



NUCLEAR WEAPONS IN THE NEW CYBER AGE

REPORT OF THE CYBER-NUCLEAR WEAPONS STUDY GROUP

SEPTEMBER 2018

By Page O. Stoutland, PhD and Samantha Pitts-Kiefer

Foreword by Ernest J. Moniz, Sam Nunn, and Des Browne



About the Cyber–Nuclear Weapons Study Group

In 2016, NTI convened a high-level Cyber-Nuclear Weapons Study Group to identify cyber vulnerabilities of nuclear weapons systems and develop recommendations to reduce those vulnerabilities and the potential consequences of a cyberattack. The Study Group includes high-level former and retired government officials, military leaders, and experts in nuclear systems and policy. The first phase of the project focused on vulnerabilities to U.S. nuclear weapons systems; the vulnerabilities of other countries will be examined in a later phase of the project. Participants in the Study Group are listed at the end of this report.

The Study Group met twice during the first phase. In September 2016, members validated the cyber threat as an issue of concern and began to identify the types of systems and attacks that could threaten nuclear weapons systems and lead to serious consequences. In June 2017, the group analyzed four plausible scenarios that characterized the highest-consequence cyber threats against nuclear weapons systems.

The Study Group gave NTI expert feedback on the draft content and recommendations of this report. Participation in the Study Group does not imply concurrence with each aspect of the report or its recommendations.

About the Nuclear Threat Initiative

The Nuclear Threat Initiative (NTI) works to protect our lives, environment, and quality of life now and for future generations. We work to prevent catastrophic attacks with weapons of mass destruction and disruption (WMDD)—nuclear, biological, radiological, chemical, and cyber. Founded in 2001 by former U.S. Senator Sam Nunn and philanthropist Ted Turner, who continue to serve as co-chairs, NTI is guided by a prestigious, international board of directors. Ernest J. Moniz serves as chief executive officer and co-chair, Des Browne is vice chair, and Joan Rohlfing serves as president.

www.nti.org

NUCLEAR WEAPONS IN THE NEW CYBER AGE

REPORT OF THE CYBER-NUCLEAR WEAPONS STUDY GROUP

SEPTEMBER 2018

By Page O. Stoutland, PhD and Samantha Pitts-Kiefer

Foreword by Ernest J. Moniz, Sam Nunn, and Des Browne



The views expressed in this publication do not necessarily reflect those of the NTI Board of Directors or institutions with which they are associated.

© 2018 Nuclear Threat Initiative

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission of the publisher and copyright holder.

Cover image (top): U.S. General Services Administration

Cover image (bottom): Zenobillis for Shutterstock

Table of Contents

Acknowledgments	4
FOREWORD	5
EXECUTIVE SUMMARY	7
UNDERSTANDING THE CYBER THREAT TO NUCLEAR WEAPONS AND RELATED SYSTEMS	9
POLICY RECOMMENDATIONS	21
CONCLUSION	29
MEMBERS OF THE STUDY GROUP	30
About the Authors	32

Acknowledgments

We are grateful to Nuclear Threat Initiative (NTI) Co-Chair and Chief Executive Officer Ernest Moniz, Co-Chair Sam Nunn, and Vice Chair Des Browne for their leadership on reducing nuclear threats and for serving as co-conveners of the Cyber-Nuclear Weapons Study Group. We also thank NTI President Joan Rohlfing for her important contributions to this project. NTI's leadership recognized the urgent need to address cyber threats to nuclear weapons and related systems, and their commitment to and intellectual engagement with this project was vital to its success.

We also owe a deep debt of gratitude to the members of the Cyber-Nuclear Weapons Study Group, which includes some of the most highly respected civilian and military experts from the United States and elsewhere. They have been extremely generous with their time, and we have done our best to ensure that their perspectives were taken into account as we wrote this report.

In addition, we would like to thank the NTI Board of Directors for its support, and we give special thanks to NTI's generous funders, including the John D. and Catherine T. MacArthur Foundation and the Carnegie Corporation of New York, for their support of this work.

Finally, we are indebted to our colleagues at NTI who provided invaluable contributions not only to our work on cyber threats to nuclear systems but also to this report. In particular, we thank Mimi Hall and Carmen MacDougall of NTI's communications team. We also thank Steve Andreasen, Catherine Crary, Erin Dumbacher, Brian Rose, and Lynn Rusten for their significant contributions to the project, as well as Hope Fasching, Mary Fulham, Julia Habiger, Andreas Pavlou, Alexandra Van Dine, and Margaret Williams for their additional support.

