INSTITUTE FOR DEFENSE ANALYSES

Protecting Nuclear Command, Control, and Communications Below the Threshold of Armed Conflict: Don't Count on Deterrence

Kayla T. Matteucci

June 2021
Approved for public release;
distribution is unlimited.
IDA Paper NS P-14360
Log: H 20-000380

INSTITUTE FOR DEFENSE ANALYSES
730 E. Glebe Road
Alexandria, VA 22305

About This Publication
The work was conducted by the Institute for Defense Analyses (IDA) under CRP C6535.

Disclosure:
Human Subject Protections (HSP) protocols have been used in this paper in accordance with the appropriate statutes and Department of Defense (DOD) regulations governing HSP. The views of the sources rendered anonymous by HSP are solely their own and do not represent the official policy or position of DOD or the U.S. Government (or other agency or group as appropriate).

Acknowledgments
I am deeply grateful to the Institute for Defense Analyses and my team in the Strategy, Forces, and Resources Division. Maj Gen (Ret.) William Chambers, Adm (Ret.) John Harvey, Gen (Ret.) Larry Welch, Priscilla Guthrie, Dr. Caroline Milne, Mr. John Warden, and Dr. Rhiannon Hutton have provided invaluable guidance throughout this process.
During their command of U.S. Strategic Command, Gen John Hyten and Adm David Kriete were central to deepening my interest in the strategies surrounding nuclear command, control, and communications. I am indebted to Martin Doebel, Robert Taylor, and Maj Anthony Cato at STRATCOM for hosting me graciously and challenging me to consider operational perspectives.
Dr. Raymond Kuo was a constant voice of affirmation. Dr. John Harvey was an unwavering source of mentorship and motivation. My partner, Douglas Ottino, has read many, many drafts of this paper. I am grateful for his unconditional support.

For More Information:
Maj. Gen. William A. Chambers, Project Leader
wchamber@ida.org, 703-845-2133

ADM John C. Harvey, Jr., USN (Ret), Director, SFRD
jharvey@ida.org, 703-575-4530

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper NS P-14360

Protecting Nuclear Command, Control, and Communications Below the Threshold of Armed Conflict: Don’t Count on Deterrence

Kayla T. Matteucci

This page is intentionally blank.

Executive Summary

The United States considers nuclear command, control, and communications (NC3) to be the backbone of its nuclear deterrent, ensuring that nuclear weapons are always available for use by the president and never by an unauthorized actor. Since the late days of the Cold War, NC3 has faced a growing array of non-kinetic threats which fall below the traditional threshold of armed conflict. Malicious non-kinetic activity continues to intensify in potency and prominence, creating fear among U.S. leaders that a hostile actor could utilize means short of war to significantly compromise NC3 systems and, by extension, the United States' nuclear deterrent. Responding to such concern, this paper argues that deterrence is an ill-suited strategy for managing non-kinetic threats to NC3.

The DOD is in the initial stages of recognizing that it needs survivability and resilience standards to protect against non-kinetic threats. However, it has yet to act on this urgent need in a meaningful way. Rather than hoping for deterrent protection that may never materialize, the United States should take a proactive approach to defending NC3 against non-kinetic threats by implementing the following recommendations. (A more expansive list of recommendations can be found in the body of this text.)

- **Incorporate into doctrine the assumption that NC3 will inevitably be compromised, instead of striving for impervious defenses**.
    - Stemming from this assumption, **create a requirement for the survivability and resilience of NC3 against non-kinetic attacks** at all stages of its lifecycles, including design, production, maintenance, and, if applicable, life extension. Toward that end, in order to achieve awareness of its vast and complex NC3 architecture, the U.S. should appoint a Chief Engineer* to oversee the fielding and maintenance of Next Generation NC3, moving away from viewing NC3 in terms of individual subsystems and toward the interoperability of subsystems within a unified whole.
    - Make an internal, classified determination regarding the **level of risk to NC3** that the U.S. government is willing to tolerate in order for its nuclear deterrent to be considered survivable and resilient overall.
    - If cost and resource constraints inhibit designers from achieving a gold standard of survivability and resilience throughout *all* NC3 subsystems, the U.S. should

* This recommendation stems from conversations with Priscilla Guthrie.

  endeavor to defend a **"thin line,"** or smaller grouping of its most vital subsystems, concentrating funds and expertise toward protecting that thin line from non-kinetic threats.[**]

  - **Create dedicated red teams** to actively test the vulnerability of NC3 to various types of non-kinetic attack, adapting as NC3 and the threat environment evolve. Allow U.S. military red teams and other NC3 specialists to remain in their roles for extended periods of time in order to amass the requisite expertise and create institutional memory.[***]
  - **Prepare to operate under incomplete or incorrect information**. Plan as though immediate attribution of non-kinetic attacks is impossible and prepare for crisis situations in which aggressors remain anonymous.

- **Ensure that NC3 modernization and changes to the strategy and doctrine impacting NC3 remain integrated into a cohesive vision of strategic stability**.[****] Deterrence strategies, modernization efforts, and arms control dialogues have a shared aim of preventing nuclear war. As such, they should go hand in hand. Although it is not the focus of this paper, recent research demonstrates that it may be enormously beneficial to initiate dialogue with other nuclear weapon states (NWS) about perceived threats to NC3, seeking to improve mutual understanding of doctrine, declaratory policies, and most pressing concerns. Absent meaningful dialogue with NWS, conversations about the survivability and resilience of NC3 lack critical context. Pursuing such dialogue can reduce undue pressure on U.S. NC3 by potentially limiting or disincentivizing non-kinetic attacks on sensitive systems.

As was the case throughout the Cold War, deterrence is an imperfect instrument, resting first and foremost on an adversary's perception. Nuclear weapons can likely still be used to inspire restraint in other NWS, and the United States' nuclear deterrent need not depend upon a binary view of NC3 systems as either secure or not secure. In openly assuming that hostile actors can and will compromise NC3 systems below the threshold of armed conflict, the U.S. does not forego the opportunity to maintain a credible (if imperfect and ever-evolving) *nuclear* deterrent. By

[**] Although its overall findings conflict with the arguments made above, the DSB's *Task Force on Cyber Deterrence* provides useful recommendations on defending vital weapon systems against cyberattacks by upholding a cyber "thin line." See: United States Department of Defense and United States Defense Science Board, *Task Force on Cyber Deterrence (*Washington, DC: Department of Defense, February 2017), https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf.

[***] The author benefitted from discussions on this subject with Priscilla Guthrie, Dr. John Harvey, and Jim Gosler.

[****] Strategic stability is a contested term. For thoughtful consideration of differing types of stability such as "arms race stability" and "crisis stability," see James Acton's analysis in "Reclaiming Strategic Stability," chap. 4 in *Strategic Stability: Contending Interpretations*, ed. Elbridge Colby and Michael Gerson (Carlisle, PA: Strategic Studies Institute, 2013), 117.

embracing an emphasis on resilience, the U.S. can demonstrate its ability to actively respond to below-the-threshold attacks on NC3, overall providing for a nuclear deterrent that is more credible in the eyes of other NWS and allies, while also engaging in dialogue that clarifies misperceptions and reduces nuclear risks.

In the coming decades, the safekeeping of U.S. NC3 will require unremitting and honest appraisal of its vulnerabilities. The analysis contained here demonstrates that, at present, deterrence is not a reliable strategy for managing non-kinetic threats to NC3. Given rapid evolutions, for example, in cyber offensive capabilities augmented by artificial intelligence or potential breakthroughs in quantum computing, the severity of non-kinetic threats to NC3 may quickly increase.

NWS have ostensibly determined that the perceived protective benefits of nuclear arsenals continue to outweigh the potential risks of nuclear use—intentional or not. However, NC3's non-kinetic vulnerabilities may become so pronounced that the perceived benefits of possessing a nuclear deterrent no longer outweigh the perceived risks. Simple principles such as the law of large numbers tell us that undesired events such as incursions and accidents will occur. In times of rapid technological development, governments have managed the inevitable failures of humans and machines both through luck and by embracing safety precautions that provide the opportunity to back away from nuclear use. The U.S. government and all NWS would benefit from revisiting these considerations often, especially in light of the compounding risks created by non-kinetic threats to NC3.

This page is intentionally blank.

Contents

1. Introduction 1
   A. Background 2
   B. Roadmap and Methodology 3
2. What is NC3? 5
3. Threats to NC3 Below the Threshold 11
4. Relevant Literature 15
   A. The “Gray Zone,” Calculated Risk, and Secrecy 15
   B. Deterrence and its Limits 17
   C. Cyber Deterrence: The New Kid on the Block 20
5. Summary..25
6. Analysis 27
   A. Why Deterrence Won’t Work 39
      1. Credible Threats 39
      2. Detection and Attribution 40
      3. Transparency Versus Ambiguity..40
7. Defending NC3 Below the Threshold 43
   A. Actualizing Survivability and Resilience 43
8. Policy Recommendations 47
9. Areas for Further Research..51
   A. Collecting and Analyzing Empirical Data..51
   B. Exploring Implications for Strategic Stability..52
   C. Avenues for Risk Reduction..52
   D. The Future of Nuclear Strategy 53
10. Conclusion..55

Appendix A. Nuclear Close Calls Caused by Human Error and System Malfunction.. A-1

Appendix B. Illustrations..B-1

Appendix C. References C-1

Appendix D. Abbreviations D-1

This page is intentionally blank.

1. Introduction

For good reason, nuclear command, control, and communications (NC3) has been thrust to the forefront of conversations within the nuclear policy and broader defense community. Regardless of one's beliefs about nuclear weapons, the goal of stable and secure NC3 should be viewed as a universal benefit. As long as nuclear weapons exist and nuclear possessors view one another in an adversarial light, all policy practitioners, elected officials, bureaucrats, activists, and academics alike have a shared incentive to advocate for the safekeeping of NC3.

The majority of NC3 subsystems are derived from an era that predates the internet and modern concerns about threats[1] to the United States in cyberspace.[2] Since the late days of the Cold War, NC3 has faced a growing array of non-kinetic[3] threats capable of undermining the United States' nuclear forces in ways that previously only nuclear weapons could. Among policymakers and military leaders, there is concern that malicious state actors could exploit non-kinetic tools to achieve the equivalent of a "strategic attack."[4] In other words, an adversary could utilize means short of armed conflict to significantly compromise NC3 and, by extension, the United States' nuclear deterrent.

As a reaction to this rising concern, the 2018 Nuclear Posture Review (NPR) asserts that the U.S. reserves the right to respond with nuclear weapons to "significant non-nuclear strategic attacks" in "extreme circumstances." According to the NPR, these might include non-nuclear "attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[5] Notably, the heading under which these statements appear is "Deterrence of Nuclear and Non-Nuclear Attack," a title which suggests that the Trump

[1] I define a threat as "anything that can exploit a vulnerability to harm a system, either intentionally or by accident." As seen in United States Government Accountability Office, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," GAO-19-128 (Washington, DC: GAO, October 2018), https://www.gao.gov/products/gao-19-128.

[2] Although "cyberspace" is a contested term, the DOD defines cyberspace as "the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Chiefs of Staff, *Cyberspace Operations,* JP 3-12, (Washington, DC: Joint Chiefs of Staff, June 2018) https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[3] While there is no official DOD definition for non-kinetic actions, the Air Force defines them as "[producing] effects without direct use of the force or energy of moving objects." See: Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-0 Operations and Planning." 2016.

[4] Office of the Secretary of Defense, "Nuclear Posture Review" (Washington, DC: Department of Defense, February 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

[5] Ibid., 21.

administration may have selected deterrence as its chosen strategy to confront non-nuclear threats to NC3, including those that might fall below the threshold of armed conflict.[6]

The Biden administration's forthcoming NPR will shed light on its intended strategy for managing non-kinetic threats to NC3. Its review of existing policies should include a critical examination of potential strategies for mitigating non-kinetic threats to the U.S. nuclear arsenal. The following argues that deterrence is ill-suited to be the predominant strategy for addressing threats to NC3 short of war. The 2018 NPR appropriately grapples with the urgent issue of non-kinetic threats to NC3, but it does not identify a credible plan for managing them. Although the threat to consider using nuclear weapons in "extreme circumstances" might successfully deter severe and openly hostile uses of non-kinetic tools, it is insufficient to deter non-kinetic attacks of a more ambiguous and continually changing nature. This paper's central thesis is that deterrence is a tool much too blunt and imprecise to have the desired effect of *preventing* below-the-threshold attacks on NC3.

A. Background

While it is impossible to know whether the absence of major war for the last 75 years is attributable to nuclear weapons and their intended deterrent effects, nations can at least expect to know immediately when their nuclear deterrence strategies have failed (assuming that they are predicated on preventing the use of nuclear weapons). Nuclear weapons are conspicuously destructive, and their deliberate use by any actor would be instantly recognizable as a catastrophic international event and irrefutable deterrence failure.

By contrast, attacks on NC3 short of war would evade such sharp categorization. Adversaries working below the threshold of armed conflict would employ tools such as offensive cyber weapons, which are more readily exploitable than bombs and bullets due to a comparative lack of stigma. Additionally, non-kinetic attacks are often conveniently clouded by questions of detection and attribution, making them valuable for achieving covert aims. Nations such as Russia and China repeatedly exploit non-kinetic tools for malicious purposes during peacetime, demonstrating that they are willing to carry out aggressions in the "gray zone" between war and peace.

This "gray zone" is far from new and has characterized strategic competition for time immemorial.[7] Indeed, Sun Tzu writes in the 5th century text, *The Art of War*, that "a skillful general must defeat the enemy without coming to battle," elucidating a compelling incentive to incur advantages without provoking costly conflict. The 2018 Joint Concept for Integrated Campaigning, produced by the Joint Chiefs of Staff, emphasizes these "emerging patterns of

[6] See later discussion of the threshold of armed conflict.

[7] Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, December 15, 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

competition below the threshold of armed conflict"[8] or "below a threshold that invokes a direct military response from the United States."[9]

Given the strong appeal of such hostile activity and the ease with which adversaries can obscure their culpability, the U.S. cannot count on preventing below-the-threshold attacks on NC3 via deterrence, let alone accurately measure the effectiveness of any prospective deterrence strategy. As it stands, scholarly and governmental theories of deterring below the threshold are nascent and uncorroborated. It is possible that below-the-threshold deterrence will someday become a viable tool when these concepts mature, but the Biden administration and its successors should not rely on an unverified strategy for the overarching security of assets as critical as nuclear weapons. Rather, designers of the United States' future NC3 architecture must strive for resilience in the face of attacks, and U.S. doctrine must treat breaches as both inevitable and manageable.

As was the case throughout the Cold War, deterrence is an imperfect instrument, resting first and foremost on the adversary's perception. Nuclear weapons can likely still be used to inspire restraint in adversaries, and the United States' nuclear deterrent need not depend upon a binary view of NC3 systems as either secure or not secure. In openly assuming that the adversary can and will compromise NC3 systems below the threshold of armed conflict, the U.S. does not forego the opportunity to maintain a credible (if imperfect and ever-evolving) *nuclear* deterrent. By embracing an emphasis on resilience, the U.S. can demonstrate its ability to actively respond to below-the-threshold attacks on NC3, overall providing for a nuclear deterrent that is more credible in the eyes of adversaries and allies, while also engaging in dialogue that clarifies misperceptions and reduces nuclear risks.

B. Roadmap and Methodology

First, this paper will provide an overview of NC3, its key functions, and the concerns surrounding its modernization. Next, it will discuss perceptions of non-kinetic actions and the threshold of armed conflict, offering example scenarios to demonstrate the serious ramifications for NC3. It will then provide a brief review of relevant literature, proceeding to analyze factors that make deterrence a less-than-ideal strategy for managing below-the-threshold threats. Finally, this paper provides policy recommendations and identifies areas for further research.

The conclusions reached here are informed by a series of on-site visits and interviews with subject matter experts at U.S. Strategic Command in 2019; approximately 25 earlier interviews with subject matter experts across the technical and policy realms from 2017-18; and synthesis of

[8] Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning* (Washington, DC: Joint Chiefs of Staff, March 2018) https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257, 6.

[9] Ibid., 3.

relevant scholarly literature, government reports, and public statements made by U.S. officials. The author selected interview subjects who are:

- Key contributors to scholarly discourse and literature surrounding NC3,
- Technical experts in various aspects of potential vulnerabilities to NC3, or
- Direct advisors to the process of NC3 modernization, either as current or former government officials.

2. What is NC3?

According to U.S. strategy, NC3 is the backbone of U.S. nuclear forces, facilitating decision-making and force execution by the president, who is the sole individual authorized to use nuclear weapons. Accordingly, NC3 is defined as:

> "... a large and complex system comprised of numerous land-, air-, sea-, and space-based components used to ensure connectivity between the president and nuclear forces."[10]

It is important to distinguish between NC3 and NC2, or nuclear command and control, which is defined as:

> "the exercise of authority and direction, through established command lines, over nuclear weapon operations by the president as the chief executive and head of state."[11]

While NC2 connotes the authority vested in the president to use nuclear weapons, NC3 describes the array of subsystems that must function properly in order to make that possible. Broadly, NC3 must enable five key functions:[12]

1. Force Direction: entails the implementation of decisions regarding the execution of nuclear strike orders.[13]
2. Planning: involves the development and modification of plans for the employment of nuclear weapons and other operations in support of nuclear employment.
3. Situation Monitoring: comprises the collection, maintenance, assessment, and dissemination of information on friendly forces, adversary forces and possible targets, emerging nuclear powers, and worldwide events of interest.

[10] United States Government Accountability Office, Nuclear Command, Control, and Communications: Update on Airforce Oversight Effort and Selected Acquisition Programs, GAO-17-641R (Washington, DC: GAO, August 2017), https://www.gao.gov/products/gao-17-641r.

[11] The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *The Nuclear Matters Handbook 2020 [revised]* (Washington, DC: ODASD(NM), 2020), chap. 2.

[12] Ibid.

[13] This function relates to nuclear surety, accomplished through procedures, physical security (e.g., gates, guns, and guards), and internal warhead locks and disabling mechanisms to prevent unauthorized use of nuclear weapons. It also relies on positive control, accomplished through procedures, continuous training, equipment, and communications that ensure the president's nuclear control orders are received and properly implemented through the nuclear C3 system.

