APRIL 2017

Project on Nuclear Issues

A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series

EDITOR

Mark Cancian

AUTHORS

Christopher M. Conant
Jared Dunnmon
Dean Ensley
Ashley E. Green
Rebecca Friedman Lissner
Harrison Menke
Sarah Shirazyan
Alexandra Van Dine
Brittney Washington
Tracey-Ann Wellington
Rachel Wiener

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by the generous support of the Defense Threat Reduction Agency and the National Nuclear Security Administration.

ISBN: 978-1-4422-8001-4 (pb); 978-1-4422-8002-1 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.**csis**.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.**rowman**.com

Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace

Jared Dunnmon[1]

Cyber vulnerabilities in the space-based component of U.S. nuclear command, control, and communications (NC3) systems represent a significant risk to ensuring continuing nuclear stability. This paper examines emerging threats to the surety of the U.S. nuclear deterrent resulting from asymmetric threats to space-based assets from actors in the cyber domain, and considers how responses to such threats could be framed in terms of the laws of armed conflict. Several scenarios are developed to demonstrate both the immediacy and the inherent difficulty of operational problems that could result from current NC3 architectures. Finally, distinct sets of recommendations spanning both technology and policy domains are developed with the goal of reducing the possibility of nuclear destabilization caused by a cyber attack on U.S. NC3.

---

1. Jared Dunnmon is a PhD candidate in engineering at Stanford University. His academic interests encompass energy and propulsion systems, artificial intelligence, nuclear deterrence, and improving cyber-physical resilience in critical infrastructure systems. In addition to his research work, Dunnmon is affiliated with the Stanford Hacking for Defense (H4D) project, focused on applying Silicon Valley rapid innovation techniques to pressing problems in defense and national security. Dunnmon holds a bachelor's degree in mechanical engineering from Duke University in addition to master's degrees in both scientific computing and business administration from Oxford University. This manuscript would not have been possible without the support, time, and effort of a wide variety of individuals. The author would especially like to thank Ambassador Linton Brooks, Dr. James Miller, Dr. John Harvey, Dr. James A. Lewis, Professor Scott Sagan, Admiral James O. Ellis, Dr. Herbert Lin, and Mallory Stewart for their engagement during this project.

INTRODUCTION

In the years following the conclusion of the Cold War, the nature of international nuclear dynamics has fundamentally changed. Instead of a nuclear community dominated by mutually assured destruction between two superpowers, the last several decades have seen proliferation of nuclear capabilities in new locations such as Iran and North Korea combined with unprecedented democratization of powerful technology previously confined to nation-states.[2] In particular, the rapid global uptake of high-performance computational capability, reduced barriers to space access, and widespread proliferation of knowledge via the Internet have eroded many of the technological advantages previously held by nation-states.[3]

The challenges associated with these new realities are particularly important in the ongoing process of ensuring the security and strategic stability of the U.S. nuclear deterrent through the nuclear command, control, and communications (NC3) system. The purpose of the NC3 system is to link nuclear forces to presidential authority; this is accomplished via a complex system that includes space-borne and terrestrial early warning radar, facilities to interpret early warning information, various terrestrial and airborne command and control posts, and communications infrastructure comprised of satellite, radio frequency (RF), and land-line communications.[4] As noted by Admiral Cecil Haney in his capacity as United States Strategic Command (USSTRATCOM) commander, "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 success is increasing. Our challenges include operating aging legacy systems and addressing risks associated with today's digital security environment."[5]

Much of Admiral Haney's testimony focuses on the specter of threats in the cyber domain, the full definition of which can be succinctly stated as "an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructure."[6] This emphasis on cyber threats to NC3 systems echoes conclusions of both the Defense Science Board[7] and the 2014 Quadrennial Defense Review (QDR).[8] In addition, a variety

---

2. George P. Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn, "A World Free of Nuclear Weapons," *Wall Street Journal*, January 4, 2007.

3. Jason Fritz, "Hacking Nuclear Command and Control," International Commission on Nuclear Nonproliferation and Disarmament, 2009, http://icnnd.org/documents/jason_fritz_hacking_nc2.doc.

4. John Harvey, "Nuclear Command and Control for the 21st Century" (speech given at the DNUG Conference, September 23, 2014, Lorton, VA).

5. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney, Commander, United States Strategic Command," 113th Cong., 2nd sess., February 27, 2014, 9.

6. Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart Starr, and Larry Wentz (Dulles, VA: Potomac Books, 2009).

7. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013).

8. U.S. Department of Defense (DoD), *Quadrennial Defense Review Report, 2014* (Washington, DC: DoD, March 2014).

of scholars have described the dire consequences of an NC3 architecture compromised by cyber incursion, including false alarms, inadvertent launches, loss of contact with nuclear weapons, premature detonation, and a fundamental loss of nuclear strategic stability.[9] It is therefore imperative for global safety and security that NC3 systems be safeguarded from cyber intrusion.

