system reliance on software or navigation systems.

Perhaps a more dangerous and more likely effect of cyber operations on nuclear stability is the opportunity that network design creates for inadvertent and accidental nuclear use. The same proliferation of sensors that makes situational awareness of nuclear threats so much more robust also introduces entanglement and complexity issues. Sensors and platforms are used for both conventional and nuclear missions, making them attractive targets in conventional warfighting, which could easily be misperceived as an initial, deliberate step toward nuclear use. Analysis of dense sensor networks versus sparse weapons networks suggests that the danger of inadvertent escalation is most likely to occur with cyberattacks on weapons platforms. These cyberattacks, however, are also very difficult to execute because they require either supply-chain access to hardware components within the platforms or line-of-sight cyberattack capabilities.

The most likely and therefore most dangerous cyberattacks are neither those that threaten platforms nor the extremely difficult cyberattacks on central nodes that disable a facility. Instead, the most dangerous and likely are cyber operations that attack data and create decision-making vulnerabilities that induce accidental nuclear use. For instance, the fear of cyber operations that incentivizes preemptive nuclear use could lead to forces being placed on nuclear alert and pre-delegation of control to weapons platforms.

62 This includes both war-gaming data from Schneider et al., "Hacking Nuclear Stability," as well as historical anecdotes about US-USSR false alarms from Anthony Barrett, "False Alarms, True Dangers," *RAND Corporation*, document PE-191-TSF, *DOI* 10 (2016), https://www.rand.org/pubs/perspectives/PE191.html.

63 Ash Rossiter, "Cable Risk and Resilience in the Age of Uncrewed Undersea Vehicles (UUVs)," *Marine Policy* 171 (2025): 106434.

In high-stress situations like these, with little room for error, even cyber operations that marginally degrade weapons or command platforms could lead to accidental nuclear use. As networks become more dense, diffuse, and complicated, it is harder for cyber operations to destroy those networks—but easier for cyber operations to affect our trust of them and of the information that flows within them. Centralized information nodes, buttressed by big data and algorithmic parsing of information, are especially susceptible to attacks on operator trust because their complexity makes it more difficult for human decision-making to rely on entire networks.

In the end, cyber operations will likely not have the Armageddon effects on nuclear stability that many fear. The most acute dangers are more insidious, and reflect vulnerabilities in trust that come from decisions made to optimize digital effectiveness. Countries seeking both credible nuclear deterrence and nuclear stability will have to think about distributed networks and manual operations, finding both technical and organizational solutions to create graceful degradation options for nuclear stability in a cyberspace era.

Dr. Jacquelyn Schneider *is the Hargrove Hoover Fellow and director of the Wargaming and Crisis Simulation Initiative at the Hoover Institution, Stanford University. Her research operates at the nexus of technology, national security, and political psychology, with an emphasis on cybersecurity and autonomous systems. A prominent voice in defense policy, Dr. Schneider is the coauthor of* The Hand Behind Unmanned: Origins of the US Autonomous Military Arsenal *(Oxford University Press, 2025). The book provides a definitive history of how cultural identities and bureaucratic "policy entrepreneurs" shaped the development of the American autonomous arsenal. Dr. Schneider is an affiliate at Stanford's Center for International Security and Cooperation and previously served as a senior advisor to the Cyberspace Solarium Commission. Her work has appeared in a series of academic and policy outlets, including* International Organization, Security Studies, Foreign Affairs, Financial Times, *and* The New York Times. *She holds a PhD from George Washington University.*

Stanford University, Stanford, CA, USA, email: jacquelyn.schneider@stanford.edu.

Acknowledgments: *The author would like to thank Harold Trinkunas and Herb Lin for shepherding this piece through publication, and Sheena Greitens, Rose McDermott, Josh Rovner, Colin Kahl, Jon Lindsay, and other members of the stability group for comments on the piece and ideas about network theory.*

Image: *Using AI to improve intelligence gathering by US Air Force.*[64]

64 For image, see https://www.afmc.af.mil/News/Photos/igphoto/2002301759/mediaid/4226077/.