4. Decision Making: refers to the assessment, review, and consultation that occurs when the employment or movement of nuclear weapons is considered for the execution of other nuclear control orders.
5. Force Management: includes the assignment, training, deployment, maintenance, and logistic support of nuclear forces and weapons before, during, and after any crisis.

In the event of a nuclear attack on the U.S., NC3 must facilitate timely launch detection and provide relevant information to leadership for optimal situational awareness. It must allow the president and her senior advisors to communicate, evaluating the attack and deciding upon an appropriate course of action. The president must then convey an Emergency Action Message (EAM) to warfighters operating the nation's nuclear forces. In the event of a U.S. nuclear response, operators must be prepared to execute launch orders. Force direction must be performed in a matter of minutes and with the utmost confidence in the authenticity of the information being communicated.

NC3 subsystems include ground-based early warning radars, launch detection satellites, terrestrial and space-based communication links, airborne and fixed command centers, and facilities for interpreting sensor data. Figure 1 depicts some of the numerous NC3 subsystems operating daily.[14]

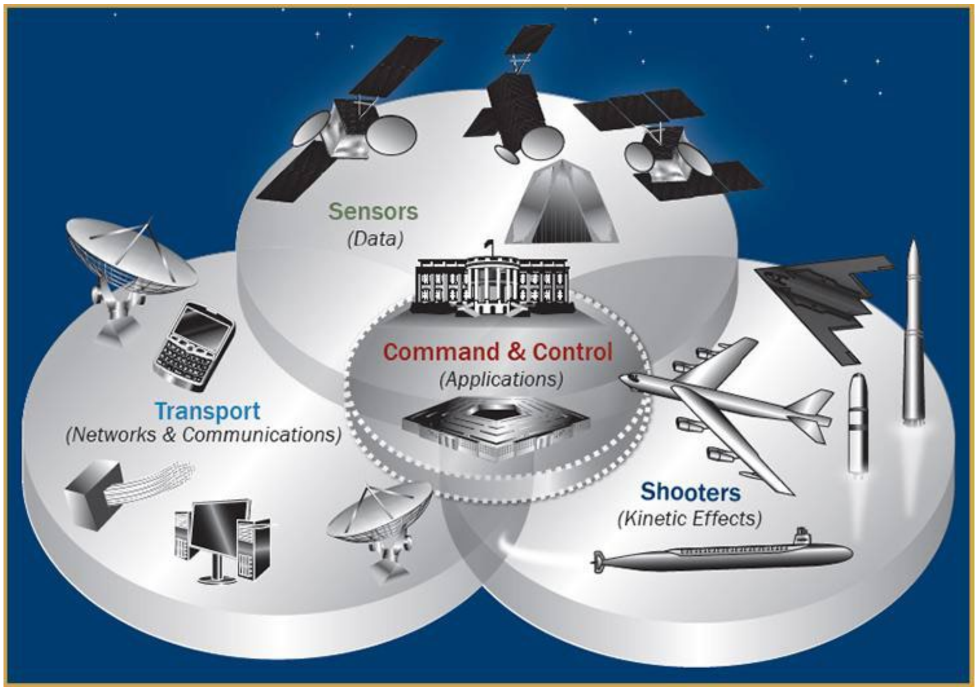

Figure 1. NC3 Subsystems Operating Daily

[14] The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *The Nuclear Matters Handbook.*

The U.S. strives to maintain NC3 that is "reliable, assured, enduring, redundant, unambiguous, survivable, secure, timely, flexible, and accurate."[15] Critically, certain NC3 assets support both nuclear and conventional operations and must always be available during peacetime, as well as throughout every stage of a potential conflict.[16]

Vulnerable NC3 can contribute to the risk of escalation or inadvertent use. Scholars theorize that a breach of NC3 by sophisticated adversaries could result in false alarms for incoming nuclear attacks, inability to detect incoming attacks, unauthorized launch of U.S. nuclear weapons, unintended detonation of a nuclear device, or an inability to send or receive signals from nuclear weapons. An adversary could persuade the U.S. that it had disabled NC3, regardless of whether this had actually occurred. Additionally, an adversary could disrupt or disable communication between key U.S. leaders to create confusion or inhibit effective decision-making. Malicious actors could "hide" within computer systems, making it difficult to know whether NC3 had been compromised until the crucial moment of its use.

Lastly, adversaries may eschew accountability for non-kinetic breaches into NC3 networks, claiming that they intended, for example, to conduct espionage on conventional systems. This is especially true in light of recent reports that the U.S. will field a so-called Joint All Domain Command and Control system, which will integrate much of U.S. nuclear and conventional command, control, and communications.[17]

Modernization in a Changing World

It is valuable to note the context in which changes to the operational concepts surrounding NC3 will play out. U.S. nuclear forces, comprised of a strategic triad, are currently undergoing modernization. The 2018 NPR noted the ongoing replacement of the Minuteman III intercontinental ballistic missile and Trident II submarine-launched ballistic missile, the transition from the Ohio-class submarine to the Columbia-class, the refurbishing of the B-2 and B-52H bombers, and the acquisition of a new bomber, the B-21. It also ordered the development of a new Long Range Stand Off cruise missile, as well as a low-yield SLBM and a new submarine-launched cruise missile.

In addition to nuclear weapons and their associated delivery systems, the 2018 NPR called for a parallel modernization of NC3. The Commander of U.S. Strategic Command (STRATCOM) was designated as the NC3 enterprise lead in 2018, responding to years of concern that "NC3 did

[15] Ibid.

[16] United States Government Accountability Office, "Nuclear Command, Control, and Communications," GAO-17-641R.

[17] Clark, Colin, "Nuclear C3 Goes All Domain: Gen Hyten," Breaking Defense, February 20, 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

not have a cohesive governance structure."[18] As enterprise lead, STRATCOM has "increased responsibilities for operations, requirements, and systems engineering and integration," while the Office of the Secretary of Defense "will handle resources and acquisition."[19]

As the only branch of the military possessing both bombers and ICBMs, comprising a large portion of U.S. nuclear assets and around 80% of NC3, the Air Force is a major decision-maker on matters relating to NC3. The Navy, overseeing substantially smaller portions of the arsenal, has a smaller role in the process but join in the broader effort of the Department of Defense (DOD) to facilitate modernization.[20] Some recent changes to NC3 have already occurred.[21] However, many aging NC3 subcomponents remain untouched and require replacement.[22] Hundreds of scientists and engineers are working on behalf of government contractors to develop potential improvements to NC3, awaiting the DOD's selection of new systems.[23]

The modernization of NC3 is twofold:

1. Identify and resolve issues within the existing "as-is" system, and
2. Design and implement the "to-be" or "Next Generation" architecture of the future, creating a plan to build this system within the next 10 to 15 years.[24]

These complicated undertakings are made even more difficult by the fact that there is no common understanding of exactly what comprises NC3, as it is said to include as few as 107 subsystems or as many as 240.[25] Due to the sprawling and nebulous nature of the NC3 architecture, the costs associated with modernization, and the disparate ages of technology deployed, the DOD is challenged to resource a comprehensive system with state-of-the-art security.

In a 2014 statement to the Senate Armed Services Committee, Admiral Cecil D. Haney, former Commander of U.S. Strategic Command, summarized the challenge of modernizing NC3:

> "Assured and reliable NC3 is critical to the credibility of our nuclear deterrent. The aging NC3 system continues to meet its intended purpose, but risk to mission

[18] Sandra Erwin, "U.S STRATCOM to Take Over Responsibility for Nuclear Command, Control and Communications," *SPACENEWS,* July 23, 2018, https://spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications/.

[19] Ibid.

[20] Martin Doebel, in Conversation with the Author.

[21] Liam Stack, "Update Complete: U.S. Nuclear Weapons No Longer Need Floppy Disks," *The New York Times*, October 24, 2019, https://www.nytimes.com/2019/10/24/us/nuclear-weapons-floppy-disks.html.

[22] Major General Robert Wheeler, in Conversation with the Author.

[23] Senior Government Official, in Conversation with the Author.

[24] John R. Harvey, "US Nuclear Command and Control for the 21st Century," *NAPSNet Special Reports*, May 24, 2019, https://nautilus.org/napsnet/napsnet-special-reports/u-s-nuc-ear-command-and-control-for-the-21st-century/.

[25] Philip Reiner and Alexa Wehsener, "The Real value of Artificial Intelligence in Nuclear Command and Control" *War on the Rocks,* November 4, 2019, https://warontherocks.com/2019/11/the-real-value-of-artificial-intelligence-in-nuclear-command-and-control/.

> success is increasing. Our challenges include operating aging legacy systems and addressing risks associated with today's digital security environment. Many NC3 systems require modernization, but it is not enough to simply build a new version of the old system—rather; we must optimize the current architecture while leveraging new technologies so that our NC3 systems interoperate as the core of a broader, national command and control system."[26]

The varied composition of NC3 poses challenges to those that seek to address the ailments of aging subsystems, while also thinking ahead to the improved architecture of the future. NC3 is an amalgamation of subsystems built as early as the 1950s and as recently as this year.[27] Some of its common features include analog controls, air-gapping, multiple redundancies, and archaic operating systems for which few modern code-writers still receive formal training.[28] Furthermore, aging systems often do not support functions that the U.S. requires today, and they contain brittle code that is difficult or impossible to modify. Decades after the initial fielding of legacy systems, the absence of design documentation or lack of remaining system specialists can make it unclear whether glitches are the result of malicious activity or system malfunctions.[29]

As early as the 1970s, key military leaders recognized America's NC3 as being "fragile" and "susceptible to electronic countermeasures, electromagnetic pulse, and sabotage."[30] In 1978, the Defense Science Board (DSB) attempted to alert leaders about some of the very same risks faced today, stating, "Our command and control systems have not kept up with the changes in the type of warfare or the changes in weapons and available command and control technology."[31] After decades of neglect, the same arguments continue to ring true, but with greater urgency. To date, DOD survivability standards have traditionally focused on protecting NC3 against nuclear and electromagnetic pulse attacks. In the absence of strong requirements to protect against non-kinetic attacks, the U.S. nuclear arsenal is left highly vulnerable.[32]

In extending the as-is architecture and fielding a more resilient Next-Gen system, leaders will face several distinct hurdles. These include the United States' overwhelming reliance on space-

[26] Senate Committee on Armed Services, "Statement of Admiral C. D. Haney, Commander, United States Strategic Command," 113th Cong., 2nd sess., February 27, 2014, 9, https://www.stratcom.mil/Media/Speeches/Article/986430/air-force-association-national-defense-industrial-association-and-reserve-offic/.

[27] Major General Robert Wheeler, In Conversation with the Author.

[28] Ibid.

[29] Kathleen A. Jordan et al., "Legal System Wrapping for Department of Defense Information System Modernization," IDA Paper P-3144 (Alexandria, VA: Institute for Defense Analyses, July 1995), https://apps.dtic.mil/dtic/tr/fulltext/u2/a326906.pdf.

[30] Erik Gartzke and Jon Lindsay. "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 2017): 38, https://doi.org/10.1093/cybsec/tyw017.

[31] Office of the Under Secretary of Defense and United States Defense Science Board, *Report of the Defense Science Board Task Force on Command and Control Systems Management* (Washington, DC: Department of Defense, July 1978), https://dsb.cto.mil/reports/1970s/a110933.pdf.

[32] OASD(NM), *Nuclear Matters Handbook 2020 [revised]*, chap. 9.

based systems and information technology, which can create singular points of failure for NC3.[33] An additional pressure point may take shape in the further compression of presidential decision-making time, intensifying a trend that began during the Cold War; due to the increased speed of weapons delivery and, in some cases, increasing maneuverability of missiles to evade detection, it is possible that future leaders may be unable to consider nuclear response options in great depth.[34]

Finally, today more than ever, states can use conventional and non-kinetic weapons to hold nuclear assets at risk.[35] In particular, as is the focus of this inquiry, potential below-the-threshold threats to NC3 have intensified in number and potency, improving prospects for adversaries who wish to extract benefits short of entering a full-scale conflict. Elements of Russian and Chinese doctrine have confirmed that they intend to use below-the-threshold means to alter the status quo in their favor.[36] It is thus critical that the U.S. identify and pursue a credible strategy for managing below-the-threshold threats to NC3.

[33] Benjamin W. Bahney, Jonathan Pearl, and Michael Markey, “Antisatellite Weapons and the Growing Instability of Deterrence,” chap. 6 in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Eric Gartzke and Jon R. Lindsay (New York City, NY: Oxford University Press, 2019), doi: 10.1093/oso/9780190908645.003.0006, 124; 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 (August 2019): 841-863, doi: 10.1080/01402390.2019.1627209.

[34] Dean Wilkening, *Hypersonic Weapon and Strategic Stability* (Baltimore, MD: Johns Hopkins Applied Physics Laboratory, January 2020), https://nsiteam.com/social/wp-content/uploads/2020/01/200115-Wilkening-Slides.pdf.

[35] Ibid.

[36] For Russia, see: Marie Snegovaya, *Russia Report I Putin's Information Warfare In Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, September 2015), http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare. For China, see: Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York, NY: Oxford University Press, March 2015). On China and space, see: Kevin Pollpeter, “Space, the New Domain: Space Operations and Chinese Military Reforms,” *Journal of Strategic Studies* 39, no. 5–6 (August 2016): 709–727, https://doi.org/10.1080/01402390.2016.1219946.

3. Threats to NC3 Below the Threshold

Non-kinetic threats to NC3 fall below the traditional threshold of armed conflict, posing substantial challenges to deterrence. While there is no official DOD definition for non-kinetic actions, the Air Force defines them as "[producing] effects without direct use of the force or energy of moving objects." Among examples of non-kinetic actions, the Air Force lists "electromagnetic radiation, directed energy, information operations, etc." For context, the Air Force defines kinetic actions as utilizing "the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles."[37]

Throughout history, kinetic actions and physical damage have been central characteristics of armed conflict,[38] which is defined by the International Committee of the Red Cross as "resort to armed force between two or more States." Notably, there is no authoritative definition of armed conflict either under international law or within the U.S. government. As such, it is unclear what is sufficient to provoke hostilities between states and where exactly the threshold of armed conflict lies.[39] Today as always, the potential for interstate conflict is dependent on those in leadership positions at any given time, and the situations that provoke a direct military response from one U.S. president may not provoke the same response from her successor.

Notwithstanding variable thresholds among decisionmakers, this analysis takes "threshold of armed conflict" to mean the *traditional* threshold, informed by centuries of conceptualizing war in terms of kinetic actions. As Herbert Lin notes in the International Review of the Red Cross, "The UN Charter and the Geneva Conventions are relevant to cyber operations, but the specifics of such relevance are today unclear because cyberspace is new compared to these instruments."[40] To say that the traditional threshold of armed conflict is a kinetic one is not to dismiss the potentially destructive effects of non-kinetic tools. Rather, it is meant to reflect that existing

[37] Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-0 Operations and Planning." 2016.

[38] Under international law and within the US government, there is no common definition of armed conflict.

[39] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (Geneva, Switzerland: International Committee of the Red Cross, May 2009), https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

[40] Herbert Lin, "Cyber conflict and International Humanitarian Law," *International Review of the Red Cross* 94, no. 886 (Summer, 2012), https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf.

definitions of armed conflict have focused more on the *means* used to inflict damage, rather than reflecting the *effects* of such actions.

Example Scenarios

Consider two hypothetical scenarios that demonstrate how non-kinetic actions can have a range of troubling effects, some of which might remain undetected and some which would be clearly distinguishable as hostile:

> **Scenario 1:** *U.S. Navy crewmembers aboard a Columbia-class submarine do not know that multiple submarines were compromised by supply chain*[41] *infiltrations during production, making their networks vulnerable to remote access by Country X, either to gain intelligence or obstruct its missions. Exercises to test the platform go off without a hitch, but in the event of a crisis, Country X could activate its exploits, for example, by disabling transmission of messages to STRATCOM and the president. The U.S. remains unaware of the security breach and believes that communications are sound.*
>
> **Scenario 2:** *Amid a resource dispute with Country Y, a nuclear weapons possessor, the U.S. believes war might be unavoidable. Within Country Y and its bases abroad, U.S. intelligence has noted unusual movement of forces that might indicate preparation for conflict. Following a heated exchange between the U.S. president and the leader of Country Y, the U.S. attempts to signal resolve by conducting airstrikes on industrial targets in a remote region of Country Y. The next day, U.S. forces around the world detect what appear to be a series of cyber network intrusions. Early warning systems display false messages and communications between the president, and U.S. nuclear forces are degraded. At the same time, both government and commercial satellites supporting the U.S. military and domestic critical infrastructure are undergoing jamming and spoofing attacks, emanating from regions where Country Y and its allies operate. With some of its warning systems and communications compromised or disabled, the U.S. suspects that Country Y is preparing for a nuclear strike and feels pressure to "use it or lose it." Country Y contacts U.S. leadership, claiming that it has penetrated the vast majority of NC3 subsystems, and demands that the U.S. abandon its efforts to*

[41] The U.S. intelligence community defines the supply chain as "Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of [information and communications technology] products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer." See John Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," NIST Special Publication 800-161 (Washington, DC: NIST, April 2015), http://dx.doi.org/10.6028/NIST.SP.800-161. The DSB notes that supply chain infiltrations can take place in the form of "malicious insertion of defect or malware" or "exploitation of latent [supply chain] vulnerabilities." Such breaches can take place during acquisition or sustainment of weapon systems. See: United States Defense Science Board, *DSB Task Force on Cyber Supply Chain* (Washington, DC: Office of the Under Secretary of Defense, February 2017), https://www.hsdl.org/?view&did=799509.

> *capture scarce natural resources. Country Y publishes media reports echoing the claims of zero-day exploits,[42] causing panic among operators.*

The above scenarios show the range of effects that can be produced using non-kinetic tools, from hidden to immediately apparent and severe. Numerous publications[43] have discussed the possibility of "nuclear blackmail" using cyberattacks, similar to the dynamic described in Scenario 2. But just as a decapitating first strike during the Cold War was unlikely to destroy an adversary's entire nuclear arsenal, a massive cyberattack on U.S. nuclear forces would almost certainly fail to disable them completely. Thus, it is important to question the real-world likelihood of such an attack by rational actors who would no doubt be the target of swift retaliation by surviving forces.