Unfortunately, given the increasingly complex nature of the NC3 systems described above, there exist a variety of potential attack vectors that could be exploited by malicious interests, including both state and non-state actors. Such attacks could be categorized as follows: communicating inaccurate actions or intentions, increasing perceived time pressures to act or respond, disrupting or destroying communications channels, and hindering the search for viable alternatives.[10] For effective NC3 operation, for instance, it is crucial that early warning sensors give accurate information on whether another state has launched a nuclear attack; otherwise, erroneous assessments could result in an unintended nuclear exchange. Ambiguity in early warning systems is particularly problematic given that watch personnel generally have only three minutes to initially differentiate a nuclear launch from such mundane events as solar reflection off the water, wildfires, and ever more common commercial satellite launches.[11]

Effective NC3 operation is also directly reliant on assured communications between key elements of leadership. Specifically, the minimum essential electronic communications network (MEECN) represents the critical linkage between presidential authority and the three legs of the command, control, and communications triad. This system includes airborne (E-6B TACAMO, E-4B NAOC, B-52 bomber), satellite (AFSATCOM, MILSTAR, AEHF), seaborne (SSBN), and ground-based (NMCC, MRT) assets. Disruption of this communications network would erode or neutralize U.S. capability to rapidly execute decisions made by strategic leaders.[12]

Finally, reduction in the number of viable nuclear response alternatives detracts from strategic stability. If part of the nuclear enterprise (e.g., any leg of the command, control, and communications triad, or a component of the NC3 system) is believed to have been compromised by an adversary, it becomes much more likely that any further perceived aggression will be met with nuclear response.[13] In the end, it is clear that any degradation of the U.S. NC3 system materially increases the possibility of nuclear conflict and the associated human catastrophe. It thus remains imperative that vulnerabilities to this architecture be minimized.

---

9. Andrew Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age" (paper presented at the ISA Annual Conference, New Orleans, LA, February 2015); Eric Schlosser, *Command and Control: Nuclear Weapons, The Damascus Accident, and the Illusion of Safety* (New York: Penguin, 2013); Bruce Blair, "Rogue States: Nuclear Red Herrings," *Defense Monitor*, January 2004; Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington, DC: Center for New American Security, 2014).

10. Futter, "Hacking the Bomb."

11. Blair, "Rogue States."

12. Fritz, "Hacking Nuclear Command and Control." AEHF, Advanced Extremely High Frequency; AFSATCOM, Air Force Satellite Communications; MILSTAR, Military Strategic and Tactical Relay; MRT, Miniature Receive Terminal; NAOC, National Airborne Operations Center; NMCC, National Military Command Center; SSBN, strategic ballistic missile submarine.

13. Futter, "Hacking the Bomb."

This paper will first present an overview of how the democratization of key technologies in the early twenty-first century has led to the development of asymmetric threats to NC3 systems in the space and cyber domains. Next, it will consider how the traditional laws of armed conflict could be adapted to the cyber domain within the context of its interaction with NC3. Analysis then proceeds to consider two different scenarios to demonstrate how the combination of asymmetric threats, current NC3 technology, and ambiguous laws of armed cyber-conflict could put U.S. leadership in difficult strategic decisionmaking situations. Finally, the discussion concludes with a set of technical and policy recommendations intended to reduce the possibility that such scenarios would ever come to pass.

ASYMMETRIC THREATS TO NC3 IN THE TWENTY-FIRST CENTURY

While rapid advances in information technology, communications, and computation have yielded many improvements to NC3 systems, these improvements have come at the cost of NC3 surety and security. The two domains in which these costs are most apparent are the two newest arenas of conflict: outer space and cyberspace. In the words of Admiral Haney, "the space domain, along with cyberspace, is simultaneously more critical to all U.S. operations yet more vulnerable than ever to hostile actions."[14] The worrisome combination of international norms that have been far outpaced by the speed of technological advancement and democratization of key space and cyber technologies has led the United States to a point where it is difficult to be confident that the current NC3 structure is resilient in a cyber-physical sense.

Outer Space

The major threat to NC3 posed by vulnerabilities in space-based assets results from potential disruptions to both early warning and communications functions. As noted by Frank Rose, former deputy assistant secretary of state for defense policy and verification operations,

> The United States in particular is deeply reliant upon space. While such reliance enables the United States and our allies and partners to undertake a range of operations in support of peace and security, this reliance has increasingly been viewed by potential adversaries as a vulnerability to be exploited through the development of counterspace capabilities.[15]

This reality is particularly emergent in the context of NC3. At present, it is known that Russia and China are actively pursuing or already maintain such capabilities as laser weapons for satellite denial,[16] electromagnetic (EM) jamming for communications degradation, and physical antisatellite

14. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney Commander United States Strategic Command."

15. Frank Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment" (remarks at International Symposium on Ensuring Stable Use of Outer Space, Tokyo, March 3, 2016).

16. Ibid.

(ASAT) systems.[17] Given heavy reliance on satellites such as Advanced Extremely High Frequency (AEHF) and Air Force Satellite Communications (AFSATCOM) in the NC3 system, ensuring both reliability and resiliency to these types of threats will be critical to creating a flexible and efficient NC3 system.