In Scenario 1, multiple Columbia-class submarines are compromised through a breach in the supply chain. If nuclear submarines are unable to respond to EAMs, the U.S. suffers degradation of what should be the most survivable leg of the nuclear triad, forcing the U.S. decision-makers to rely solely on more vulnerable land- and air-based platforms. In a time of crisis or war, Country X's supply chain breach would surely be deemed strategic and possibly sufficient to justify kinetic response. However, Country X acts covertly in peacetime, using non-kinetic tools that allow it to avoid a violent confrontation. An adversary could achieve similar effects using kinetic means, for example, by targeting communication nodes with conventional ordnance—an action that would clearly constitute armed hostility. Yet, Country X's supply chain breach allows it to secretly undermine US nuclear forces, avoiding responsibility and preserving an advantage it can leverage if war ensues. Conversely, in Scenario 2, Country Y moves to directly sabotage U.S. NC3. Ostensibly working in preparation for a major strike, Country Y takes little care to conceal its actions. Regardless of whether they are concealed or not, non-kinetic attacks can do grave harm and can be used to confuse, manipulate, or severely compromise U.S. forces.

This paper aims to afford greater attention to managing non-kinetic attacks on NC3, whose effects can mirror or potentially exceed those produced by kinetic attack. The NPR's mention of "non-nuclear strategic attacks" reinforces this possibility and highlights a key difference between past and present. For the majority of the Cold War, American military planners generally acknowledged that only a largescale nuclear strike by the Soviet Union could succeed in severely compromising the United States' nuclear deterrent force. Since the late days of the Cold War, however, NC3 has faced a growing array of non-kinetic threats capable of undermining the United States' nuclear forces in ways that previously only nuclear weapons could. While some non-kinetic threats predate the deployment of nuclear weapons (Take for example, "insider threats" posed by

[42] According to Wired magazine, "Zero-day vulnerability refers to a security hole in software—such as browser software or operating system software—that is yet unknown to the software maker or to antivirus vendors." A zero-day exploit takes advantage of vulnerabilities known only to attackers. See Kim Zetter, "Hacker Lexicon: What is a Zero Day?" *Wired*, November 11, 2014, https://www.wired.com/2014/11/what-is-a-zero-day/.

[43] Liu Caiyu,"Chinese Academician Warns of 'Nuclear-Bomb Like Cyber Attack' from US Against 5G," *Global Times,* August 5, 2020, https://www.globaltimes.cn/content/1196855.shtml; Martin C Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica, CA: RAND Corporation, 2013), https://www.rand.org/pubs/research_reports/RR175.html.

foreign agents planted to spy or sabotage operations.), most non-kinetic threats are becoming more pervasive, undetectable, and advanced, posing a greater risk to NC3 than in previous decades.

4. Relevant Literature

Articles and studies directly addressing the deterrence of below-the-threshold threats to NC3 have yet to be published. Discussions on non-kinetic threats to NC3 have focused largely on "cyber" threats but have failed to identify a shared definition of "cyber," while also neglecting other non-kinetic threat vectors. Literature on cyber threats to NC3 (however variably they are defined) has been limited to risk reduction, concentrating on subjects such as network intrusions or system malfunctions that could cause unintended escalation toward armed conflict.[44] Another body of literature has focused on modernization and the design of the United States' "Next Generation" NC3 architecture.[45] Overall, the conversation has thus far failed to address the ways in which rational state actors might be incentivized to interfere in NC3 using non-kinetic means.

This literature review begins by discussing relevant work on the so-called "gray zone" and the compelling incentives for rational state actors to conceal their actions and identity. Next, it discusses deterrence theory and its limitations. Finally, it evaluates an emerging discourse on cyber deterrence, which, although it does not deal directly with threats to NC3, is a valuable point of reference when considering why deterring non-kinetic attacks on nuclear assets is currently an unreasonable goal.

A. The "Gray Zone," Calculated Risk, and Secrecy

While not oriented toward challenges facing NC3, there is a sizable body of literature discussing malicious activity below the threshold of armed conflict. Scholars and officials alike

[44] Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences* (London, UK: Chatham House, January 2018), https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf; Paige O. Stoutland and Samantha Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group* (Washington, DC: NTI, September 2018), https://media.nti.org/documents/Cyber_report_finalsmall.pdf; Debra Decker et al., *Nuclear Cybersecurity Risks and Remedies,* (Vienna, Austria: Fissile Materials Working Group, Stimson, March 2019), https://armscontrolcenter.org/wp-content/uploads/2019/03/FMWG_CyberReport_webready.pdf.

[45] James Acton, "Command and Control in the Nuclear Posture Review: Right Problem, Wrong Solution," *War on the Rocks,* February 5, 2018, https://warontherocks.com/2018/02/command-and-control-in-the-nuclear-posture-review-right-problem-wrong-solution/; Jared Dunnmon, "Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace," Project on Nuclear Issues, 15-31 (Washington, DC: CSIS, Lanham, MD: Rowan & Littlefield, 2017), https://www.csis.org/programs/international-security-program/project-nuclear-issues; David Deptula, William A. LaPlante, and Robert Haddick, *Modernizing US Nuclear Command, Control and Communications* (Arlington, VA: The Mitchell Institute for Aerospace Studies and The MITRE Corporation, February 14, 2019), https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_ed45cfd71de2457eba3bcce4d0657196.pdf; John R Harvey, "US Nuclear Command and Control for the 21st Century."

have voiced their concern that adversaries can challenge the U.S. using non-kinetic means, achieving their objectives without provoking a full-scale war.[46] Such aggression was characterized in 1948 by George Kennan as "political warfare," but today's analysts might venture to call it "gray zone conflict" [47] or "hybrid warfare."[48] Will Spears points out the fleeting nature of such terms, arguing that these concepts can be more "accurately regarded as [a] characteristic of warfare" or a description of a problem, rather than a solution.[49]

Setting aside contested terminology, literature on the so-called gray zone yields one significant insight: when adversaries desire to prevent armed conflict while continuing to extract benefits, they take calculated risks below a perceived threshold and often endeavor to obscure their actions. Alexander Lanoszka argues that especially in the case of states such as Russia, which has inferior conventional forces, "Not having global escalation dominance means that the belligerent wishes to contain the conflict" while altering the status quo.[50] Lanoszka is clear that weaker powers have a greater incentive to use non-kinetic tools to their advantage, fearing armed confrontation with more powerful militaries.

Secrecy is central to obfuscation of responsibility for below-the-threshold aggression. A relatively new body of literature examines the incentives for rational actors to conceal or reveal "clandestine capabilities," which Austin Long and Brendan Rittenhouse Green have coined to mean "elements of military power" that "depend on secrecy for their battlefield effectiveness."[51] Long and Rittenhouse Green find that states will only reveal an advantage if the benefits of doing so outweigh the costs. If states judge that the adversary will respond punitively, or if they judge that any given capability is "unique," meaning that the holder of that capability would fear permanently losing it if revealed, they will have a minimal incentive to reveal that advantage in peacetime scenarios.[52] If they are accurate, these findings have profound implications for future analysis of below-the-threshold threat to NC3. Due to the highly sensitive nature of nuclear assets whether in peacetime or wartime, adversaries wishing to compromise NC3 will have a significant

[46] See U.S. Army, *The U.S. Army in Multi-Domain Operations 2028.* 525-3-1, Washington, DC: TRADOC, 2018. https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028.

[47] James Andrew Lewis, *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (Washington, DC: CSIS, Lanham, MD: Rowan & Littlefield, 2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf.

[48] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no. 1 (January 2016): 189, doi: 10.1111/1468-2346.12509.

[49] Will Spears, "A Sailor's Take on Multi-Domain Operations," *War on the Rocks*, May 21, 2019, https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/.

[50] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Eeterrence in Eastern Europe."

[51] Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (Winter 2019/20), 48, doi.org/10.1162/ISEC_a_00367.

[52] Ibid., 59.

incentive to conceal their actions. Furthermore, the capability to significantly undermine an adversary's NC3 would certainly qualify as "unique."

Overall, the literature on gray zone conflict and clandestine capabilities suggests an incentive for adversaries to work below the threshold of armed conflict to secure their objectives while eschewing accountability. Although descriptions of this problem abound, solutions are scarce. Existing literature does not argue convincingly for the effectiveness of deterrence as a mitigating strategy, if only because deterring below the threshold is a challenge that has just recently been taken up by the scholarly community. Scholars have struggled to characterize nontraditional formulations of deterrence[53] that move beyond, for example, the deterrence of nuclear attack using nuclear weapons or of kinetic attack using kinetic weapons.

This paper argues that deterrence is an unproven strategy for managing below-the-threshold threats to NC3. The section below examines seminal literature on deterrence and identifying the basic criteria for a successful nuclear deterrence strategy. It then reviews more nascent literature on cyber deterrence, which, although it does not deal explicitly with NC3, is a springboard for questions on deterrence below the threshold.

B. Deterrence and its Limits

Thomas Schelling writes in his 1966 publication entitled *Arms and Influence* that deterrence is a type of *coercion* aimed at preventing certain behavior by adversaries.[54] Deterrent threats can take the shape of *denial* or *punishment*. Deterrence by denial is meant to prevent an adversary from acting by making a task so costly or labor-intensive that it becomes unattractive. Deterrence by punishment, on the other hand, aims to prevent undesired actions by threatening retaliation so severe that the benefits of any action would be dwarfed by the cost of punishment.[55] Deterrence stands in contrast to another type of coercion called *compellence*, which seeks to induce behavior or change an undesired behavior once it has already begun.[56] Coercion, encompassing both deterrence and compellence, is distinct from *brute force*, which simply overpowers an adversary's defenses, ignoring coercive threats and gaining an actor's compliance "by physically forcing him to do so."[57] See Figure 2.

[53] Beyond inconclusive literature considering deterrence across the US military's domains of battle (e.g., air, land, sea, space, cyberspace), most writing on deterrence takes place within compartmentalized scholarly communities, impeding cross-pollination among various strands of deterrence theory. See Eric Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019), doi: 10.1093/oso/9780190908645.001.0001.

[54] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2020).

[55] Richard K Betts, "The Lost Logic of Deterrence: What the Strategy that Won the Cold War Can--and Can't-- do Now," *Foreign Affairs* 92, no. 2 (March/April 2013), https://www.foreignaffairs.com/articles/united-states/2013-02-11/lost-logic-deterrence.

[56] Thomas C. Schelling, *Arms and Influence*, 69.

[57] Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979): 297, doi:10.2307/2009945.

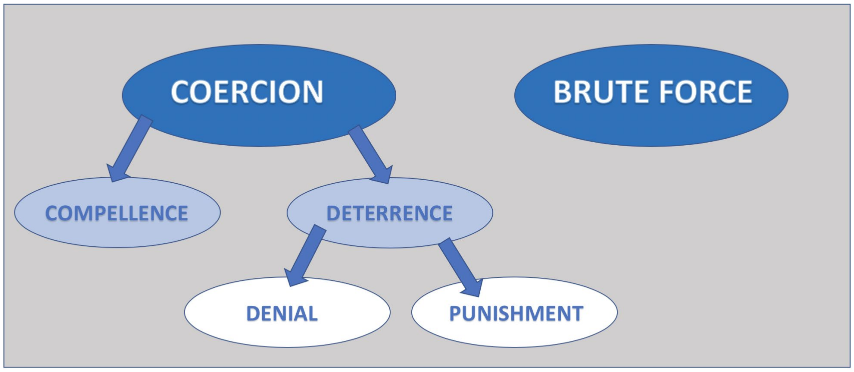

Figure 2. Conditions of Threat

Deterrence theory holds that a threat must play out under certain conditions in order to be successful. First, those involved will ideally be *rational actors*, intent on avoiding war if possible and open to the "feasibility of non-violence."[58] According to Schelling, deterrence must involve the use of *credible threats*[59] and a *clear communication* of what must be done to avoid punishment.[60] Effective communication is needed to ensure that threats are "correctly perceived" and that the adversary understands that "by undertaking the prohibited action he will incur substantial loss, or that by not undertaking it he can make a substantial gain."[61] Defense experts note in the 2009 document *America's Strategic Posture* that "while an element of *calculated ambiguity* remains essential, there should be enough clarity that potential foes will be deterred."[62] Overall, deterrence must exploit an understanding of *"enemy wants and fears,"* demonstrating the *resolve* and *capability* to carry out believable threats.[63]

Scholars continue to disagree about how and whether deterrence works, and indeed it is typically impossible to tell with great certainty. Cold War nuclear deterrence was far from straight-forward and, in fact, was forged slowly, through constant iterations of policy. Historian Frank Gavin aptly summarizes the barriers to studying nuclear war and deterrence, arguing that "explaining why something has never happened is difficult and at best speculative." Gavin notes that claims about deterrence are based upon immeasurable and subjective qualities, such as "fear,

[58] Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (February 2019): 5, doi: 10.1080/01402390.2018.1563779.

[59] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University, 1980), 187, and Thomas C. Schelling, *Arms and Influence*, 3.

[60] Thomas C. Schelling, *Arms and Influence*, 56.

[61] Naval Studies Board, *Post-Cold War Conflict Deterrence* (Washington, DC: National Academy Press, 1997), https://doi.org/10.17226/5464.

[62] Ibid., 36.

[63] Thomas C. Schelling, *Arms and Influence*, 3.

uncertainty, and resolve." Without agreed methods of quantifying and assessing these qualities, Gavin argues, it is difficult to make factual claims about them.[64]

Throughout the nuclear era, assumptions about nuclear weapons and their utility were frequently upended. At the outset of the Cold War, U.S. leaders such as Gen. Curtis LeMay viewed nuclear weapons as a type of cure-all, advocating for their deployment to manage a multitude of varied threats. America quickly learned, however, that nuclear weapons were far from an all-encompassing deterrent. During the Korean War, they proved to be "slippery tools of statecraft" and an ineffective means of deterrence, creating "more responsibility for restraint than disposable power."[65] Recent work by political scientist Vipin Narang asserts not only that "not all nuclear postures deter equally well," but also that "nuclear weapons do not ipso facto deter conventional conflict."[66]

The unpredictability of deterrence strategies is apparent in Robert McNamara's account of the Cuban Missile Crisis. McNamara recalls that incomplete information and human fallibility nearly caused a nuclear war. The crisis occurred in 1962, yet today the U.S., Russia, and Cuba continue to learn and share new information about the event, revealing the extent of misperceptions and solidifying that, in heated crises, leaders can never be certain of their immediate impressions.[67]

French theorist Benoit Pelopidas attributes the prevention of disaster largely to luck, stating that a war was avoided "not through restraint on the part of President Kennedy and the Soviet leadership only, but as a result of decisions made by individual nuclear operators, under conditions of incomplete or incorrect information."[68] Robert Jervis maintains that "It is hard to find cases of even mild international conflict in which both sides fully grasp the other's views."[69] Jervis and others confirm that deterrence is primarily about perception, which often differs vastly from reality and can vary based on each actor's self-centric worldview.

Despite over four decades of experience navigating nuclear tensions during the Cold War, deterrence remains an imperfect instrument with uncertain effects—a useful lesson when considering emerging theories such as cyber deterrence. Still, the deterrence of nuclear attacks using nuclear weapons holds the obvious outcome that, if deterrence fails and nuclear weapons are

[64] Francis J Gavin, "We Need to Talk: the Past, the Present, and Future of the U.S. Nuclear Weapons Policy," *War on the Rocks*, January 2, 2017, https://warontherocks.com/2017/01/we-need-to-talk-the-past-present-and-future-of-u-s-nuclear-weapons-policy/.

[65] Roger Dingman, "Atomic Diplomacy During the Korean War," *International Security* 13, no. 3 (Winter 1988): 91, muse.jhu.edu/article/446784.

[66] Vipin Narang, "What Does It Take to Deter? Regional Power Nuclear Postures and International Conflict," *The Journal of Conflict Resolution* 57, no. 3 (June 2013): 500, http://www.jstor.org/stable/23414723.

[67] Robert S. McNamara, "Apocalypse Soon," *Foreign Policy,* October 21, 2009, https://foreignpolicy.com/2009/10/21/apocalypse-soon/.

[68] Benoît Pelopidas, "The Unbearable Lightness of Luck: Three Sources of Overconfidence in the Manageability of Nuclear Crises," *European Journal of International Security* 2, no. 2 (2017): 244, doi:10.1017/eis.2017.6.

[69] Robert Jervis, "Deterrence Theory Revisited."

used, that action cannot be hidden from the world. As the following section will examine, it is much more arduous to trace individual actions in cyberspace, a fact that poses significant challenges to cyber deterrence.

C. Cyber Deterrence: The New Kid on the Block

Scholar Alex Wilner observes that, compared to conventional and nuclear deterrence theory, "cyber deterrence theory is still in its messy infancy," with most literature having appeared within the last decade and a half. In Wilner's words, "U.S. cyber deterrence practice outpaces cyber deterrence theory," meaning that "tactics, strategy, doctrine, and policy have been developed... before corresponding theories from academia are properly understood..."[70] Like nuclear deterrence theory, cyber[71] deterrence theory is challenged by a lack of empirical data, especially as it pertains to wartime; just as a full-scale nuclear war has never been fought, the world has not yet seen what war featuring unconstrained use of cyber weapons would look like.

Despite the fact that cyber deterrence is a hotly contested concept, most scholars are united around a few shared beliefs. Many agree, for example, that any attempt at cyber deterrence would be complicated by the impossibility of perfect defenses and the advantages often possessed by offensive actors; the constantly evolving nature of cyberspace; the anonymity of actors; the resulting challenge of attribution, although its speed and accuracy are improving; the uncertainty of any action and its potential collateral damage; the difficulty of distinguishing between espionage and intent to sabotage; the sheer number of actors in cyberspace and proliferation of advanced offensive cyber tools; the lack of geographic boundaries; and finally, the inability of actors to sustain a prolonged advantage.