Cyberspace

In the cyber domain, potential vulnerabilities exist in all three parts of the command, control, and communications triad. Specifically,

> due to cyberspace's relatively low cost of entry, cyber threats range from state-sponsored offensive military operations and espionage activities, to [violent extremist organizations] intent on disrupting our way of life, to cyber criminals and recreational hackers seeking financial gain and notoriety. Additionally, the U.S. supply chain and critical infrastructure remains vulnerable to cyber attack, and even as we detect and defeat attacks, attribution remains a significant challenge.[18]

At present, assumptions are that NC3 is secured via a combination of air gaps, technological superiority in outer space and cyberspace, and human intervention in the control loop. Unfortunately, this is not always the case. In the intercontinental ballistic missile (ICBM) program, for instance, documented vulnerabilities include potential entry into the firewalled NC3 system, phony orders being conveyed via a backup antenna, distributed denial of service (DDoS) attacks on the nuclear infrastructure, and even a direct attack on thousands of feet of cable of the Hardened Intersite Cable System.[19] For the strategic ballistic missile submarine (SSBN) component, it has been widely publicized that the United States has chosen to use Linux-based operating systems in its SSBNs, as opposed to Windows XP-based architectures currently used by the British Trident program.[20] While neither of these operating systems is inherently problematic, the fact that their use in specific functional domains has been published so widely will enable hackers to focus on the correct class of exploits to use against these systems.[21] This observation, furthermore, hints at a distressing reality: with the emergence of ubiquitous cyber threats, the U.S. acquisition process has already begun moving toward increased levels of security and classification across the Department of Defense (DoD) enterprise, which hinders efficiency at all levels of the acquisition process. Without firing a shot, the opponent may well have caused substantial cost to the United States already due to the inefficiency resultant from broadly increased data security and classification procedures.

With the bomber airborne component of the command, control, and communications triad, the Air Force has experienced several NC3 breakdowns in the past several decades, the most recent of which involved the inadvertent placement of several nuclear warheads in a strategic bomber that

17. Harvey, "Nuclear Command and Control for the 21st Century."

18. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney Commander United States Strategic Command."

19. Blair, "Rogue States."

20. Futter, "Hacking the Bomb."

21. Fritz, "Hacking Nuclear Command and Control."

flew over the United States.[22] While this latter situation was not necessarily a cyber failure of commission, it is certainly one of omission in the sense that appropriate command and control safeguards were not in place to prevent such a mistake from occurring.

Critical infrastructure that either directly or indirectly supports the nuclear enterprise, such as the domestic power grid is also vulnerable to cyber attack.[23] Janet Napolitano, former secretary of homeland security, recently estimated that an adversary could disable one of the major U.S. power grids with 80 to 90 percent probability of success.[24] The frequency of such cyber vulnerabilities generally correlates with the size of the codebase—one can usually assume one error per thousand lines of code. For perspective, a generic Linux operating system had 15 million lines of code as of 2011.[25] Thus, while the National Nuclear Security Administration (NNSA) currently deploys a wide variety of cyber-defense techniques in defense of nuclear assets, including vulnerability scanning, firewalls, commercial antivirus systems, encryption, data loss prevention, data at rest security, network monitoring, enterprise forensics, and automated security control assessment, it is impractical to find every possible vulnerability in a large codebase and thus impossible to guarantee absolute security from zero-day exploits.[26] Further, post-detection attribution remains a challenge that usually takes weeks to sort out, meaning that attribution may be unachievable on timescales characteristic of a crisis.[27]

Combined Threats in Cyberspace and Outer Space

Many of the most daunting challenges for NC3 resilience lie at the intersection of cyberspace and outer space domains, where cyber attacks are directed at space-based NC3 assets. A recent study revealed substantial numbers of exploitable flaws in many widely used commercial satellite architectures, including the Iridium constellation, International Maritime Satellites (INMARSAT), and other satellites commonly used by both North Atlantic Treaty Organization (NATO) forces and critical infrastructure systems.[28] Key vulnerability categories included hard-coded credentials (undocumented credentials that can authenticate in documented interfaces), undocumented protocols (protocols not intended for end users), insecure protocols (end-user protocols that pose a security risk), and backdoors (mechanisms used to access features not intended for end users). Outcomes from reported exploits included control over systems as varied as

22. Douglas Raaberg, "Commander Directed Report of Investigation Concerning an Unauthorized Transfer of Nuclear Warheads," unclassified document, August 30 2007, available at http://scholar.harvard.edu/files/jvaynman/files/minot_afb_report.pdf.

23. Janene Scully, "VAFB Power Plant to Help During Crisis," *Lompoc Record* (Santa Maria, CA), June 4, 2001, http://lompocrecord.com/news/local/vafb-power-plant-to-help-during-crisis/article_a5129e90-46f6-5459-ad26-754a42294f52.html.

24. Ted Koppel, "How Vulnerable Is US to Cyberattack on Power Grid? Very," *News & Observer* (Raleigh, NC), November 3, 2015.

25. Danzig, *Surviving on a Diet of Poisoned Fruit*.

26. "Stockpile Stewardship Management Plan," National Nuclear Security Administration, 2016, https://nnsa.energy.gov/ourmission/managingthestockpile/ssmp.

27. James A. Lewis, personal conversation with the author.

28. Ruben Santamarta, "A Wake-up Call for SATCOM [Satellite Communications] Security," IOActive, April 17, 2014, http://blog.ioactive.com/2014/04/a-wake-up-call-for-satcom-security.html.

land-based communication and aircraft navigation, either of which could have a debilitating effect on MEECN integrity and ultimate NC3 efficacy. Understanding and mitigating the potential effects of these cyber threats to space-based assets will be imperative in ensuring the continued effectiveness of NC3.

LAWS OF ARMED CONFLICT: OLD RULES FOR NEW DOMAINS

While technical capabilities in outer space and cyberspace have continued to evolve, the laws of armed conflict have still not been updated to fully cover the new environment. Degradation of NC3 via cyber attack, with space-based assets being particularly vulnerable, can have a debilitating impact on the credibility of the nuclear deterrent. Even one successful cyber attack could have devastating consequences for global stability. As has been widely chronicled, the cyber domain poses unique difficulties to traditional application of conventional laws of armed conflict.[29] Such challenges are exacerbated when nuclear systems are involved.

For instance, to maintain nuclear strategic stability, it is generally helpful that any actions happen slowly (adversaries would have time to observe an action and respond), openly (actions can be observed by all parties and accurately attributed), and symmetrically (both sides can perform similar actions, and similar actions would cause similar levels of damage). Cyber operations against NC3, however, have none of these attributes. Activation of malicious code via backdoors or undocumented credentials can occur in a matter of seconds. Cyber attacks also have the potential to cause outcomes varying from simple annoyances all the way to catastrophic failures—occasionally, the only difference is a few lines of code that are not visible to the attacked party. Further, even if it were possible to detect and analyze every protocol stored or running on an NC3 system, attribution processes are generally too slow to enable accurate response in any time shorter than a matter of days, making it possible for the United States to be victimized by a debilitating cyber attack without knowing what adversary was responsible.[30] Finally, and perhaps most disturbingly, cyber attacks are not limited to state actors. While it would most likely require sophisticated hacker teams with significant financial backing to find any vulnerabilities in NC3-specific systems,[31] increasing levels of intermingling between conventional and nuclear command, control, and communications (C3) systems (notably in the satellite domain) means that additional vulnerabilities may well have been introduced into current NC3 architectures.[32] It is even possible that unanticipated threat vectors that could be accessible to amateur hackers have already been introduced into U.S. C3 systems. Thus, these realities represent a dangerous dynamic that fundamentally weakens the stabilizing framework of mutually assured destruction.[33]

---

29. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

30. Lewis, personal conversation with the author.

31. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*.

32. Harvey, "Nuclear Command and Control for the 21st Century"; Santamarta, "A Wake-up Call for SATCOM Security."

33. Danzig, *Surviving on a Diet of Poisoned Fruit*.

Given that many of these challenges will persist for the foreseeable future, it becomes important to consider how the United States should both deter and respond to cyber threats to NC3 systems in the context of international laws of armed conflict. Understanding these dynamics would not only elucidate specific policy challenges, but perhaps also assist in the process of formulating viable solutions to the difficult problem of credibly protecting NC3 via a combination of targeted technical development, cost-effective system deployment, and specific policy assertions. While a variety of documents exist that could be used to guide this process, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents a particularly appropriate framework for this analysis given that it was composed by an international group of experts (GoE) with the explicit goal of understanding how concepts of *jus ad bellum*, *jus in bello*,[34] and international humanitarian law apply to the cyber domain.[35] While the manual is not a formal statement of accepted international law and has not been broadly adopted, it represents a useful (though often nonunanimous) perspective from which to frame this discussion given its specific focus on "cyber operation[s] against a State's critical infrastructure, or a cyber attack targeting enemy command and control systems."[36]

Several key points that have particular application to NC3 are discussed here, with a particular emphasis on the interaction between the nuclear domain and cyber and space domains. Importantly, these ideas are not only considered from the U.S. point of view, but also from the standpoint of potential adversary nations who could conceivably use this framework as justification for actions taken against U.S. NC3.

Jurisdiction and Sovereign Immunity

Jurisdiction, which refers to the "authority to prescribe, enforce, and adjudicate," is allocated for cyber activities to any state "over (a) persons engaged in cyber activities in its territory, (b) cyber infrastructure located on its territory, and (c) extraterritorially, in accordance with international law." Importantly, national security threats including "any cyber operation that interferes with a state's military defensive systems (early warning radar and air defense)" constitute a valid justification for extraterritorial action. Further, the *Tallinn Manual* specifically states that "the fact that a State is capable of taking control of a piece of cyber infrastructure does not affect jurisdiction—specifically, a state can't take control of [a] commercial drone operated by another state over international waters." Logically, this should extend to satellites in the internationally accessible space domain as well.

Sovereign immunity fundamentally safeguards the right of a government to control its own systems. Specifically, "Sovereign immunity provides that assets controlled by the government of one sovereignty cannot be taken control of by another sovereignty without a violation of sovereignty—this includes vessels, aerial assets, and space assets."

---

34. *Jus ad bellum*: international law governing resort to force by States as an instrument of their foreign policy; *Jus in bello*: international law governing actions in armed conflict.

35. Scott Sagan, personal conversation with the author.

36. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

The jurisdictional and sovereign immunity arguments above indicate that any action taken against a satellite owned by a particular country would be generally prohibited outside of wartime. However, the GoE proposed several specific exceptions to this rule. First, in order to enjoy sovereign immunity, a particular platform must be *exclusively* performing government functions. In particular, the GoE makes the point that satellites with different transponders for commercial and non-commercial traffic do *not* have sovereign inviolability, meaning that countries could reasonably argue they are not violating U.S. sovereignty by interfering with satellites that perform key NC3 functions, but have other nongovernmental purposes as well.[37] Thus, even if broadly accepted, this specific portion of international law would not seem to provide a strong formulaic disincentive to cyber attacks on either dedicated NC3 communications satellites or those (e.g., AEHF) performing multiple functions including NC3. This is particularly true given that the *Talllinn Manual* only stipulates that a state should not "knowingly allow cyber infrastructure located within its territory or under its exclusive government control to execute operations harmful to another state." The question of what states should reasonably be expected to know about cyber infrastructure within their borders remains open.[38]

Responsibility

In general, a "state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation." However, states could be shielded from sanction for cyber operations by the clause stating that "the law of state responsibility is not implicated or prohibited by acts of international law, per se. Thus, a state's responsibility for cyber espionage is not to be engaged as a matter of international law."