Scholars are further unified by a commonly held view that, while it may be possible to dissuade hostile activity in a *general* sense, it is extremely difficult to trace the effects of singular acts in cyberspace. Scholars differ in their views on how to articulate this belief, with some considering a general dissuasion of aggression to constitute deterrence and others not.

Michael Fischerkeller and Richard Harknett, for instance, contend that "within cyberspace the protection or advancement of national interests cannot rest on deterrence..."[72] Instead, they advocate for "persistent engagement," an approach which became the basis for U.S. Cyber

[70] Alex S Wilner, "US Cyber Deterrence: Practice Guiding Theory," 3.

[71] While this paper avoids broad use of "cyber" as a term, the literature on cyber deterrence employs it frequently. Joseph Nye writes that "Analysts use the prefix 'cyber' to refer to a variety of digital, wireless, and computer-related activities." Within cyber deterrence literature, "cyberattack" tends to refer to the use of any number of means (e.g., supply chain breaches, malicious insiders, remotely executed network intrusions) to degrade or extract intelligence from information technology systems. See Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016): 44-71, https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

[72] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no.3 (2017): 391-393, https://doi.org/10.1016/j.orbis.2017.05.003.

Command's (CYBERCOM) 2018 vision statement.[73] The document summarizes persistent engagement as follows:

> "Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate—globally, as close as possible to adversaries and their operations. It describes when we operate—continuously, shaping the battlespace. It describes why we operate—to create operational advantage for us while denying the same to our adversaries."[74]

In a scholarly companion piece to the CYBERCOM vision statement, Fischerkeller and Harknett affirm the need to "increase resiliency, defend forward as close as possible to the origin of adversary activity, and contest cyberspace actors," which they believe will overall "generate continuous tactical, operational, and strategic advantage" despite the impossibility of deterring individual acts.[75] The statement reflects their belief that, while deterrence is incompatible with cyberspace, it is possible over time to generate an "advantage," convincing adversaries (if even momentarily) that it is not worth their time and resources to provoke the U.S.

Joseph Nye criticizes persistent engagement, calling it a "truncated concept of deterrence that places too much emphasis on the dimension of retaliation and denial."[76] Nye maintains that cyber deterrence is ill-defined but alive and well, noting his belief that it is "possible to reduce the likelihood of adverse acts causing harm in the cyber realm," even if no ideal tool exists.[77] Such an approach would aim over time to "influence calculations of costs and benefits" to limit malicious activity while expecting some deterrence failures as an inevitability.[78] Additional calls for "cumulative" rather than "absolute" deterrence have been prominently featured in cyber deterrence literature.[79]

[73] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command" (Fort Meade, MD: US Cyber Command, 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[74] Ibid.

[75] Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*, IDA Document NS D-9076 (Alexandria, VA: Institute for Defense Analyses, 2018), https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

[76] See reference to email correspondence between Jason Healey and Joseph Nye in: Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): tyz008, https://doi.org/10.1093/cybsec/tyz008.

[77] Nye, Joseph. "Deterrence and Dissuasion in Cyberspace," 62.

[78] Ibid., 68

[79] Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* 40, no. 1-2 (December 2015): 92-117, doi: 10.1080/01402390.2015.1115975.

The DSB's 2017 *Task Force on Cyber Deterrence* offers an optimistic view, advocating for the use of deterrence by denial and punishment to prevent cyberattacks on the U.S. Much of the DSB's report focuses on potential tools for deterring cyberattacks, such as "diplomatic, economic, law enforcement, and military," while still acknowledging that "not all cyberattacks or costly intrusions will be deterrable." The report leans heavily upon nuclear deterrence theory, often overlooking qualitative differences between cyber and nuclear weapons. It ventures to assume, for example, the existence in cyberspace of a metaphorical "escalation ladder,"[80] which was first described in Herman Kahn's writings on nuclear war.[81] But war games have shown that escalation in the cyber domain does not comport with expectations derived from other types of confrontation.[82] The report's implication of an equivalence between cyber and nuclear weapons seems to ignore the possibility that deterrence may not be an appropriate tool for managing below-the-threshold aggression.

In a 2020 report by the Cyberspace Solarium Commission (CSC), created through the 2019 National Defense Authorization Act, experts and former officials advocate for a "layered" approach to cyber deterrence. Yet the report's three "layers" ("shape behavior," "deny benefits," and "impose costs") are simply the central tenets of deterrence theory as laid out by Schelling. Like other documents advocating for cyber deterrence, the CSC's report does little more than project the concepts of nuclear deterrence theory onto cyberspace, neglecting to prove that they are indeed transferrable.[83]

This review of literature on cyber deterrence affirms that although experts believe in the broad possibility of dissuasion, they struggle to articulate how individual acts might be deterred. Jason Healey writes in a 2018 Council on Foreign Relations blog that the first "well-documented instance of cyber deterrence" may have come in the form of President Obama's reluctance to respond to Russian interference in the 2016 election.[84] However helpful such accounts might be in starting to validate concepts of cyber deterrence, it is troubling that a seasoned cyber policy expert can only identify a single potential example of cyber deterrence. In this case and others, the parties involved did not communicate their deterrence strategies if they even had any. The *impact* of Russia's actions is unclear (President Obama may have refrained from responding due to domestic political

[80] United States Department of Defense and United States Defense Science Board, *Task Force on Cyber Deterrence (*Washington, DC: Department of Defense, February 2017).

[81] Herman Kahn*, On Escalation: Metaphors and Scenarios*. Introduction by Thomas C. Schelling (London, UK: Routledge, July 2017).

[82] Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects Based Logic," *Journal of Cybersecurity* 5, no. 1 (September 2019): 4. doi: 10.1093/cybsec/tyz007.

[83] United States Cyberspace Solarium Commission, *United States of America Cyberspace Solarium Commission* (n.p., March 2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[84] Jason Healey, "Not the Cyber Deterrence the United States Wants," *Council on Foreign Relations* (blog), June 11, 2018, https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants.

constraints rather than fear of further Russian aggression.), and it is questionable whether these events reveal cyber deterrence in action.

Those who believe cyber deterrence can be operationalized provide limited suggestions on how to implement such a policy or how its success would be measured. Wilner writes that "anonymity robs deterrence of its potency."[85] Notwithstanding a sizable debate about attribution of cyberattacks,[86] it is clear at least that the vastness of cyberspace, the low buy-in cost, the abundance of unidentified actors, and the temptation to test defenses would be significant barriers to effective deterrence.

[85] Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," 5

[86] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts" (Stanford, CA: Hoover Institution, September 2016), https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0; David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, IDA Paper P-3792 (Alexandria, VA: Institute for Defense Analyses, October 2003), https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf; David D. Clark. and Susan Landau, "Untangling Attribution," essay from Harvard Law School National Security Journal 2 (2011), https://harvardnsj.org/wp-content/uploads/sites/13/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf; Nicholas Tsagourias, "Cyber Attacks, Self-Defense and the Problem of Attribution," *Journal of Conflict & Security Law* 17, no. 2 (2012): 229–244, https://ssrn.com/abstract=253827; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (December 2014): 4-37, doi: 10.1080/01402390.2014.977382.

This page is intentionally blank.

5. Summary

This literature review has shown the compelling incentive for rational actors to take calculated risks, acting below a perceived threshold of war. Due to the sensitive nature of nuclear assets and the "uniqueness" of capabilities that undermine them, adversaries are likely to conceal attacks on NC3 unless they are intended to signal a message.

Deterrence is an imperfect instrument that has yet to bear the fruits of deterring non-kinetic threats, including cyberattacks. CYBERCOM's vision for persistent engagement that generates an "operational advantage" over time is not unlike Joseph Nye's assertion that, with patience, the U.S. government can cumulatively shape an adversary's "calculations of costs and benefits." Experts disagree, however, on whether to call this deterrence. Regardless, the literature reinforces that, in spite of high hopes for cyber deterrence, it has so far created many more questions than answers. Nye and others do not provide proof that the success or failure of a cumulative deterrence strategy can be clearly traced; in the view of this paper, a cohesive deterrence strategy must have at least somewhat observable results so that it can be modified as necessary.

The next chapter will (1) examine non-kinetic threats to NC3 in depth and (2) explain why below-the-threshold threats conflict with deterrence as a mitigating strategy. Subsequently, this paper argues for an alternative vision to deterrence, placing an emphasis on the practical aspects of resilience to non-kinetic threats. Finally, it offers policy recommendations and considers areas for further research.

This page is intentionally blank.

6. Analysis

Non-kinetic, below-the-threshold threats to NC3 are examined here in detail. To provide clarity and specificity, the below devotes individual attention to five key areas: cyber network intrusions, electronic warfare, supply chain infiltration, disinformation, and insider threats.

In spite of their qualitative differences, these potential threats to NC3 share five characteristics:

- The **threshold of armed conflict, as it pertains to these tools, is undefined,** leaving non-kinetic attacks on NC3 in murky waters. It is not clear which uses of these tools, if any, constitute hostility under international law, or how governments view this question. The use of these tools, if done with restraint, can fall safely short of war.
- At the same time, all of these tools can have the **equivalent of kinetic effects** on NC3, constituting a strategic attack. According to the DOD, "strategic" refers to "the highest level of an enemy system that, if degraded, will contribute most directly to the achievement of our national security objectives."[87]
- When using these tools, adversaries can **evade detection or attribution**, making their actions difficult to characterize. When aiming to undermine NC3, adversaries will have a significant incentive to act covertly.
- With a number of new actors employing these tools today, there is a **lack of norms** for responding to their use and a likelihood that they will continue to proliferate.
- All of these tools are **used frequently in peacetime** and have historically been employed without provocation of armed hostilities.

Below, I describe each potential non-kinetic threat to NC3, addressing seven questions for each vector:

1. **DEFINITION:** How is this tool defined?
2. **EFFECTS:** What effects can this tool generate? How severe and/or reversible are those effects?
3. **INCENTIVES:** What are the incentives for a rational actor to use this tool to undermine NC3, both in peacetime and wartime?

[87] Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: Joint Chiefs of Staff, January 2017), https://www.jcs.mil/Doctrine/DOCNET/JP-3-0-Joint-Operations/.

4. **PROMINENCE:** How common is this tool/tactic? Are there any significant barriers to its proliferation?
5. **ATTRIBUTION:** How difficult is it to attribute malicious applications of this tool?
6. **COUNTERMEASURES:** If the use of this tool is discovered, can the target quickly implement countermeasures?
7. **EXAMPLES:** What are the most prominent examples of the hostile use of this tool? (All examples of non-kinetic actions given below are based on incidents reported either in the media or by governments. In some cases, it is impossible to verify the validity of these accounts. This paper takes such accounts at face value but recognizes that new details may emerge.)

This analysis hopes to offer an exhaustive overview of all potential non-kinetic means for adversaries to undermine NC3, recognizing, of course, that new threats will continue to arise. In determining the proper grouping and description of non-kinetic threats, the author avoids referring broadly to "cyber" threats. Thus far, the nuclear policy community lacks a shared definition of "cyber" as a term, a fact which has stifled productive debate and calls for clarification. Moreover, a singular focus on "cyber" threats has excluded other non-kinetic threat vectors. For instance, acknowledgment of the deep reliance between the electromagnetic spectrum and computer networks is noticeably absent in recent open sources literature.

Following an in-depth examination of non-kinetic threats to NC3, analysis will support that deterrence is not the right strategy to address them.

CYBER NETWORK INTRUSIONS

DEFINITION: Intrusions into cyber networks can be categorized as either a Cyber Network Attack (CNA) or Cyber Network Exploitation (CNE). The DOD defines CNA as "the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[88] The DOD has defined CNE as "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks."[89]

[88] Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington, DC: Joint Chiefs of Staff, February 2006), https://www.hsdl.org/?view&did=461648.

[89] Joint Chiefs of Staff, *Department of Defense: Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: Joint Chiefs of Staff, November 2010), https://fas.org/irp/doddir/dod/jp1_02.pdf; Note: The US military no longer officially uses CNE as a term, but its use continues outside of government and in the expert community. https://csrc.nist.gov/glossary/term/computer_network_exploitation.

EFFECTS: The effects of a cyber network intrusion are sometimes reversible or reparable, but they can take days or weeks to fix and can cause massive financial damage or loss of classified information. In other cases, they cause permanent and even unintended damage.

INCENTIVES: In peacetime, adversaries might find network intrusions useful for gathering information or degrading NC3 without provoking full-scale conflict. In wartime, network intrusions might accompany or enhance kinetic operations. It is possible that malware embedded covertly in a network during peacetime could be used to provide kinetic advantages during wartime. (Although not accompanied by a formal declaration of war, a relevant instance of this is the Israeli government's alleged introduction of a Trojan horse into the computer of a Syrian government official months before Israel bombed a Syrian nuclear facility, using the malware to disable Syrian air defenses on the day of the bombing.[90])

PROMINENCE: DOD networks come under attack millions of times per day.[91] Although the vast majority of attempts are unsuccessful, this fact underscores the sheer volume of malicious activity in cyberspace targeting the U.S. government. As a tool, so-called cyber weapons are relatively cheap and not yet restricted by arms control agreements or export controls, meaning that cyber weapons have proliferated quickly and will likely continue to do so.[92] Knowledge required to create advanced cyber weapons can spread quickly, as was the case with "Project Raven," an initiative that saw several ex-NSA employees use their years of training to create malware for the United Arab Emirates (UAE), which ultimately used it to spy on citizens of the UAE and the US. Prior to receiving contractors' assistance, the UAE did not have the capability to carry out sophisticated cyberattacks.[93]

ATTRIBUTION: Attribution of malicious cyber network intrusions is a constantly evolving challenge. As Herbert Lin of the Hoover Institution notes, states are getting better at attributing

[90] Jim Michaels, "U.S. Could Use Cyberattack on Syrian Air Defenses," *USA Today*, May 16, 2013), https://www.usatoday.com/story/news/world/2013/05/16/syria-attack-pentagon-air-force-military/2166439/.

[91] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[92] Daniel Hughes and Andrew M. Colarik, "Predicting the Proliferation of Cyber Weapons into Small States," *Joint Force Quarterly* 83, no. 4 (2016): 19-26, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-83/jfq-83_19-26_Hughes-Colarik.pdf?ver=2016-10-19-102201-033.

[93] Robert Chesney, "Project Raven: What Happens When U.S. Personnel Serve a Foreign Intelligence Agency?" *Lawfare* (blog), February 11, 2019, https://www.lawfareblog.com/project-raven-what-happens-when-us-personnel-serve-foreign-intelligence-agency.

malicious attacks and simultaneously improving their capacity to deceive, confusing attribution efforts. The greatest barrier to effective attribution is time.[94]

COUNTERMEASURES: If an intrusion into relevant networks is detected, responses may include patching to address vulnerabilities, using honeypots to confuse perpetrators, taking subsystems offline to limit further damage, or attempting to identify the intruder and attack back.[95]

EXAMPLES: Cyber network intrusions occur in such great volume that they are impossible to count. While many are merely irritating, some have more serious impacts. These include attacks allegedly staged by Russia, both in 2007 when Estonia's internet was disabled[96] and in 2015 when large portions of Ukraine's electrical grid were shut down, leaving thousands of Ukrainians without power.[97] Recent research reveals that the latter may have been intended to cause permanent damage to Ukraine's grid, aiming to destroy physical components, rather than just corrupt and destroy data.[98] In 2018, hackers with a similar objective targeted oil company Saudi Aramco, attempting to trigger an explosion and destroy machinery vital to the company's operations.[99]

Russian and Chinese[100] hacking targets have consistently included high-level U.S. government entities and defense contractors with critical knowledge of U.S. weapons systems.[101] As is discussed separately below, often cyber network intrusions are facilitated by malicious insiders, who possess access to restricted and classified systems, or by way of the defense supply chain.

[94] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts."

[95] Ari-Veikko Anttiroiko and Mälkiä Matti, in *Encyclopedia of Digital Government* (Hershey, PA: Idea Group Reference, July 2006).

[96] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 8, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

[97] 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/.

[98] Ibid.

[99] Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

[100] United States Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" (Washington, DC: May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[101] Raphael Satter, Jeff Donn, and Justin Myers, "Digital Hit List Shows Russian Hacking Went Well Beyond U.S. Elections," *Chicago Tribune*, November 2, 2017, https://www.chicagotribune.com/nation-world/ct-russian-hacking-20171102-story.html.

ELECTRONIC WARFARE

DEFINITION: The DOD defines electronic warfare as "Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[102] The Congressional Research Service (CRS) further clarifies that electronic attack is meant to "degrade or deny an enemy's use of the spectrum."[103]

EFFECTS: Electronic attacks can be used to blind, disable, deceive, or permanently damage systems. Severity of effects can vary. Jamming, for example, is reversible, and full function of a system can be restored once the jammer is out of range or otherwise disengaged. Spoofing is also usually reversible, but it can have damaging effects whose results may be irreversible.[104]

INCENTIVES: In peacetime, adversaries are likely to avoid electronically attacking systems they perceive to be critical. They are more likely to experiment with low stakes jamming, targeting less sensitive systems. In wartime, it is likely that adversaries would use electronic capabilities to blind, temporarily disable, or confuse U.S. systems that would be off-limits during peacetime.

PROMINENCE: The May 2020 document Joint Electromagnetic Spectrum Operations states, "Advances in electromagnetic spectrum (EMS) technologies over the last few decades have led to an exponential increase in civil, commercial, and military EMS-enabled and dependent capabilities. This proliferation, coupled with the U.S. military's critical reliance on the EMS and the low entry costs for adversaries, pose significant military challenges."[105] The rise in advanced EMS capabilities has prompted the U.S. military to shift its attention back to electronic warfare.[106]

[102] Joint Chiefs of Staff. *Department of Defense: Dictionary of Military and Associated Terms*.

[103] Congressional Research Service, *Defense Primer: Electronic Warfare*, § updated October 2019, https://fas.org/sgp/crs/natsec/IF11118.pdf.

[104] Tyler Way, "Counterspace Weapons 101," *Aerospace Security*, July 23, 2020, https://aerospace.csis.org/aerospace101/counterspace-weapons-101/.