While cyber espionage should be differentiated from cyber reconnaissance in the sense that espionage relates only to activities performed within an enemy state, it is nonetheless unclear that insertion of malicious code within an enemy C3 system from within its own networks would constitute an act punishable under international law, even if accurately attributed. However, the *Tallinn Manual* also explicitly indicates that a state may engage in counter-hacking if faced with aggressive hacking against its own critical infrastructure. The key technical issue here is that differentiating espionage and reconnaissance from aggressive attack can be nearly impossible, and that the same code could perform both functions under different operating conditions. Thus, the idea that espionage and attack should be treated differently seems to be inconsistent in the cyber domain, wherein perfect knowledge about enemy capabilities once inside a sensitive network will never be possible. While this particular section opens many questions that are beyond the scope of this work, the key point is that responsibility considerations do not specifically provide any sort of protection to NC3 systems from cyber attack.

Use of Force

The *Tallinn Manual*'s prescriptions on the use of force also do not provide protection for NC3 systems. First, even if passwords are broken and firewalls are bypassed, it states that "cyber espionage and exploitation lacking an element of coercion do not per se violate the non-intervention

37. Ibid.

38. Ibid.

principle." Technically, it would be very difficult to differentiate coercion from benign activity in real time. Further, the manual specifically states that encouraging or expressing support for others' activities does not cause a state to be held responsible, and, thus, while providing hacktivist groups with malware would comprise a use of force, funding them (or other forms of enabling, nontangible support) would not. Consequently, there exists little barrier in this framework to countries' funding extremely capable third parties to execute malicious cyber activities against U.S. NC3 on their behalf.[39]

Self Defense

A key consideration in the laws governing armed conflict is under what circumstances an entity is entitled to take action in self-defense. The asymmetric nature of the cyber domain has caused it to be one of the few arenas in which attacks by a non-state actor can trigger the right to self-defense.[40] Further, while a traditional school of thought has been that self-defense is only valid after an attack has been launched, the speed at which a first cyber attack would occur might obviate any chance for a response. The GoE considered this case, and strongly backed the applicability of "anticipatory self-defense" against a cyber attack. The idea behind this term is that a nation need not wait idly while enemies prepare a cyber attack; given the speed of cyber attacks, the "last window of opportunity to defend oneself" may well be before any attack has actually occurred.[41] An example given involves insertion of a logic bomb into a government's systems—however, in this case the GoE contends that this insertion does not per se represent an armed attack, and that such a determination should not only consider the consequences of the code, but also the achievability of the conditions for activation. Unfortunately, the practicality of this particular example is burdened by the fact that it is not generally possible to know the intent or inner operation of a piece of malware before time-consuming code analysis has taken place. As mentioned above, decisions regarding responses to a potential attack on nuclear systems must be made on far shorter timescales. Thus, anticipatory self-defense appears to be a particularly strong concept in support of preemptive action against prospective cyber attack on critical nuclear systems.[42]

Law of Armed Conflict

Once it has become apparent that states are in conflict, the Law of Armed Conflict (LOAC) applies to actions taken in the cyber domain. However, several aspects of the traditional LOAC require further exploration in the context of cyber attacks on NC3 systems. The question of proportionality, for instance, becomes very difficult to assess. Specifically, the LOAC states that active response to aggression should be similar in scope and magnitude, or "proportional," to the original aggression. If part of the nation's NC3 system were compromised by adversary action, however, what would be an appropriate response, particularly if no physical damage had been done? Is this considered an attack on the nuclear infrastructure, which could potentially merit a nuclear

39. Ibid.

40. Ibid.

41. Ibid.

42. Adm. James O. Ellis, personal conversation with the author.

response? While cyber attacks against adversaries would be permitted as a proportional response, would even proportional U.S. action against enemy NC3 systems cause escalation toward nuclear conflict? How should this risk be managed? For perspective, for a time it was Russian policy to respond to strategic cyber attack with the choice of any strategic weapon in its arsenal.[43] Finally, how does the United States consider attacks on systems that perform both conventional and nuclear C3 functions, such as AEHF satellites? Would a response from any element of the military be appropriate given the possibility of an implied nuclear threat? Each of these is an unanswered question that requires a nuanced response in the context of relevant technology and policy. The *Tallinn Manual* represents a good start in addressing many of these issues, but much work remains.

A TOUGH CONFLUENCE: PLAUSIBLE SCENARIOS, DIFFICULT DECISIONS

To bring an aspect of concreteness to the analyses above, it is helpful to consider two separate scenarios where cyber operations involving the space-based portion of NC3 are compromised. Each of these is purely hypothetical, but grounded in technical reality. Further, while the analysis presented here does not propose command-level solutions to these difficult problems, the goal will be to present difficult situations that remain possible today, but could be reduced in probability by a combination of technology and policy strategies outlined in a later section.