[105] Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations,* Joint Publication 3-85 (Washington, DC: Joint Chiefs of Staff, May 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347.

[106] Sydney J. Freedberg Jr., "Electronic Warfare: Better, But Still Not Good Enough," *Breaking Defense*, November 1, 2019, https://breakingdefense.com/2019/11/electronic-warfare-better-but-still-not-good-enough/.

ATTRIBUTION: The ability to attribute electronic attacks depends on the type of attack and the system it targets. According to Tyler Way of the Center for Strategic and International Studies (CSIS), attributing jamming is complicated because "the source can be small and highly mobile."[107] Way specifies that "Unlike jamming, spoofing can subvert the loss-of-signal alarm system by fooling the system into believing that the fake signal is in fact real." This makes attribution of spoofing even more difficult.[108] In a contested battle space involving multiple actors, it is difficult to identify the source of jamming and spoofing.

COUNTERMEASURES: If the hardening of NC3 and use of emission control is ineffective, potential responses include attacking back (e.g., jamming), taking subsystems offline, or using deception to "spoof" enemy systems.

EXAMPLES: Gen. Raymond Thomas, former Commander of U.S. Special Operations Command, stated in 2018 that Syria was "the most aggressive EW [electronic warfare] environment on the planet." Gen. Thomas complained that Russian forces were "testing us every day, knocking our communications down, disabling our EC-130s, etcetera."[109] Russian jamming has also allegedly targeted American F-22s and F-35s in the Middle East,[110] as well as shut down cellular and radio networks in Ukraine.[111] While electronic attacks by China are less documented, there is speculation that the Chinese government may be testing its newest electronic warfare capabilities on ships in the Port of Shanghai.[112] In 2018, it was reported that China installed jamming equipment on the Spratly Islands in the South China Sea.[113]

[107] Tyler Way, "Counterspace Weapons 101."

[108] Ibid.

[109] Colin Clark, "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria," *Breaking Defense*, April 24, 2018, https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.

[110] Arie Egozi, "Why Would Russia Spoof Israeli GPS? F-35 & Iran," *Breaking Defense*, June 28, 2019, https://breakingdefense.com/2019/06/if-russia-is-spoofing-israeli-gps-then-why-iran-f-35/.

[111] Sébastien Roblin, "Electronic Warfare: The U.S. Is Losing the Invisible Fight to Russia's Dominant Capabilities," *NBC News*, November 26, 2019, https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101.

[112] Joseph Trevithick, "New Type of GPS Spoofing Attack In China Creates 'Crop Circles' Of False Location Data," *The Drive*, November 18, 2019, https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data.

[113] Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," *The Wall Street Journal*, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320.

SUPPLY CHAIN INFILTRATION

DEFINITION: The U.S. intelligence community defines the supply chain as "Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of [information and communications technology] products and services and extends through development, sourcing, manufacturing, handling, and delivery of [information and communications technology] products and services to the acquirer."[114] The DSB notes that supply chain infiltrations can take place in the form of "malicious insertion of defect or malware" or "exploitation of latent [supply chain] vulnerabilities." Such breaches can take place during acquisition or sustainment of weapon systems.[115]

EFFECTS: According to the DSB, "system configurations typically remain unchanged for very long periods of time," meaning that "compromising microelectronics can create persistent vulnerabilities." When the supply chain is compromised, "exploitation of vulnerabilities... can cause mission failure in modern weapon systems," which "have depended on microelectronics since the inception of integrated circuits over fifty years ago."[116]

INCENTIVES: In peacetime, the successful implantation of corrupted parts can aid adversaries in espionage efforts or can actively compromise the functionality of U.S. weapon systems. During wartime, supply chain breaches perpetrated at an earlier time could provide adversaries with a kinetic advantage, allowing them to sabotage U.S. weapon systems.

PROMINENCE: According to Symantec, supply chain attacks increased by 78% in 2018.[117] In a 2018 survey by CrowdStrike fielded to 1,300 senior IT decision-makers across industry in the US, UK, Canada, Mexico, Australia, Germany, Japan, and Singapore, two-thirds of respondents said that their organization had suffered from a software supply chain attack.[118]

[114] John Boyens, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations."

[115] United States Defense Science Board, *DSB Task Force on Cyber Supply Chain (*Washington, DC: Office of the Under Secretary of Defense, February 2017), https://www.hsdl.org/?view&did=799509.

[116] Ibid.

[117] *Internet Security Threat Report*. Symantec Corporation, February 2019. Accessed September 2021, https://docs.broadcom.com/doc/istr-24-2019-en.

[118] "Securing the Supply Chain," VansonBourne, Crowdstrike.com, July, 2018, https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf.

ATTRIBUTION: The DSB laments the difficulty of attributing supply chain breaches, stating that "when done effectively, malicious insertion will not be detectible until actuated..."[119] The DSB elaborates that supply chain breaches "can be difficult to distinguish from electrical or mechanical failures... because effects can run the gamut from system degradation to system failure to system subversion."[120]

COUNTERMEASURES: A proactive approach to addressing supply chain threats is preferable. Once corrupted parts are discovered, it is difficult to know the extent of the problem and retroactively address the damage. The DSB recommends implementing a plan that tracks the fidelity and security of the defense supply chain throughout the entire lifecycle of any given weapon system. This includes performing regular vulnerability assessments.[121]

EXAMPLES: Supply chain breaches perpetrated by nations are not well documented in the public record. Most relevant references are nondescript statements, such as the one made in 2019 by Defense Logistics Agency director Lt. Gen. Darrell Williams when he recalled that an unidentified group of vendors had inserted "nonconforming parts" into the defense supply chain.[122] The DSB affirms that "it is difficult to know whether such activity is widespread."[123] However, a cursory glance at the global defense supply chain leaves ample room for concern. Take, for example, the Taiwan Semiconductor Manufacturing Company,[124] which produces half of the world's computer chips, including those used in the American F-35 fighter jet, Apple devices, and telecommunications technologies for Huawei, a company that has come under intense scrutiny for its dubious ties to the Chinese government.[125]

[119] United States Defense Science Board, *DSB Task Force on Cyber Supply Chain.*

[120] Ibid.

[121] Ibid.

[122] Jill Aitoro, "US Logistics Boss Talks Risks to the Supply Chain and Protective Measures," *Defense News*, October 28, 2019), https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/.

[123] Ibid.

[124] Lauly Li and Cheng Ting-Fang, "Exclusive: Washington Pressures TSMC to Make Chips in US," *Nikkei Asia*, January 15, 2020, https://asia.nikkei.com/Business/Technology/Exclusive-Washington-pressures-TSMC-to-make-chips-in-US.

[125] Lauren Feiner, "U.S. Tightens Restrictions on Huawei Access to Technology and Chips," *CNBC*, August 17, 2020, https://www.cnbc.com/2020/08/17/us-to-tighten-restrictions-on-huawei-access-to-technology-chips-sources-say.html.

DISINFORMATION

DEFINITION: CRS defines disinformation as the act of spreading "intentionally false" information. Some examples are "planting deliberately false news stories in the media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release."[126]

EFFECTS: At the societal level, disinformation campaigns can cause distrust in democracy, aggravate preexisting social or political divisions, and alter the outcome of democratic processes such as elections.[127] Within the narrow context of sensitive military operations, disinformation might target individual operators, affecting their ability to maintain situational awareness and carry out their duties based on credible information.[128]

INCENTIVES: In peacetime, adversaries can use disinformation campaigns to create a sense of uncertainty and division, undermining trust in governments and institutions. In wartime, disinformation could be used to confuse leaders and operators, complicating military planning by lengthening the process that is required to vet intelligence and make critical decisions.

PROMINENCE: Disinformation operations are growing in their scope and severity. A 2019 study by the University of Oxford found that "media manipulation campaigns" had happened in up to 70 countries, a number that grew from 48 countries in 2018 and just 28 in 2017. Seven countries have used social media for foreign influence operations to achieve their political aims.[129]

ATTRIBUTION: According to the Department of Homeland Security, "Attributing a targeted disinformation campaign to a specific threat actor is often a painstaking process. Developments

[126] Catherine A. Theohary, "Information Warfare- Issues for Congress," report no. R45142 (Washington, DC: Congressional Research Service, March 2018).

[127] Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue*, Analytic Exchange Program, October 2019, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

[128] Marta Kepe, "NATO: Prepared for Countering Disinformation Operations in the Baltic States?" RAND Corporation, June 7, 2017, https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.html.

[129] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," working paper at The Computational Propaganda Project (University of Oxford, UK: September 26, 2019), https://comprop.oii.ox.ac.uk/research/cybertroops2019/.

in technology and tactics that help mask the identity of threat actors outpace developments in technology and tactics that unmask these threat actors, especially as threat actors become more adept at exploiting authentic users."[130]

COUNTERMEASURES: With considerable success, the European Union has enlisted independent fact-checkers, among other methods, to counter disinformation.[131] In a paper on countering disinformation, the Brookings Institution recommends that governments "promotes news literacy and strong professional journalism in their societies."[132] However, in nations such as the U.S. where public trust in journalism is at an all-time low[133] and false information is sometimes spread by high-ranking government officials, it is difficult to establish and maintain public trust.

EXAMPLES: China is known to have interfered in Taiwan's presidential elections, using false claims on social media and Chinese news outlets.[134] Russian disinformation targets have included Ukraine, Georgia, Poland, Germany, Spain, the United Kingdom, Sweden, France, and the U.S., among many others.[135] Russia has also directly targeted the armed forces of NATO, the U.S., and Ukraine, most shockingly in 2018 when Russia sent fake texts to the family members of Ukrainian soldiers claiming, "Your son is killed in action." The result was a rush of worried phone calls to soldiers, which allowed the Russian military to pinpoint the location of a heavy concentration of cellphones, striking it with artillery shortly after.[136]

INSIDER THREAT

[130] Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue.*

[131] "Coronavirus: EU Strengthens Actions to Tackle Misinformation," *European Commission*, June 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006.

[132] Darrell M. West, "How to Combat Fake News and Disinformation," Brookings, December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

[133] Ibid.

[134] Joshua Kurlantzick, "How China Is Interfering in Taiwan's Election," *Council on Foreign Relations*, November 7, 2019, https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

[135] Maggie Tennis, "Russia Ramps up Global Elections Interference: Lessons for the United States," *Center for Strategic and International Studies*, July 20, 2020, https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states.

[136] Sébastien Roblin, "Electronic Warfare: The U.S. Is Losing the Invisible Fight to Russia's Dominant Capabilities."

DEFINITION: The National Insider Threat Task Force states that an insider threat is "posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource." Insider threats can cause "damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[137]

EFFECTS: The impacts of malicious insiders can range from the theft of information to damage of high-value systems.

INCENTIVES: In peacetime and in wartime, adversaries can use insiders for espionage or sabotage.

PROMINENCE: In a 2020 report, the Ponemon Institute noted a 31% increase in the average cost of insider threat incidents taking place in private industry from 2018 to 2020. The frequency of incidents rose 47% during the same timeframe.[138]

ATTRIBUTION: Once an insider threat is detected, attributing blame can be more difficult than one would expect. Unless security breaches can be attributed directly to an individual, it can be difficult to hold them to account. Investigations are often lengthy, and the threat may only become apparent when damage has already been done.

COUNTERMEASURES: Following a security breach by insiders, there is little to do beyond investigating the extent of damage and removing the threat(s). It is best to take a proactive approach, as is encouraged by the 2011 Executive Order (E.O.) 13587, which directed departments and agencies to develop programs for detecting and mitigating insider threats. To this end, the 2017 Insider Threat Guide compiles best practices, including actively cultivating a vigilant security culture and training staff to detect anomalous behavior.

[137] Department of Justice and NCSC, "National Insider Threat Task Force- Mission Fact Sheet," n.p.: n.d., https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

[138] Linn F. Freedman, "Frequency and Cost of Insider Threats Continue to Increase," *The National Law Review*, 9, no. 256 (September 2021), https://www.natlawreview.com/article/frequency-and-cost-insider-threats-continue-to-increase.

EXAMPLES: Two famous cyber network intrusions were likely perpetrated using insiders. In 2010, an insider brought malware called Stuxnet into the internal network of an Iranian nuclear facility using a USB flash drive, resulting in the destruction of a large percentage of Iranian nuclear centrifuges.[139] Not long after in 2012, oil company Saudi Aramco was breached by individuals suspected to be working for Iran, temporarily shutting down the company's operations. Investigators reported that the attack was almost certainly the work of insiders who possessed high-level access to Saudi Aramco's systems.[140]

There is a long history of spying by malicious insiders on U.S. nuclear programs, most famously in the 1940s by Klaus Fuchs, a lead Manhattan Project scientist and agent of the Soviets.[141] In the late 1990s, Los Alamos scientist Wen Ho Lee was accused of stealing nuclear secrets that were thought to have assisted China in developing the technology to miniaturize its nuclear weapons.[142]

In 2016, Chinese national Su Bin pleaded guilty to working with two unidentified insiders to access computer networks containing classified design information on the C-17, F-22, and F-35 aircrafts, which he then turned over to the Chinese government. The breach is credited with allowing China to exploit billions of dollars' worth of U.S. research and development to build similar aircraft for its own military.[143]

Each of the threat vectors above is qualitatively different, but each presents underlying similarities that make deterrence an unreliable strategy at present. To be clear, the greatest peacetime threats to NC3 are posed by cyber network intrusions, supply chain breaches, and insider threats, namely because vulnerabilities can be implanted for wartime exploitation. Disinformation is likely most effective in a wartime scenario, when the parties involved might act under pressure with less time to identify false claims.

At present, electronic warfare is also more applicable to wartime scenarios due to the fact that detection and attribution of electronic attack is easier than say cyber network intrusions. Unsurprisingly, electronic warfare is becoming increasingly sophisticated and convergent with cyber offensive capabilities. Some spoofing attacks are deceptive enough that they may be

[139] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[140] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[141] Marian Smith Holmes, "Spies Who Spilled Atomic Bomb Secrets," Smithsonian Magazine, April 19, 2009, https://www.smithsonianmag.com/history/spies-who-spilled-atomic-bomb-secrets-127922660/.

[142] Matthew Purdy, "The Making of a Suspect: The Case of Wen Ho Lee," *The New York Times*, February 4, 2001, https://www.nytimes.com/2001/02/04/us/the-making-of-a-suspect-the-case-of-wen-ho-lee.html.

[143] Jeffery B. Jones, "Confronting China's Efforts to Steal Defense Information" (Cambridge, MA: Belfer Center for Science and International Affairs, May 2020), https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

misidentified as system errors, and it is possible that future advances in electronic warfare will allow users to directly affect cyber networks. Thus, leaders should not rule out electronic attacks on NC3 in peacetime, especially as adversaries' electronic warfare capabilities become more advanced.

A. Why Deterrence Won't Work

Taken together, the threats to NC3 described above are not easily thwarted by deterrence for three key reasons:

1. Credible Threats

Deterrence rests on credible threats and the demonstrated capability to carry out those threats. Thus far, the U.S. has made no such credible threats to deter below-the-threshold attacks on NC3, stating only in the 2018 NPR that it would consider the use of nuclear weapons in "extreme circumstances" including "non-nuclear strategic attack." While openly hostile actions might be deterred by the NPR's statement, it does nothing to address more discreet non-kinetic acts, which can still seriously undermine the U.S. nuclear deterrent.

In order to deter below-the-threshold attacks on NC3 by punishment, the U.S. must specify credible response options, which to date, it has not done. For this and other reasons, CYBERCOM has embraced an alternative strategy of persistent engagement, which is purported to entail "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver."[144] Whether persistent engagement will succeed in generating an "advantage" in cyberspace is yet to be seen. Regardless, attempts to deter below the threshold have thus far fallen short, leaving policymakers with a lack of credible options either for deterrence by denial or punishment.

Central in the consideration of response options would be exploiting an understanding of "enemy wants and fears," ensuring that the costs of undermining NC3 outweigh potential benefits.[145] Due to their destructive power, nuclear weapons easily sway this calculus in favor of those that possess them. But when considering non-kinetic attacks on NC3, it is difficult to imagine a response that is both proportional and adequately fear-provoking. Precisely because they typically fall below the threshold of war, non-kinetic attacks provide assurance to adversaries that they will almost certainly avoid kinetic retaliation and other serious forms of punishment. Retaliating in kind, hitting back at enemy NC3 could be dangerously destabilizing and should not be normalized. Yet other response options may not be sufficiently fear-provoking to make costs outweigh benefits.

[144] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command."

[145] Thomas C. Schelling, *Arms and Influence*, 3.

Deterrence by denial is also an unappealing approach since it is difficult to convince adversaries that they should not test the strength of U.S. defenses. Even if the U.S. possesses strong defenses, they will still be constantly tested by adversaries, whose capabilities for non-kinetic attack will continually evolve and likely improve. If adversaries are unsuccessful in their attempts to break through U.S. defenses, it is not because they were *deterred* from acting; they simply faced resistance that prevented them from reaping benefits. The U.S. should expect that adversaries will continue to experiment with novel means of targeting NC3 below the threshold of war.

2. Detection and Attribution

To varying degrees, non-kinetic tools will allow an attacker to maintain anonymity and, in some cases, avoid detection. This analysis has demonstrated the significant incentive for adversaries to conceal their abilities to undermine NC3, as they fear both punishment and the relinquishment of a "unique" capability that is hard to duplicate. Thomas Schelling writes that a deterrent threat equates to "rigging the trip-wire,"[146] yet if unwanted actions cannot be detected and/or accurately attributed, the deterrer cannot credibly claim that she will be able to identify and punish those responsible. In other words, non-kinetic tools may allow adversaries to simply step over Schelling's "trip-wire." Furthermore, if discovered, breaches may be indistinguishable to the victim as either espionage or sabotage, making it unclear what the appropriate response should be. Indeed, an intrusion initially made for espionage purposes can be easily exploited for sabotage.