Malware Discovery: Is the United States at War?

First, consider a scenario where a piece of malware is found on a Military Satellite Communications (MILSATCOM) satellite involved in both conventional and nuclear C3. It is unclear what state of armed conflict the United States should consider itself to be in. Is this the lead-up to an attack (*jus ad bellum)?* Is this actually an attack (*jus in bello*)? Did this software originate from a non-state actor, and thus neither of the above would apply?

Given this uncertainty, the code is analyzed, and over the next several weeks it is determined that while the malicious code is exfiltrating data to some particular nation-state with 80 percent probability, it is not affecting system operability. In this case, how should the United States respond? There are several key issues and questions to consider, none of which has a particularly easy answer or solution:

1. During the time between discovery and analysis completion, it is impossible for the United States to know whether the malicious code has the capability to disable key NC3 functions in addition to simply exfiltrating data.
2. During the interval between discovery and tentative attribution, the United States would not have visibility into what type of actor has infiltrated the NC3 system (state or non-state), and further would be unable to take an appropriately specific defensive posture toward the potential attacker.

43. Futter, "Hacking the Bomb."

3. Under international law, it is unclear if 80 percent probability is sufficient to justify assignation of responsibility.
4. It is possible that this is not the only piece of malware affecting the NC3 system. Discovery is by no means perfect, and other, more damaging codes could exist.
5. Given the above uncertainty regarding espionage versus attack, and assuming the attribution is correct, what would be an appropriate proportional response? Though these actions do not necessarily demonstrate intent to disrupt nuclear operations given the combination of conventional and nuclear C3, they could nevertheless be a prelude to nuclear attack or nuclear coercion (in a conventional conflict).
6. The United States could consider developing internal tools to disrupt an opponent's NC3 (if it exists), but this could be counterproductive. For instance, snippets of the Stuxnet code—speculated to have been developed jointly by the United States and Israel to attack Iranian nuclear capabilities—have begun showing up in other parties' attack code. This situation illustrates how the United States' own offensive cyber tools can be repurposed in opposition to the national interest. In fact, dissection of U.S.-developed anti-NC3 codes by the adversary could well provide the insights a malicious party would need to greatly harm U.S. assets. Further, as far as Russia is concerned, even U.S. development of technology to interfere with NC3 is seen as inherently destabilizing; such considerations must necessarily play into decisions about whether tools to disrupt an opponent's NC3 should be developed.[44]
7. What is standard procedure for ensuring that NC3 is not compromised in the aftermath of a potentially malicious software activation? Should an event like this be disclosed to an international legal body? What steps can be taken to ensure that other parties do not attempt to take advantage of the fact that U.S. systems may be compromised?
8. Should anticipatory self-defense remain an option in such a scenario?

The Regional Scenario: Is the United States Fighting a Nuclear or Conventional War?

We now propose a scenario wherein the United States is involved in a conventional regional conflict with a peer nuclear power. Several recent studies have, for instance, explored the possibility either of a Russian attempt to annex the Baltic states or of a Chinese attempt at territorial expansion in the South China Sea.[45] In the course of such a conventional conflict, consider the set of issues and questions that would arise if a U.S. AEHF communications satellite suddenly ceased functioning:[46]

---

44. Lewis, personal conversation with the author.

45. David Shalpak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND, 2016); Bonnie S. Glaser, "Armed Clash in the South China Sea," Contingency Planning Memorandum No. 14, Council on Foreign Relations, April 2012, http://www.cfr.org/asia-and-pacific/armed-clash-south-china-sea/p27883.

46. Ellis, personal conversation with the author.

1. What are the consequences of a relatively important node in the communications network no longer functioning? Can this node be compensated for? How long would it take to replace?
2. Did the satellite simply malfunction, or was it attacked?
3. If it was a malfunction, is this a systemic issue with the AEHF constellation or an isolated incident?
4. If it was an attack, who was the aggressor, and what was the method of the attack? If this was a physical attack, what was the mechanism? If there are co-orbital objects moving, are they passive debris or an active enemy weapons system?
5. If this was a cyber attack, are other systems compromised or are other AEHF satellites at risk?
6. If this was an attack, was the goal to attack conventional or nuclear C3? Was the opponent attempting to degrade U.S. nuclear deterrent capability? Or was it a patriotic hacker attempting to stop conventional artillery fire near his hometown? How could the United States tell one of these situations from the other? Would it and should it matter in formulating a response?

NEXT STEPS: MOVING FROM PROBLEMS TO SOLUTIONS

One approach to the above scenarios would be an in-depth analysis of each question to determine exactly how the United States should respond. However, in light of substantial modernization to the NC3 system currently planned and under way, it is perhaps most useful to consider technological and policy avenues that could be pursued with the goal of ensuring that the above scenarios, each of which is fraught with uncertainty around nuclear intentions and appropriate U.S. response, would never come to pass. Distinct sets of technology and policy recommendations intended to inform discussion around modernization and design of the future nuclear enterprise are presented below.

Technological Directions

Several concrete technological initiatives would help reduce operational uncertainty and ensure resilient NC3 functionality.