Issues of detection and attribution contribute to above questions regarding credible threats as well; a threat is far less believable if the deterring party cannot reasonably claim that it knows when its systems have been compromised or by whom. Returning to Schelling's delineation of *coercion* (including deterrence and compellence) and *brute force* (disregard for coercive threats that instead favors forcefully extracting benefits), it is possible that the tendency toward concealing one's actions, identity, and intent lends itself to brute force; if adversaries suspect that their attacks will go undetected, they can easily take what they want without asking, ignoring the potential consequences. If adversaries are intent on brute force, deterrent threats become a moot point.

3. Transparency Versus Ambiguity

Lastly, deterrent threats usually involve a degree of calculated ambiguity, while they also must be clear enough that they are not misinterpreted by adversaries. It is difficult to conceive of a statement that balances ambiguity and transparency while also convincing adversaries not to interfere in NC3 below the threshold of armed conflict. In constructing such a statement, the U.S. would need to maintain some amount of ambiguity to avoid drawing undesirable red lines. Tying its hands in relationship to NC3 could either be destabilizing, or, in the event of its failure to honor a red line, embarrassing and discrediting. But for the U.S. to be sufficiently clear about which particular actions it wished to deter, it would potentially need to breach sensitive and complex

[146] Ibid., 70.

subject matter; in addition to being highly classified, NC3 systems are sprawling, variegated, and entangled with conventional systems. To achieve clear communication with adversaries about a deterrent threat, the U.S. would walk a fine line between revealing too much or being so vague that adversaries either do not take threats seriously or severely misunderstand U.S. intent.

The above is not meant to entirely discount deterrence; as mentioned previously, the NPR's threat to respond to "non-nuclear strategic attacks" with nuclear weapons might successfully deter extremely hostile non-kinetic attacks. But in the event of such attacks, the U.S. would likely already be at war. The concern of this analysis is the range of actions that can take place below the traditional threshold of armed conflict and before overt aggression takes place. So, while deterrence might function as intended with regard to brazen hostilities, the point is that it is seemingly less useful at lower levels.

Additionally, it is possible that the U.S. may find some utility for *immediate deterrence* in isolated instances involving short-term goals to defend NC3. According to Michael Mazarr of RAND, immediate deterrence involves "urgent attempts to prevent a specific, imminent attack, most typically during a crisis."[147] In explaining immediate deterrence, Mazarr gives the example of preventing Soviet aggression against Berlin, whereas general deterrence took place "for decades by publicizing ongoing promises of defense and punishment if the Soviet Union attacked Western Europe."[148] In a crisis situation, desperate for solutions, the U.S. might attempt to use immediate deterrence to prevent specific behaviors. Although this research found no relevant examples of immediate deterrence below the threshold, it is possible that tracing the effects of an immediate deterrent threat would be simpler than tracking the broad success or failure of a general deterrence strategy.

Overall, however, deterrence of non-kinetic attacks is yet unproven and should not form the basis of the United States' strategy to defend NC3 short of war. Figure 3 shows that in peacetime, adversaries are likely to take calculated risks, targeting NC3 discreetly with non-kinetic tools; intervening factors would include the resilience of NC3 and a potential use of compellence or other alternative strategies to curtail unwanted behavior once an attack has been detected and attributed. During wartime, expected behaviors include direct provocation; to deter blatant hostilities at a high level, the U.S. employs a strategy of general deterrence, including through its willingness to respond with nuclear weapons. Of course, there is inevitable gray area, for instance with aggression that would be deemed an act of war by some leaders and not by others. Yet, in situations of unconcealed sabotage such as Scenario 2, the barrage of unconcealed non-kinetic attacks by Country Y is a far cry from the quietly implanted supply chain vulnerabilities in Scenario 1.

[147] Michael Mazarr, *Understanding Deterrence* (Santa Monica, CA: RAND Corporation, 2018), https://doi.org/10.7249/pe295.

[148] Ibid.

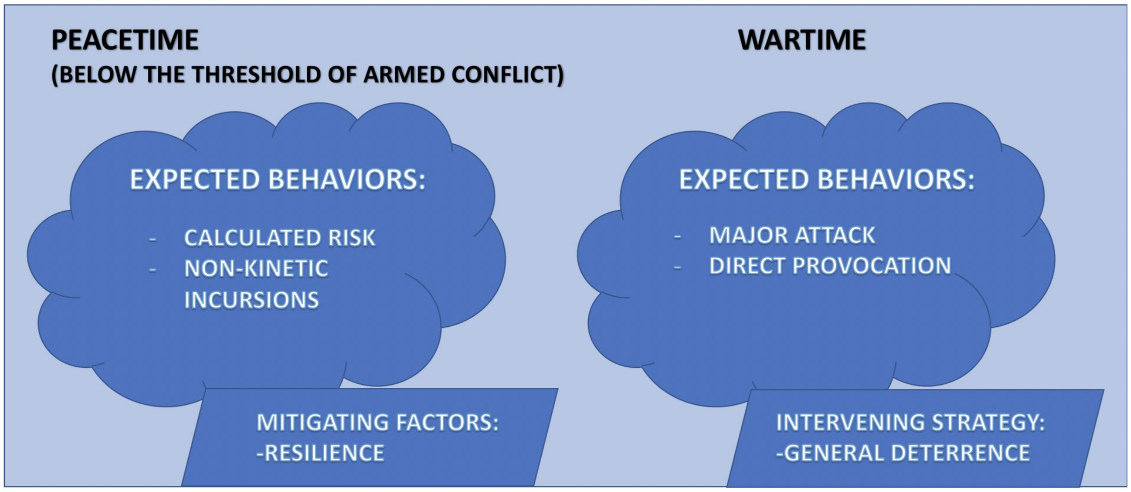

Figure 3. General Deterrence Preventing Large-Scale Kinetic Attacks

The following section argues for an emphasis on survivability and resilience when confronting non-kinetic threats to NC3, both in peacetime and in wartime. Given the high probability of continued attempts to undermine NC3 and low likelihood of deterring them, the U.S. must strive for resilience in the face of attacks, treating breaches as both inevitable and manageable.

7. Defending NC3 Below the Threshold

When it comes to securing NC3 against non-kinetic subversion, the U.S. should not rely on an unproven strategy of deterrence. Theories abound in the defense community, but various renderings of cross-domain deterrence, multi-domain deterrence, cyber deterrence, deterrence in the gray zone, and hybrid warfare have not yielded practicable suggestions for managing non-kinetic threats to NC3. Instead of relying on deterrent protection that may never materialize, U.S. policymakers should take a proactive approach to defending NC3 by (1) creating and implementing survivability and resilience standards to counteract the threat of non-kinetic attack at every stage of subsystem lifecycles and (2) actively searching for vulnerabilities in NC3, subjecting it to constant testing, red-teaming, and reassessment.

A. Actualizing Survivability and Resilience

The DOD defines survivability broadly as including "All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy."[149] A more specific definition appears in Ellison and Woody's widely consulted *Survivability Analysis Framework,* which holds that survivability is:

> "The ability for systems to withstand (i.e., "operate through") predicted and unpredicted adverse events and provides, at minimum, mission-critical functions throughout the event. The ability of a software-intensive space system to continue its mission, in a timely manner, in the occurrence of attacks, defects/vulnerabilities, accidents, or failures."[150]

According to the DOD, resilience is:

> "...the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is 'more resilient' if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats."[151]

[149] Joint Chiefs of Staff, *Joint Engineer Operations*, Joint Publication 3-34 (Washington, DC, January 2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_34.pdf.

[150] Robert J. Ellison and Carol Woody, "Survivability Analysis Framework," report no. CMU/SEI-2010-TN-013 (Pittsburgh, PA: Software Engineering Institute, June 2010), http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9323.

[151] Department of Defense, "Resilience of Space Capabilities," 2011, https://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD Fact Sheet - Resilience.pdf.

As terms, resilience and survivability are often used interchangeably. Ideally, the DOD will strive for the survivability needed to "withstand" adverse events, expecting that it will also need the resilience to support critical functions "in spite of hostile action or adverse conditions."

The DOD is in the initial stages of recognizing that it needs survivability and resilience standards to protect against non-kinetic threats. However, it has yet to act on this urgent need in a meaningful way. The 2020 Nuclear Matters Handbook[152] states that the evolving threat to NC3 includes "cyber, electronic warfare, and advanced conventional capabilities." It further specifies that NC3 must be "capable of operating on internet-like networks to provide survivable, reliable support for senior U.S. government officials, the U.S. military, and U.S. allies, as appropriate." Despite its recognition of the importance of survivability against non-kinetic attacks, the handbook contains no mention of non-kinetic threats in its ninth chapter pertaining exclusively to survivability. Instead, it focuses squarely on electromagnetic pulse (EMP) and nuclear weapons detonations, as the U.S. government has done for decades.[153]

Similarly, U.S. Air Force Instruction 13-550 calls for "resilience against threats to include, but not limited to, EMP and cyberspace threats," yet it does not encompass the creation of enforceable survivability and resilience standards for non-kinetic threats to parallel existing standards of hardening against EMP attack.[154] Recently, "cyber survivability" was added to the Joint Capabilities Integration and Development System's Key Performance Parameters for Survivability. Yet as the defense community continues to discuss how to develop new standards,[155] there is ample opportunity to ensure that they are rigorous.

Although an at-length discussion of mechanisms for testing survivability and resilience is not within scope, a few are briefly reviewed below. Drawing from an old principle of cybersecurity, survivability and resilience standards should ideally guarantee that NC3 subsystems uphold Confidentiality, Availability, and Integrity (CAI) at all junctures; in other words, information must be kept confidential among authorized personnel, critical nodes must remain available and functional at all times, and data must remain uncorrupted and intact. To achieve CAI across critical

[152] The Nuclear Matters Handbook is not an authoritative U.S. government document. However, its contents are a helpful indicator of the status of U.S. government conversations on a range of nuclear policy matters.

[153] The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *The Nuclear Matters Handbook 2020 [revised]* (Washington, DC: ODASD(NM), 2020), https://www.acq.osd.mil/ncbdp/nm//NMHB2020rev/.

[154] Department of the Air Force, "Air Force Nuclear Command, Control, and Communications (NC3)," Air Force Instruction 13-550 (Washington, DC.: Department of the Air Force, 2019), https://static.e-publishing.af.mil/production/1/af_a10/publication/afi13-550/afi13-550.pdf.

[155] See Don Snyder et al., *Measuring Cybersecurity and Cyber Resiliency* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR2703.html; Deborah Bodeau, Richard Graubart, and Ellen Laderman. *Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes: Enabling Controls, Requirements, Solutions, and Metrics to Be Identified* (Bedford, MA: The MITRE Corporation, September 2019), https://www.mitre.org/sites/default/files/pdf/CR-Cyber-Survivability.pdf.

NC3 subsystems for the entire duration of their respective lifecycles, some productive steps might include the following recommendations.

This page is intentionally blank.

8. Policy Recommendations

- **Incorporate into doctrine the assumption that NC3 will inevitably be compromised**, instead of striving for perfect security.
    - Stemming from this assumption, **create a requirement for the survivability and resilience of NC3 subsystems against non-kinetic attacks** at all stages of their respective lifecycles, including design, production, maintenance, and, if applicable, life extension. Make an internal, classified determination regarding the **level of risk to NC3** that the U.S. government is willing to tolerate in order for its nuclear deterrent to be considered survivable overall.
    - If cost and resource constraints inhibit designers from achieving a gold standard of survivability and resilience throughout *all* NC3 subsystems, the U.S. should endeavor to defend a **"thin line,"** or smaller grouping of its most vital subsystems, concentrating funds and expertise toward protecting that thin line from non-kinetic threats.[156]
- **Create dedicated red teams** to actively test the vulnerability of NC3 to various types of non-kinetic attack, adapting as NC3 and the threat environment evolve.[157] Beyond traditionally conceived red teams, such as those that have been used historically to improve cybersecurity in industry, the DOD will need to think creatively. In 2011, the Department of Homeland Security performed a basic test, dropping computer discs and USB flash drives in the parking lot of the Pentagon. 90% of discs with cases showing an official logo were inserted by Pentagon employees into Pentagon computers, and of those retrieved, 60% were inserted into office computers.[158] There is no evidence that the DOD is taking advantage of such simple, low-cost approaches, which can provide volumes of information about the preparedness of personnel to confront malicious non-kinetic activity targeting NC3.
- **Prepare to operate under incomplete or incorrect information**. Plan as though immediate attribution of non-kinetic attacks is impossible and prepare for crisis situations in which aggressors remain anonymous. While it may be possible to build

[156] Although its overall findings conflict with the arguments made above, the DSB's *Task Force on Cyber Deterrence* provides useful recommendations on defending vital weapon systems against cyberattacks by upholding a cyber "thin line." See United States Defense Science Board, *Task Force on Cyber Deterrence.*

[157] The author benefitted from discussions on this subject with Priscilla Guthrie, John Harvey, and Jim Gosler.

[158] Bruce Sterling, "The Dropped Drive Hack," *Wired*, June 29, 2011, https://www.wired.com/2011/06/the-dropped-drive-hack/.

systems that maintain their most basic functions even in the event of a breach, it is less feasible to expect immediate attribution of attacks on NC3, especially during times of crisis.

- **When hiring the individuals who will manage survivability and resilience for NC3, allow for longevity and competitive pay.** Appoint a Chief Engineer[159] to oversee all phases of subsystem lifecycles within Next Generation NC3, conducting tests to ensure that its dozens of systems work in harmony despite often being designed by different contractors. Require the Chief Engineer to occupy her position for a minimum period that allows accumulation of expertise and preparation to pass that knowledge on to a successor. When hiring operators who oversee, for example, defense against cyber network intrusions, allow them to remain in their positions for longer than active duty military rotations would typically permit. The fast-paced overturn of such positions is contributing to a lack of sustained expertise on NC3. Additionally, by paying cybersecurity experts competitively with industry, the U.S. government can recruit the most qualified experts to secure NC3. Given the seriousness of non-kinetic threats to NC3, the U.S. should make a proper investment in hiring technical experts at the top of their respective fields.
- **Require contractors to develop, maintain, and share with the NC3 Chief Engineer a thorough documentation of system design**, ensuring that future operators will not be left in the dark. If Next Generation NC3 is to age well, system designers will need to provide a roadmap for future operators, as well as contractors who will perform maintenance and life extension.
- **Abandon cybersecurity metaphors such as trenches, walls, doors, and moats**, as the adversary cannot be kept out. Instead, build systems that envision a booby-trapped house with a locked front door, using active security features (e.g., honeypots or script white-listing).[160]
- **Ensure that NC3 modernization and changes to the strategy and doctrine impacting NC3 remain integrated into a cohesive vision of strategic stability.[161]** Deterrence strategies, modernization efforts, and arms control dialogues have a shared aim of preventing nuclear war. Although it is not the focus of this paper, recent

[159] This recommendation stems from conversations with Priscilla Guthrie.

[160] See Dunnmon, "Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace," in *Project on Nuclear Issues*, by Mark Cancian (2016 Nuclear Scholars Initiative and PONI Conference Series, October 2017), last updated January 2020, https://nuclearnetwork.csis.org/project-nuclear-issues/.

[161] Strategic stability is a contested term. For thoughtful consideration of differing types of stability such as "arms race stability" and "crisis stability," see James Acton's analysis in "Reclaiming Strategic Stability," chap. 4 in *Strategic Stability: Contending Interpretations*, ed. Elbridge Colby and Michael Gerson (Carlisle, PA: Strategic Studies Institute, 2013), 117.

> research[162] demonstrates that it may be enormously beneficial to initiate dialogue with adversaries about perceived threats to NC3, improving mutual understanding of doctrine, declaratory policies, and most pressing concerns. Absent meaningful dialogue with adversaries, conversations about the survivability and resilience of NC3 lack critical context. Pursuing such dialogue can reduce undue pressure on U.S. NC3 by potentially limiting or disincentivizing non-kinetic attacks on sensitive systems.

If leaders can learn to accept imperfect security, they can shift toward viewing non-kinetic breaches in NC3 as both inevitable and manageable. Relatedly, they can recognize that systems designed by humans are fallible. In fact, the majority of nuclear close calls have resulted from human error. See Appendix A. To counter the inevitability of manmade vulnerabilities and threats posed by adversaries, the U.S. must constantly reexamine NC3, identifying weaknesses, both technical and organizational, and bolstering strengths.

Thus far, in the minimal discussion on strategies for mitigating threats to NC3 below the threshold of armed conflict, deterrence has received the bulk of attention. The U.S. should explore the efficacy of compellence and other alternative strategies as a supplement to resilient NC3.

Notably, the architects of CYBERCOM's persistent engagement strategy contend that "coercion theory and associated strategies are not well aligned with the cyber strategic competitive space short of armed conflict."[163] Technicalities aside, the U.S. should observe lessons drawn from CYBERCOM's attempts at persistent engagement, which constitutes a significantly more forward-leaning stance than the U.S. has previously had in cyberspace.

Persistent engagement is new and still empirically unproven. Thus, it should not be casually applied to the defense of NC3 (for instance, aggressive responses to non-kinetic attacks on NC3 should require approval at the highest levels of U.S. leadership, involving decision-makers who grasp the grave implications of targeting adversaries' NC3 networks.) Still, persistent engagement may offer useful lessons about dealing with threats to NC3 below the threshold. In the coming years, CYBERCOM will perform analysis of its classified data on the successes and failures of persistent engagement. The DOD should take note of such analysis, extrapolating whether it might offer insights into the defense of NC3.

[162] Ariel E. Levite et al., "China-U.S. Cyber-Nuclear C3 Stability," *Carnegie Endowment for International Peace*, April 2021, https://carnegieendowment.org/2021/04/08/china-u.s.-cyber-nuclear-c3-stability-pub-84182.

[163] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," *Lawfare* (blog), February 6, 2020, https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

This page is intentionally blank.

9. Areas for Further Research

To support a robust discussion on the future safekeeping of NC3, several areas would benefit from further research.

A. Collecting and Analyzing Empirical Data

The single greatest obstacle to analyzing management of below-the-threshold threats to NC3 is a lack of empirical data. There is a noteworthy amount of research analyzing nuclear escalation during the Cold War and a much smaller, but still relevant, strand of work analyzing the dynamics surrounding recent, publicly documented cyberattacks. However, access to information regarding non-kinetic attacks on NC3 is limited,[164] mainly because such systems are rightfully subject to the highest levels of classification.