Apply Advanced Forensics Techniques

All NC3 satellites should be outfitted with advanced forensics capability. Motion sensors, heat sensors, and EM intensity sensors should be emplaced in order to assess whether any given satellite inoperability resulted from external physical attack.[47] For protection from cyber attack, domestic control over supply chains should be pursued to reduce the possibility of backdoors, insecure or undocumented protocols, and hard-coded credentials. Finally, in addition to traditional antivirus scans of satellite software, commercially available assessments based on computationally efficient

47. Ibid.

code-level machine learning tools that proactively detect both new variants and repackaged versions of existing malware should be implemented.[48] Such methods should prove powerful in reducing the possibility of a successful cyber attack on NC3 systems.

Emphasize Modern Network Defense Techniques in NC3

Traditionally, network defense has focused on keeping attackers outside of a virtual "wall," while keeping all critical functionality accessible to those with valid credentials. In today's democratized cyber environment, cost to attackers is substantially lower than cost to defenders. Thus it is useful to consider moving toward an architecture that is more akin to a building with all of its doors open, but riddled with traps and misdirection. As NC3 is modernized to utilize Internet-based protocols,[49] for instance, considering widespread implementation of mechanisms designed to increase costs to attackers via such methods as honeypots, script white-listing, and address scrambling would help to deter and frustrate potential attackers. Honeypots, or environments that look like useful targets to an attacker but are in fact benign, can be particularly useful in enabling U.S. personnel to identify candidate attack vectors and enact defenses before critical systems are compromised. Script white-listing entails using efficient data structures to enable a computer to run only code with a bit representation that has been explicitly pre-specified as part of an allowed execution set. Finally, address space scrambling methods such as address space layout randomization (ASLR) protect from common buffer overflow attacks by randomly arranging address space positions of key portions of a process, such that an attacker cannot jump between different points reliably.

As a higher-level consideration, the United States should consider the idea that it is generally not possible to be completely sure that a networked computer system has not been compromised. If an adversary informed the United States that it had compromised U.S. NC3 and that surety of the nuclear deterrent had been affected, it would be extraordinarily difficult for the United States to prove otherwise, which fundamentally undermines the strength of the U.S. deterrent posture. Thus, it is imperative that the United States be able to viably make the argument that compromising the entirety of NC3 would be a statistical impossibility; and for this to occur, there must exist no possible mechanism for a single point of failure. While the command, control, and communications triad architecture ensures this posture adequately from a physical standpoint, it is imperative that NC3 systems be constructed with the same ideas in mind. Specifically, the United States should consider a fractionated NC3 network design, with a large number of sub-networks, each secured via different sets of protocols or standards. In this case, it would be nearly impossible for an adversary to convince either itself, the United States, or third parties that the surety of the U.S. nuclear deterrent could be fully compromised by what would effectively be a first cyber strike.

Minimize Code Base Size

As systems are modernized to take advantage of twenty-first century information technology (IT), the temptation will exist to implement a great deal of additional functionality. While there may exist

48. "Turning Cyberattack Prevention into a SecOps Advantage," Cylance, 2015, https://www.cylance.com/hubfs/2015_cylance_website/assets/case_studys/Malware_SecOps_v3.pdf?t=1465600534915.

49. Fritz, "Hacking Nuclear Command and Control."

substantial operational benefits to additional features, these should always be balanced with the reality that more code almost always equates to more vulnerability—and NC3 is an area wherein a vulnerability could result in mistakes of nuclear import.[50] Thus, the usual analysis around the cost-benefit trade-off of IT upgrades may not apply to NC3 systems, and this reality should be taken into account in system design processes.

Maintain Small-Scale Launch and Inexpensive NC3 Communications Hardware

A particularly interesting suggestion put forth by Dr. John Harvey, former principal deputy assistant secretary of defense for nuclear, chemical, and biological defense, is that "small, single-purpose 'cheap-SATs' to replenish lost communication or GPS [global positioning system] functionality" could improve system-level resilience of space-based NC3 assets. Instead of or in addition to large, multifunctional satellites, leveraging the widespread proliferation of small, inexpensive CubeSats[51] that cost on the order of $100,000[52] to construct and launch could substantially reduce overall system cost and improve reliability. In addition to allowing inexpensive system updates as technology improves, these small satellites would be extremely difficult to target for ASAT operators. Further, since Dr. Harvey's address in 2014, small-scale launch technology has seen significant advances. In fact, several commercial entities currently have the technology to offer 150-kilogram payloads to sun-synchronous orbit (500-kilometer altitude) on a single dedicated rocket costing only $5 million.[53] These rockets could be retained specifically for emergency NC3 launches as backups to current satellites. In this way, expensive AEHF satellites that would require an expensive, large-scale launch to reconstitute would be supplemented or ultimately replaced by a small satellite and dedicated launch ecosystem that would result in a substantially more resilient NC3 system. Moving to a reserve of small satellites as a backup for the NC3 network would also have the advantage of increasing the number of possible launch sites the United States can use. At present, only a handful exist, and these are well-known to any potential adversary.[54]

Decrease Reliance on Space-Based NC3

In addition to shoring up the reliability of space-based NC3, ultimately decreasing U.S. reliance on these assets would likely enhance overall NC3 surety.[55] In particular, relying more on the various airborne components of the NC3 system and deploying "long-range airborne communications relay networks that could be stood up on short notice" would potentially mitigate the vulnerabilities posed by cyber threats to space-based assets. This risk reduction would result not only from the ability to more rapidly deploy space-based systems, but also from the simple reality that

50. Danzig, *Surviving on a Diet of Poisoned Fruit*.

51. A variety of companies (e.g., Planet Labs), universities, national labs (e.g., Los Alamos National Laboratory), and research institutions already fly multiple CubeSats.