As the possessor of decades of classified information, the U.S. government has an obligation to undertake internal analysis of its own classified empirical data, attempting to draw conclusions about the potentially unique escalation dynamics surrounding non-kinetic attacks on NC3.

In the absence of real-world data, war games can provide a supplement for the scholarly community. In their 2018 article *Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains,* Jacquelyn Schneider and Sarah Kreps review the takeaways from six years of war games, observing overall that "U.S. decision-makers chose not to retaliate to cyberattacks."[165] Their hesitance "cannot be explained solely by the effects created by attacks." Rather, participants exhibited a view that cyberattacks are "qualitatively different" and somehow potentially more escalatory. Their aversion to hostility in cyberspace meant that they were "statistically less likely to support retaliation with force—escalation into a kinetic response—when our scenario took place in the cyber domain."[166] More recently, Schneider colleagues Benjamin Schechter and Rachael Shaffer presented the results of multiple years of wargames centering on cyber threats to NC3. Their work suggests that nuclear possessors may tend to disbelieve the vulnerability of their own NC3 to cyberattacks, while also embracing the use of cyberattacks against other states' NC3 in

[164] One notable exception is the United States' alleged plan to attack Soviet command and control using electronic warfare. It is explored in Benjamin Fischer's 2014 article "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps," *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (May 2014): 431-464, doi: 10.1080/08850607.2014.900290.

[165] Sarah Kreps and Jacquelyn Schneider, "Escalation firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logic," 4.

[166] Ibid., 8-9.

crisis scenarios.[167] Many of these observations contradict conventional wisdom and warrant further exploration.

B. Exploring Implications for Strategic Stability

With the exception of some analysis by Erik Gartzke and Jon Lindsay,[168] recent discussions on NC3 within the think tank and scholarly communities have tended to assume that non-kinetic attacks on NC3 are destabilizing. Little attention has been devoted to the possibility that, in some instances, mutual vulnerability could be a stabilizing force. For example, although limited information is available publicly, it is rumored that the U.S. and Russia have compromised one another's power grids using cyber network intrusions. Does their mutual vulnerability stabilize relations to reduce the likelihood of a dangerous attack on critical infrastructure, or does it make such attacks more likely?[169] Furthermore, does the collection of intelligence through espionage give states stabilizing knowledge about NC3? In the event that espionage does not lead to sabotage, does it create a sort of mutual visibility? Given the threat of retaliation and taboo surrounding nuclear weapons, is NC3 a less attractive target for non-kinetic attacks than other critical military assets?

Separately, scholars should explore the question of power differentials between actors, asking how a power imbalance might influence incentives to undermine NC3 short of war. This paper has begun to explore why weaker adversaries view secretive, non-kinetic attacks on NC3 as an appealing mode of altering the status quo. The United States' powerful nuclear deterrent and conventional forces mean that it has no true peers; at the moment, any foreign entity interfering in NC3 will inevitably be militarily weaker. Between NWS, what are the implications of power imbalances for the security of NC3? If a breach in NC3 is discovered, how do power imbalances impact the likelihood of escalation? What are the incentives for weaker powers, including non-NWS or non-state actors, to target NC3 using non-kinetic tools?

C. Avenues for Risk Reduction

What avenues exist for risk reduction that acknowledge the entire range of non-kinetic threats to NC3, moving beyond vague reference to "cyber" threats? Given the lack of a formal arms control treaty between the U.S. and China, what other means might succeed in creating an open dialogue and greater transparency regarding each country's dos and don'ts? Beyond the U.S. and China, can other nuclear weapon possessors be enticed to participate in an open dialogue to avoid misperceptions about NC3? Although the U.S. cannot speak in great detail about its NC3, it is

[167] Schneider, Jacquelyn, Benjamin Schechter, and Rachael Shaffer, "Cyber Operations and Nuclear Use: A Wargaming Exploration," paper presented at the 2021 International Studies Association Meeting, virtual, April 6-9, 2021.

[168] Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar."

[169] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

possible that risk reduction dialogues would provide a vital opportunity to clarify existing misconceptions in adversarial relationships.

D. The Future of Nuclear Strategy

This paper has emphasized that deterrence is a flawed instrument with uncertain effects, arguing that it is unfit to meet the challenge of managing below-the-threshold threats to NC3. It has also reinforced that the considerable obstacles to deterrence below the threshold need not signify a complete breakdown of *nuclear* deterrence. Today is not the first time that states have sensed a shift in power dynamics capable of upsetting deterrence. At various points during the Cold War, whether due to antisatellite weapons or perceived advances in ballistic missile defense, the U.S. considered its nuclear deterrent to be undermined. As a result, it often adopted a "hedging" approach, reflecting "the belief that the United States must maintain an elaborate insurance policy against technical problems in the stockpile or adverse geopolitical developments."[170] Sometimes, U.S. intelligence was later discovered to have been faulty or poorly interpreted by leadership, meaning that fears about deterrence were frequently overstated. In the interest of embracing past lessons, of which there are many, scholars should draw upon historical examples to add perspective to present dilemmas and contextualize the role of nuclear weapons in today's world.

If further study supports that deterrence below the threshold is an unpromising strategy, what are the implications for broader nuclear deterrence? In the coming decades, the safekeeping of U.S. NC3 will require unremitting and honest appraisal of its vulnerabilities. Given rapid evolutions, for example, in cyber offensive capabilities augmented by artificial intelligence or future advances in quantum computing, the severity of non-kinetic threats to NC3 may quickly increase. At what point (including in the face of increasingly advanced non-kinetic threats) are U.S. nuclear assets no longer survivable, credible, or resilient? At what point would governments deem nuclear weapons too dangerous to possess? How do non-kinetic threats to NC3 factor into this calculus?

As long as it continues to embrace nuclear weapons, how can the U.S. government continue to flexibly assess qualities such as survivability? How can the U.S. government define such subjective terms in the context of individual breaches in NC3, keeping in mind those of which it is likely unaware? What tools are available to assist it in visualizing the sprawling subsystems that comprise NC3? What is the role of a "thin line" in achieving some reasonable standard of survivability and resilience? These are all questions that would benefit from further examination, both in scholarly and governmental settings.

[170] Dallas Boyd. "Hedging Nuclear Deterrence: Reserve Warheads or a Responsive Infrastructure?" *Strategic Studies Quarterly* 8, no. 2 (Summer 2014): 96-114, accessed September 8, 2020, http://www.jstor.org/stable/26270805.

This page is intentionally blank.

10. Conclusion

Various accounts warn that the modernization of NC3 lacks necessary funding, and the past several decades prove that NC3 has historically been neglected despite a growing risk of subversion below the threshold of armed conflict. The Biden administration should not rely on untested concepts of below-the-threshold deterrence for the security of assets as destructive as nuclear weapons. Rather, it should embrace an emphasis on resilience and survivability, striving to demonstrate the United States' ability to actively respond to below-the-threshold attacks on NC3. NC3's inevitable vulnerabilities do not eliminate the possibility of a survivable and credible nuclear deterrent, but the U.S. must adopt a proactive approach, committing to a constant reevaluation of its vulnerabilities and the growing capabilities of hostile actors to undermine NC3 below the threshold.

This page is intentionally blank.

Appendix A.
Nuclear Close Calls Caused by Human Error and System Malfunction

- In 1960, a radar unit connected to North American Air and Aerospace Defense Command misidentified the moon as a massive Soviet attack. The error was caused by a computer malfunction, wherein two zeros were "accidentally removed…from the radar feed."[171]
- Also in 1960, "…a classified U.S. military investigation found that a series of major power surges at one of the many nuclear control centers spread across the American Midwest could theoretically lead to the unintended launch of an entire fleet of fifty nuclear-armed ICBMs."[172]
- In 1962, a guard at the Duluth Sector Direction Center in Minnesota mistook a bear climbing a fence for a Soviet intruder. The guard shot at the intruder and, due to flawed wiring in the warning bell, triggered nuclear attack warnings at bases throughout the region.[173]
- In 1971, "…an operator at [North American Air and Aerospace Defense Command] accidentally transmitted an emergency message ordering all broadcasts off the air, creating the impression that the United States was preparing for a nuclear war. It took the operator 40 minutes to find the right code to cancel the message."[174]
- In 1979, computers at the North American Air and Aerospace Defense Command "indicated that a missile had been launched from a submarine in the waters off the west

[171] Erik Gartzke and Jon Lindsay, "Thermonuclear Cyberwar"; Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, DC: Georgetown University Press, April 2018), 42-43.

[172] Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, 43, http://press.georgetown.edu/book/georgetown/hacking-bomb.

[173] Alex Wellerstein, "The Hawaii Alert Was an Accident. The Dread It Inspired Wasn't," *The Washington Post*, April 1, 2019, https://www.washingtonpost.com/news/posteverything/wp/2018/01/16/the-hawaii-alert-was-an-accident-the-dread-it-inspired-wasnt/?utm_term=.4299cc10ba6f; Ben Brimelow, "9 Times the World Was at the Brink of Nuclear War - and Pulled Back," *Business Insider*, April 25, 2018, https://www.businessinsider.com/when-nuclear-war-almost-happened-2018-4.

[174] Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, 43.

coast of the US." As it turned out, a technician had erroneously inserted a training tape into a computer at the operations center.[175]

- Also in 1979, "…a submarine-launched ballistic missile radar installation at Mount Hebo, Oregon, picked up a low-orbit rocket body that was close to decay and generated a false launch-and-impact report."[176]
- In June of 1980, a computer error caused false attack alarms at NORAD, indicating a false warning message of "massive nuclear attack." As President Carter and his national security advisor, Zbigniew Brzezinski, prepared to respond, they learned that the warnings had been false alarms, caused by a defective computer chip costing only 46 cents.[177]
- In 1983, a Soviet satellite detected the sun's reflection on the clouds and mistook it for five incoming U.S. missiles, triggering a warning of an incoming attack. Stanislav Petrov, a lieutenant colonel in the Soviet Air Defense Forces, suspected it was a false alarm and opted not to notify Soviet leadership, narrowly avoiding escalation.[178]
- In 1984, a computer malfunction caused warning systems to display a notification that a nuclear-armed missile was about to launch itself from a silo. Strategic Air Command officials concluded that the missile could not have launched itself due to safeguards already in place, but, nonetheless, Air Force officials at the time feared the worst and uselessly parked an armored car on top of the silo.[179]

[175] "Nuclear 'Command And Control': A History Of False Alarms And Near Catastrophes," *NPR*, August 11, 2014, https://www.npr.org/2014/08/11/339131421/nuclear-command-and-control-a-history-of-false-alarms-and-near-catastrophes.

[176] Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, 43.

[177] Matt Stevens and Christopher Mele, "Causes of False Missile Alerts: The Sun, the Moon and a 46-Cent Chip," *The New York Times*, January 13, 2018, https://www.nytimes.com/2018/01/13/us/false-alarm-missile-alerts.html.

[178] Ibid.

[179] "Vehicle Parked on Silo After Launch Signal," *The Washington Post*, October 28, 1987, https://www.washingtonpost.com/archive/politics/1987/10/29/vehicle-parked-on-silo-after-launch-signal/14c77303-74e2-47bb-8d90-30307e2983bd/?utm_term=.c7868fde7d9c.

Appendix B.
Illustrations

Figures

Figure 1. NC3 Subsystems Operating Daily..6
Figure 2. Conditions of Threat...18
Figure 3. General Deterrence Preventing Large-Scale Kinetic Attacks. 42

This page is intentionally blank.

Appendix C.
References

“Coronavirus: EU Strengthens Actions to Tackle Misinformation.” *European Commission*, June 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006.

“Nuclear 'Command And Control': A History Of False Alarms And Near Catastrophes.” *NPR*, August 11, 2014. https://www.npr.org/2014/08/11/339131421/nuclear-command-and-control-a-history-of-false-alarms-and-near-catastrophes.

“Vehicle Parked on Silo After Launch Signal.” *The Washington Post*, October 28, 1987. https://www.washingtonpost.com/archive/politics/1987/10/29/vehicle-parked-on-silo-after-launch-signal/14c77303-74e2-47bb-8d90-30307e2983bd/?utm_term=.c7868fde7d9c.

Acton, James. “Command and Control in the Nuclear Posture Review: Right Problem, Wrong Solution.” *War on the Rocks*, February 5, 2018. https://warontherocks.com/2018/02/command-and-control-in-the-nuclear-posture-review-right-problem-wrong-solution/.

Acton, James. “Reclaiming Strategic Stability.” Chap. 4 in *Strategic Stability: Contending Interpretations*, edited by Elbridge Colby and Michael Gerson. Carlisle, PA: Strategic Studies Institute, 2013. 117.

Aitoro, Jill. “US Logistics Boss Talks Risks to the Supply Chain and Protective Measures.” *Defense News*, October 28, 2019. https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/.

Anttiroiko, Ari-Veikko, and Mälkiä Matti. In *Encyclopedia of Digital Government*. Hershey, PA: Idea Group Reference, July 2006.

Bahney, Benjamin W., Jonathan Pearl, and Michael Markey. “Antisatellite Weapons and the Growing Instability of Deterrence.” Chap. 6 in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Eric Gartzke and Jon R. Lindsay. New York City, NY: Oxford University Press, 2019. doi: 10.1093/oso/9780190908645.003.0006.

Betts, Richard K. “The Lost Logic of Deterrence: What the Strategy that Won the Cold War Can--and Can’t-- do Now.” *Foreign Affairs* 92, no. 2 (March/April 2013). https://www.foreignaffairs.com/articles/united-states/2013-02-11/lost-logic-deterrence.

Bodeau, Deborah, Richard Graubart and Ellen Laderman. *Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes: Enabling Controls, Requirements, Solutions, and Metrics to Be Identified*. Bedford, MA: The MITRE Corporation, September 2019. https://www.mitre.org/sites/default/files/pdf/CR-Cyber-Survivability.pdf.

Boyd, Dallas. “Hedging Nuclear Deterrence: Reserve Warheads or a Responsive Infrastructure?” *Strategic Studies Quarterly* 8, no. 2 (Summer 2014): 96-114. Accessed September 8, 2020. http://www.jstor.org/stable/26270805.

Boyens, John, Celia Paulsen, Rama Moorthy, and Nadya Bartol. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." NIST Special Publication 800-161. Washington, DC: NIST, April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161.

Bradshaw, Samantha, and Philip N. Howard. "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation." Working paper at The Computational Propaganda Project. University of Oxford, UK, September 26, 2019. https://comprop.oii.ox.ac.uk/research/cybertroops2019/.

Brimelow, Ben. "9 Times the World Was at the Brink of Nuclear War - and Pulled Back." *Business Insider*, April 25, 2018. https://www.businessinsider.com/when-nuclear-war-almost-happened-2018-4.

Caiyu, Liu. "Chinese Academician Warns of 'Nuclear-Bomb Like Cyber Attack' from US Against 5G." *Global Times*, August 5, 2020. https://www.globaltimes.cn/content/1196855.shtml.

Cancian, Mark. "Project on Nuclear Issues." Center for Strategic International Studies, October 4, 2017. Updated January 28, 2020. https://nuclearnetwork.csis.org/project-nuclear-issues/.

Chesney, Robert. "Project Raven: What Happens When U.S. Personnel Serve a Foreign Intelligence Agency?" *Lawfare* (blog), February 11, 2019. https://www.lawfareblog.com/project-raven-what-happens-when-us-personnel-serve-foreign-intelligence-agency.

Clark, Colin, "Nuclear C3 Goes All Domain: Gen Hyten," *Breaking Defense*, February 20, 2020. https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

Clark, Colin. "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria." *Breaking Defense*, April 24, 2018. https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.

Clark, David D. and Susan Landau. "Untangling Attribution." Essay from Harvard Law School National Security Journal 2 (2011). https://harvardnsj.org/wp-content/uploads/sites/13/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf.

Congressional Research Service. *Defense Primer: Electronic Warfare* § Updated October 2019. https://fas.org/sgp/crs/natsec/IF11118.pdf.

Decker, Debra, Kathryn Rauhut, Sara Z. Kutchesfahani, and Erin Connolly. *Nuclear Cybersecurity Risks and Remedies*. Vienna, Austria: Fissile Materials Working Group, Stimson, March 2019. https://armscontrolcenter.org/wp-content/uploads/2019/03/FMWG_CyberReport_webready.pdf.

Department of Defense. "Resilience of Space Capabilities," 2011. https://archive.defense.gov/home/features/2011/0111_nsss/docs/DOD Fact Sheet - Resilience.pdf.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Department of Homeland Security. *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue*. Analytic Exchange Program, October 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

Department of Justice and NCSC. "National Insider Threat Task Force- Mission Fact Sheet." n.p.: n.d. https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

Department of the Air Force. "Air Force Nuclear Command, Control, and Communications (NC3)," Air Force Instruction 13-550. Washington, DC.: Department of the Air Force, 2019. https://static.e-publishing.af.mil/production/1/af_a10/publication/afi13-550/afi13-550.pdf.

Deptula, David A., William A. LaPlante, and Robert Haddick. *Modernizing US Nuclear Command, Control and Communications*. Arlington, VA: The Mitchell Institute for Aerospace Studies and The MITRE Corporation, February 14, 2019. https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_ed45cfd71de2457eba3bcce4d0657196.pdf.

Dingman, Roger. "Atomic Diplomacy During the Korean War." *International Security* 13, no. 3 (Winter 1988): 50-91. muse.jhu.edu/article/446784.

Dunnmon, Jared. "Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace." In *Project on Nuclear Issues*, by Mark Cancian. 2016 Nuclear Scholars Initiative and PONI Conference Series, October 2017. Last updated January 2020. https://www.csis.org/programs/international-security-program/project-nuclear-issues

Egozi, Arie. "Why Would Russia Spoof Israeli GPS? F-35 & Iran." *Breaking Defense*, June 28, 2019. https://breakingdefense.com/2019/06/if-russia-is-spoofing-israeli-gps-then-why-iran-f-35/.

Elkus, Adam. "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense." *War on the Rocks*, December 15, 2015. https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

Ellison, Robert J., and Carol Woody. "Survivability Analysis Framework" Report no. CMU/SEI-2010-TN-013. Pittsburgh, PA: Software Engineering Institute, June 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9323.

Erwin, Sandra, "U.S STRATCOM to Take Over Responsibility for Nuclear Command, Control and Communications." *SPACENEWS*, July 23, 2018. https://spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications/.

Feiner, Lauren. "U.S. Tightens Restrictions on Huawei Access to Technology and Chips." *CNBC*, August 17, 2020. https://www.cnbc.com/2020/08/17/us-to-tighten-restrictions-on-huawei-access-to-technology-chips-sources-say.html.

Fischer, Benjamin B. "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps." *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (May 2014): 431-464. doi: 10.1080/08850607.2014.900290.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no.3 (2017): 391-393. https://doi.org/10.1016/j.orbis.2017.05.003.

Fischerkeller, Michael P., and Richard J. Harknett. "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect." *Lawfare* (blog), February 6, 2020. https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

Fischerkeller, Michael P., and Richard J. Harknett. *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*. IDA Document NS D-9076. Alexandria, VA: Institute for Defense Analyses, 2018.

Freedberg Jr., Sydney J. "Electronic Warfare: Better, But Still Not Good Enough." *Breaking Defense*, November 1, 2019. https://breakingdefense.com/2019/11/electronic-warfare-better-but-still-not-good-enough/.

Freedman, Linn F. "Frequency and Cost of Insider Threats Continue to Increase." *The National Law Review* 9, no. 256 (September 2021). https://www.natlawreview.com/article/frequency-and-cost-insider-threats-continue-to-increase.

Futter, Andrew. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington, DC: Georgetown University Press, April 2018. http://press.georgetown.edu/book/georgetown/hacking-bomb.

Gartzke, Eric, and Jon R. Lindsay. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York, NY: Oxford University Press, 2019. doi: 10.1093/oso/9780190908645.001.0001.

Gartzke, Erik, Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 2017): 37–48. https://doi.org/10.1093/cybsec/tyw017.

Gavin, Francis J. "We Need to Talk: The Past, The Present, and Future of the U.S. Nuclear Weapons Policy." *War on the Rocks*, January 2, 2017. https://warontherocks.com/2017/01/we-need-to-talk-the-past-present-and-future-of-u-s-nuclear-weapons-policy/.

Gordon, Michael R., and Jeremy Page. "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says." *The Wall Street Journal*, April 9, 2018. https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320.

Green, Brendan Rittenhouse, and Austin Long. "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition." *International Security* 44, no. 3 (Winter 2019/20): 48–83. doi.org/10.1162/ISEC_a_00367.

Greenberg, Andy. "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/.

Harvey, John R. "US Nuclear Command and Control for the 21st Century." *NAPSNet Special Reports*, May 24, 2019. https://nautilus.org/napsnet/napsnet-special-reports/u-s-nuc-ear-command-and-control-for-the-21st-century/.

Healey, Jason. "Not the Cyber Deterrence the United States Wants." *Council on Foreign Relations* (blog), June 11, 2018. https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants.

Healey, Jason. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1 (2019): tyz008. https://doi.org/10.1093/cybsec/tyz008.

Holmes, Marian Smith. “Spies Who Spilled Atomic Bomb Secrets.” *Smithsonian Magazine*, April 19, 2009. https://www.smithsonianmag.com/history/spies-who-spilled-atomic-bomb-secrets-127922660/.

Hughes, Daniel, and Andrew M. Colarik. “Predicting the Proliferation of Cyber Weapons into Small States.” *Joint Force Quarterly* 83, no. 4 (2016): 19-26. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-83/jfq-83_19-26_Hughes-Colarik.pdf?ver=2016-10-19-102201-033.

Internet Security Threat Report. Symantec Corporation, February 2019. Accessed September 2021. https://docs.broadcom.com/doc/istr-24-2019-en.

Jervis, Robert. “Deterrence Theory Revisited.” *World Politics* 31, no. 2 (January 1979): 289-324. doi:10.2307/2009945.

Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12. Washington, DC: Joint Chiefs of Staff, June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Joint Chiefs of Staff. *Department of Defense: Dictionary of Military and Associated Terms*. Joint Publication 1-02. Washington, DC: Joint Chiefs of Staff, November 2010. Amended through February 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf.

Joint Chiefs of Staff. *Information Operations*. Joint Publication 3-13. Washington, DC: Joint Chiefs of Staff, February 2006. https://www.hsdl.org/?view&did=461648.

Joint Chiefs of Staff. *Joint Concept for Integrated Campaigning*. Washington, DC: Joint Chiefs of Staff, March 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257,%206.

Joint Chiefs of Staff. *Joint Electromagnetic Spectrum Operations*. Joint Publication 3-85. Washington, DC: Joint Chiefs of Staff, May 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347.

Joint Chiefs of Staff. *Joint Engineer Operations*. Joint Publication 3-34. Washington, DC, January 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_34.pdf.

Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, DC: Joint Chiefs of Staff, January 2017. https://www.jcs.mil/Doctrine/DOCNET/JP-3-0-Joint-Operations/.

Jones, Jeffrey B. “Confronting China's Efforts to Steal Defense Information.” Cambridge, MA: Belfer Center for Science and International Affairs, May 2020. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

Jordan, Kathleen A., Brian A. Haugh, Asghar I. Noor, and D. Douglas Smith. “Legal System Wrapping for Department of Defense Information System Modernization.” IDA Paper P-3144. Alexandria, VA: Institute for Defense Analyses, July 1995. https://apps.dtic.mil/dtic/tr/fulltext/u2/a326906.pdf.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. Introduction by Thomas C. Schelling. London, UK: Routledge, July 2017.

Kepe, Marta. “NATO: Prepared for Countering Disinformation Operations in the Baltic States?” RAND Corporation, June 7, 2017. https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.html.

Kreps, Sarah, and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logic.” *Journal of Cybersecurity* 5, no. 1 (September 2019): tyz009. doi: 10.1093/cybsec/tyz007.

Kurlantzick, Joshua. “How China Is Interfering in Taiwan's Election.” *Council on Foreign Relations*, November 7, 2019. https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

Lanoszka, Alexander. “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe.” *International Affairs* 92, no. 1 (January 2016): 175-195. DOI: 10.1111/1468-2346.12509.

LeMay, Curtis. Center for Doctrine Development and Education. Annex 3-0 Operations and Planning. 2016

Levite, Ariel E., Lyu Jinghua, George Perkovich, Lu Chuanying, Xu Manshu, Li Bin, and Yang Fan. “China-U.S. Cyber-Nuclear C3 Stability.” *Carnegie Endowment for International Peace*, April 2021. https://carnegieendowment.org/2021/04/08/china-u.s.-cyber-nuclear-c3-stability-pub-84182.

Lewis, James Andrew. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, and Lanham, MD: Rowan & Littlefield, 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf.

Li, Lauly and Cheng Ting-Fang. “Exclusive: Washington Pressures TSMC to Make Chips in US.” *Nikkei Asia*, January 15, 2020. https://asia.nikkei.com/Business/Technology/Exclusive-Washington-pressures-TSMC-to-make-chips-in-US.

Libicki, Martin C. *Brandishing Cyberattack Capabilities*. Santa Monica, CA: RAND Corporation, 2013. https://www.rand.org/pubs/research_reports/RR175.html.

Lin, Herbert. “Attribution of Malicious Cyber Incidents: From Soup to Nuts.” Stanford, CA: Hoover Institution, September 2016. https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0.

Lin, Herbert. “Cyber Conflict and International Humanitarian Law.” *International Review of the Red Cross* 94, no. 886 (Summer 2012). https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York, NY: Oxford University Press, March 2015.

Mazarr, Michael J. *Understanding Deterrence*. Santa Monica, CA: RAND Corporation, 2018. https://doi.org/10.7249/pe295.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” *BBC News*, April 27, 2017. https://www.bbc.com/news/39655415.

McNamara, Robert S. “Apocalypse Soon.” *Foreign Policy*, October 21, 2009. https://foreignpolicy.com/2009/10/21/apocalypse-soon/.

Melzer, Nils. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva, Switzerland: International Committee of the Red Cross, May 2009. https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

Michaels, Jim. “U.S. Could Use Cyberattack on Syrian Air Defenses.” *USA Today*, May 16, 2013. https://www.usatoday.com/story/news/world/2013/05/16/syria-attack-pentagon-air-force-military/2166439/.

Narang, Vipin. “What Does It Take to Deter? Regional Power Nuclear Postures and International Conflict.” *The Journal of Conflict Resolution* 57, no. 3 (June 2013): 478-508. http://www.jstor.org/stable/23414723.

Naval Studies Board. *Post-Cold War Conflict Deterrence*. Washington, DC: National Academy Press, 1997. https://doi.org/10.17226/5464.

Nye Jr., Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016): 44-71. https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

Office of the Secretary of Defense. “Nuclear Posture Review.” Washington, DC: Department of Defense, February 2018. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

Office of the Under Secretary of Defense and United States Defense Science Board. *Report of the Defense Science Board Task Force on Command and Control Systems Management.* Washington, DC: Department of Defense, July 1978. https://dsb.cto.mil/reports/1970s/a110933.pdf.

Pelopidas, Benoît. “The Unbearable Lightness of Luck: Three Sources of Overconfidence in the Manageability of Nuclear Crises.” *European Journal of International Security* 2, no. 2 (2017): 240–62. doi:10.1017/eis.2017.6.

Perlroth, Nicole, and Clifford Krauss. “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.” *The New York Times*, March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

Perlroth, Nicole. “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.” *The New York Times*, October 23, 2012. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Pollpeter, Kevin. “Space, the New Domain: Space Operations and Chinese Military Reforms,” *Journal of Strategic Studies* 39, no. 5-6 (August 2016): 709-727. doi: 10.1080/01402390.2016.1219946.

Purdy, Matthew. “The Making of a Suspect: The Case of Wen Ho Lee.” *The New York Times*, February 4, 2001. https://www.nytimes.com/2001/02/04/us/the-making-of-a-suspect-the-case-of-wen-ho-lee.html.

Reiner, Philip, and Alexa Wehsener. “The Real Value of Artificial Intelligence in Nuclear Command and Control.” *War on the Rocks*, November 4, 2019. https://warontherocks.com/2019/11/the-real-value-of-artificial-intelligence-in-nuclear-command-and-control/.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1-2 (December 2014): 4-37. doi: 10.1080/01402390.2014.977382.

Roblin, Sébastien. “Electronic Warfare: The U.S. Is Losing the Invisible Fight to Russia's Dominant Capabilities.” *NBC News*, November 26, 2019. https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101.

Roblin, Sébastien. “Electronic Warfare: The U.S. Is Losing the Invisible Fight to Russia's Dominant Capabilities.” *NBC News*, November 26, 2019. https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101.

Sanger, David E., and Nicole Perlroth. “U.S. Escalates Online Attacks on Russia's Power Grid.” *The New York Times*, June 15, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Satter, Raphael, Jeff Donn, and Justin Myers. “Digital Hit List Shows Russian Hacking Went Well Beyond U.S. Elections.” *Chicago Tribune*, November 2, 2017. https://www.chicagotribune.com/nation-world/ct-russian-hacking-20171102-story.html.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2020.

Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University, 1980.

Schneider, Jacquelyn, Benjamin Schechter, and Rachael Shaffer. “Cyber Operations and Nuclear Use: A Wargaming Exploration.” Paper presented at the 2021 International Studies Association Meeting, virtual, April 6-9, 2021.

Schneider, Jacquelyn. “The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War.” *Journal of Strategic Studies* 42, no. 6 (August 2019) 841-863. doi: 10.1080/01402390.2019.1627209.

Senate Committee on Armed Services, “Statement of Admiral C. D. Haney, Commander, United States Strategic Command,” 113th Cong., 2nd sess., February 27, 2014, 9. https://www.stratcom.mil/Media/Speeches/Article/986430/air-force-association-national-defense-industrial-association-and-reserve-offic/.

Snegovaya, Maria. *Russia Report I Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare*. Washington, DC: Institute for the Study of War, September 2015. http://www.understandingwar.org/sites/default/files/Russian Report 1 Putin's Information Warfare in Ukraine- Soviet Origins of Russias Hybrid Warfare.pdf.

Snyder, Don, Lauren A. Mayer, Guy Weichenberg, Danielle C. Tarraf, Bernard Fox, Myron Hura, Suzanne Genc, and Jonathan Welburn. *Measuring Cybersecurity and Cyber Resiliency*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR2703.html.

Spears, Will. “A Sailor's Take on Multi-Domain Operations.” *War on the Rocks*, May 21, 2019. https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/.

Stack, Liam. “Update Complete: U.S. Nuclear Weapons No Longer Need Floppy Disks.” *The New York Times*, October 24, 2019. https://www.nytimes.com/2019/10/24/us/nuclear-weapons-floppy-disks.html.

Sterling, Bruce. “The Dropped Drive Hack.” *Wired*, June 29, 2011. https://www.wired.com/2011/06/the-dropped-drive-hack/.

Stevens, Matt, and Christopher Mele. “Causes of False Missile Alerts: The Sun, the Moon and a 46-Cent Chip.” *The New York Times*, January 13, 2018. https://www.nytimes.com/2018/01/13/us/false-alarm-missile-alerts.html.

Stoutland, Paigo O., and Samantha Pitts-Kiefer. *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group*. Washington, DC: NTI, September 2018. https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

Tennis, Maggie. “Russia Ramps up Global Elections Interference: Lessons for the United States.” *Center for Strategic and International Studies*, July 20, 2020. https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states.

The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. *The Nuclear Matters Handbook 2020 [Revised]*. Washington, DC: ODASD(NM), 2020. https://www.acq.osd.mil/ncbdp/nm//NMHB2020rev/.

Theohary, Catherine A. “Information Warfare: Issues for Congress.” Report no. R45142. Washington, DC: Congressional Research Service, March 2018. https://fas.org/sgp/crs/natsec/R45142.pdf.

Tor, Uri. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* 40, no. 1-2 (December 2015): 92-117. doi: 10.1080/01402390.2015.1115975.

Trevithick, Joseph. “New Type of GPS Spoofing Attack In China Creates ‘Crop Circles’ Of False Location Data.” *The Drive*, November 18, 2019. https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data.

Tsagourias, Nicholas. “Cyber Attacks, Self-Defense and the Problem of Attribution.” *Journal of Conflict & Security Law* 17, no. 2 (2012): 229–244. https://ssrn.com/abstract=2538271.

U.S. Army. *The U.S. Army in Multi-Domain Operations 2028*. TADOC Pamphlet 525-3-1. Washington, DC: TRADOC, 2018. https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028.

Unal, Beyza, and Patricia Lewis. *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*. London, UK: Chatham House, January 2018. https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

United States Cyber Command. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” Fort Meade, MD: US Cyber Command, 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf?ver=2018-06-14-152556-010.

United States Cyberspace Solarium Commission. *United States of America Cyberspace Solarium Commission*. n.p., March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

United States Defense Science Board. *DSB Task Force on Cyber Supply Chain*. Washington, DC: Office of the Under Secretary of Defense, February 2017. https://www.hsdl.org/?view&did=799509.

United States Department of Defense and United States Defense Science Board. *Task Force on Cyber Deterrence.* Washington, DC: Department of Defense, February 2017. https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf.

United States Department of Justice. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Washington, DC: May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

United States Government Accountability Office. "Nuclear Command, Control, and Communications: Update on Airforce Oversight Effort and Selected Acquisition Programs." GAO-17-641R. Washington, DC: GAO, August 2017. https://www.gao.gov/products/gao-17-641r.

United States Government Accountability Office. "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities." GAO-19-128. Washington, DC: GAO, October 2018. https://www.gao.gov/products/gao-19-128.

VansonBourne. "Securing the Supply Chain." Crowdstrike.com, July, 2018. https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf.

Way, Tyler. "Counterspace Weapons 101." *Aerospace Security*, July 23, 2020. https://aerospace.csis.org/aerospace101/counterspace-weapons-101/.

Wellerstein, Alex. "The Hawaii Alert Was an Accident. The Dread It Inspired Wasn't." *The Washington Post*, April 1, 2019. https://www.washingtonpost.com/news/posteverything/wp/2018/01/16/the-hawaii-alert-was-an-accident-the-dread-it-inspired-wasnt/?utm_term=.4299cc10ba6f.

West, Darrell M. "How to Combat Fake News and Disinformation." *Brookings*, December 18, 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

Wheeler, David A., and Gregory N. Larsen. *Techniques for Cyber Attack Attribution*. IDA Paper P-3792. Alexandria, VA: Institute for Defense Analyses, October 2003. https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf.

Wilkening, Dean. *Hypersonic Weapon and Strategic Stability*. Baltimore, MD: Johns Hopkins Applied Physics Laboratory, January 2020. https://nsiteam.com/social/wp-content/uploads/2020/01/200115-Wilkening-Slides.pdf.

Wilner, Alex S. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43, no. 2 (February 2019): 245-280. doi: 10.1080/01402390.2018.1563779.

Windrem, Robert. “Timeline: Ten Years of Russian Cyber Attacks on Other Nations.” *NBC News*, December 18, 2016. https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

Zetter, Kim. “An Unprecedented Look at Stuxnet, the World's First Digital Weapon.” *Wired*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim. “Hacker Lexicon: What is a Zero Day?” *Wired*, November 11, 2014. https://www.wired.com/2014/11/what-is-a-zero-day/.

This page is intentionally blank.

Appendix D. Abbreviations

CAI	Confidentiality, Availability, and Integrity
CNA	Cyber Network Attack
CNE	Cyber Network Exploitation
CRS	Congressional Research Service
CSC	Cyberspace Solarium Commission
CSIS	Center for Strategic and International Studies
CYBERCOM	United States Cyber Command
DOD	Department of Defense
DSB	Defense Science Board
EAM	Emergency Action Message
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum
EO	Executive Order
EW	Electronic Warfare
NC2	Nuclear Command and Control
NC3	Nuclear Command, Control, and Communications
NPR	Nuclear Posture Review
NWS	Nuclear Weapon States
STRATCOM	United States Strategic Command
UAE	United Arab Emirates

This page is intentionally blank.