52. "Commercial Space Launch Schedule and Pricing," Spaceflight.com, accessed 31 July 2016, http://www.spaceflight.com/schedule-pricing/.

53. "Space Is Now Open for Business," Rocket Lab, accessed 31 July 2016, https://www.rocketlabusa.com/.

54. Ellis, personal conversation with the author.

55. Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment."

performing diagnostics and updates on hardware that is not in outer space is a far simpler process than the reverse.[56]

Policy Considerations

Carefully Consider Unilateral Action: Anticipatory Self-Defense and Belligerent Reprisal

Given the *Tallinn Manual*'s clear authorization of anticipatory self-defense and the potentially dire consequences of the scenarios outlined above, it would be prudent to pursue a national policy that enables U.S. intervention to combat the development of cyber capabilities that would compromise NC3. In the context of peacetime international law, this would likely entail either claiming extraterritorial jurisdiction over those developing anti-NC3 cyber capabilities and/or claiming anticipatory self-defense if an attack is imminent. Were the United States to already be engaged in an armed conflict, the functional equivalent of anticipatory self-defense would be legally termed belligerent reprisal.[57] In this case, if the United States views attacks on NC3 as outside the boundaries established by the LOAC, the question would become whether a proportional attack on opponent (potentially on their NC3) would be appropriate, and, if so, what form that proportional response would take. Even in the case that U.S. NC3 is compromised, for instance, it is still desirable from the U.S. point of view for the adversary's NC3 systems to be able to verify that the United States has not launched a nuclear attack. Thus, in the context of belligerent reprisal, it is critical to make a clear policy decision on what constitutes a proportional, but practically optimal response to an attack on U.S. NC3.

Implement Cooperative Measures and Policy Standards

Perhaps most importantly, the United States should pursue implementation of cooperative measures to set international ground rules for interaction with NC3 systems. In an analogy to the military case, as recently as 2013 a Russian expert recommended developing a "non-binding international document prohibiting attacks on civil nuclear assets."[58] Further, the proposal suggests that the international community should improve existing cooperative instruments for "warning, interdiction, and consequence management" among nation-states. Separately, a similar conversation around norms and expectations for nation-state operation in space is already under way.[59]

Ultimately, U.S. security leaders have suggested that any technological progression that moves world powers, particularly the United States, Russia, and China, away from mutually assured destruction and toward the possibility of asymmetric first strike capability requires careful management. Richard Danzig, former secretary of the navy, suggests that if such a progression were to occur, the United States should directly engage Russia and China in pursuing multilateral

---

56. Harvey, "Nuclear Command and Control for the 21st Century."

57. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

58. EastWest Institute, *A Measure of Restraint in Cyberspace: Reducing Risk to Nuclear Civilian Assets* (New York: EastWest Institute, 2014), https://www.eastwest.ngo/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf.

59. Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment."

agreements for parties to refrain from intrusion into nuclear warning, command, and control systems.[60] While this certainly represents a laudable goal, these agreements should perhaps move a step further and propose binding structures to combat any incursion into NC3 systems, enforcing them via some combination of sanctions and, if necessary, military force.

Separate NC3 and Conventional C3

Of all the policy recommendations considered here, the most direct and most effective would be to separate nuclear command and control systems from their conventional equivalents. While the current architecture may deter some low-level attacks by maintaining uncertainty about whether a particular cyber incursion would be considered nuclear in nature, it also comes with an inherent signaling risk that could lead to nuclear escalation. Were NC3 satellites to be explicitly separated from conventional C3 satellites and provided with a robust backup net (perhaps using a small satellite infrastructure), adversary intentions would be clarified substantially, and the United States could perhaps make its declaratory policy on NC3 incursions significantly more direct.

CONCLUSION

There remain many unanswered questions that both policymakers and operators need to consider as they move toward the next phase of NC3 technology. At present, assumptions are that NC3 is secured via a combination of air gaps, technological superiority in outer space and cyberspace, and human intervention in the control loop. Unfortunately, with the democratization of technology, asymmetric threats to space-based NC3 assets in particular have arisen that could fundamentally change the dynamics of nuclear strategic stability if not appropriately mitigated. To a degree, the uncertainty inherent in the current system can reinforce stability in the case of a risk-averse adversary, but could also undermine it in situations in which the adversary has nothing to lose.[61] A variety of technological initiatives including improving forensics, modernizing network defense, and moving to small satellite architectures could help improve the long-term surety of the NC3 architecture. Further, policy initiatives such as disaggregating nuclear and conventional C3, pursuing international agreements against NC3 incursions with key powers, and having a clear stance on application of the LOAC to cyber attacks on the nuclear enterprise would help both to mitigate risks to U.S. systems and actively deter malicious attacks against them. Ultimately, as the nation looks to maintain nuclear stability into the twenty-first century, it is imperative that critical nuclear security infrastructure be made robust to the myriad potential vulnerabilities resultant from the rapid spread of emerging technologies.

60. Danzig, *Surviving on a Diet of Poisoned Fruit*.

61. James Miller, personal conversation with the author.