Page O. Stoutland, PhD

Vice President
Scientific and Technical Affairs
Nuclear Threat Initiative

Samantha Pitts-Kiefer

Senior Director
Global Nuclear Policy Program
Nuclear Threat Initiative

FOREWORD

By Study Group Co-Chairs
Ernest J. Moniz, Sam Nunn, and Des Browne

In 2013, the Pentagon’s Defense Science Board conducted a major study of the resilience of U.S. defense systems to cyberattacks. The results were deeply unsettling: the board found that the military’s systems were vulnerable and that the government was “not prepared to defend against this threat.”¹

In a successful cyberattack, the report warned, military commanders could lose “trust in the information and ability to control U.S. systems and forces.”²

The report made clear that “systems and forces” include nuclear weapons and related nuclear command, control, and communications systems. *Military commanders could face false warnings of attack or could lose trust in their ability to control U.S. systems and forces.* Let that sink in for a moment.

The world’s most lethal weapons are vulnerable to stealthy attacks from stealthy enemies—attacks that could have catastrophic consequences.

Today, that fact remains the chilling reality. Cyber threats are expanding and evolving at a breathtaking rate, and governments are not keeping pace. It is essential that the U.S. government and all nuclear-armed states catch up with—indeed, get ahead of and stay ahead of—this threat.

In our efforts to reduce vulnerabilities and prevent a cyberattack with potentially catastrophic consequences, NTI in 2016 released *Outpacing the Cyber Threat: Priorities for Cybersecurity at Nuclear Facilities*. That report addressed the risk that terrorists or other hackers could sabotage civilian nuclear facilities, resulting in a release of radiation; hold a nuclear facility hostage to their demands; or even use a cyber breach to facilitate the theft of nuclear bomb-making materials.

This new report, *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group*, addresses cyber risks to nuclear weapons systems and offers recommendations developed by a group of high-level former and retired government officials, military leaders, and experts in nuclear systems, nuclear policy, and cyber threats.

1 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Defense Science Board, January 2013), 1, <https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf>.

2 Ibid, 5.

As we work to improve technical security measures, all nuclear-armed states should be asking some bigger questions. If ultimately we cannot be confident that systems will work under attack from a sophisticated opponent, and if we cannot have full confidence in our ability to control nuclear weapons systems, what does this say about the continued viability of nuclear deterrence? In an age of cyberwarfare, has the nuclear deterrence strategy that helped guide the West and the Soviet Union through the Cold War become dangerously obsolete? Should our nuclear policies and force deployments be changed to mitigate the potential consequences of cyberattacks?

We believe the United States has an obligation to be a leader on addressing cyber threats to nuclear systems of all kinds, but especially to nuclear weapons systems. That is why this report is primarily U.S. focused. A subsequent effort will more directly address vulnerabilities in other countries because preventing nuclear use, whether by terrorists or by states, whether intentionally or by miscalculation, is a global issue. All countries with nuclear weapons and facilities must do more—much more—to protect their nuclear weapons and related systems. A weak link anywhere can result in catastrophe.

EXECUTIVE SUMMARY

Key Findings

- A successful cyberattack on nuclear weapons or related systems—including nuclear planning systems, early warning systems, communication systems, and delivery systems, in addition to the nuclear weapons themselves (collectively, “nuclear weapons systems”)—could have catastrophic consequences.
- Given the level of digitization of U.S. systems and the pace of the evolving cyber threat, one cannot assume that systems with digital components—including nuclear weapons systems—are not or will not be compromised.
- Technical cybersecurity measures are critically important and are being pursued in the face of determined and sophisticated adversaries, but they cannot, by themselves, provide sufficient confidence in the security and reliability of critical systems, including nuclear weapons systems.
- Cyber threats to nuclear weapons systems increase the risk of use as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and could undermine confidence in the nuclear deterrent, affecting strategic stability.
- The risk of nuclear use as a result of miscalculation or of unauthorized use existed before cyber threats became prevalent, but the cyber threat exacerbates those risks and creates new ones. The speed, stealth, unpredictability, and challenges of attribution of any particular cyberattack make it exceedingly difficult, if not impossible, to anticipate, deter, and defend against all cyber threats.
- Many digital nuclear systems are old by technological standards. As they are modernized, care must be taken to ensure that additional vulnerabilities are not introduced.
- Addressing these threats will require changes to U.S. nuclear policies and posture. Moreover, because the implications to strategic stability have global effects and because other countries also face cyber threats, a global approach to address the problem is necessary.

Policy Recommendations

The policy recommendations in this report are divided into the four categories that follow. The recommendations represent an initial, high-level set of priorities for measures to mitigate the cyber threat to nuclear weapons systems and can serve as a starting point for additional in-depth analysis.

1. Reducing the risk of launch as a result of miscalculation

- Develop options to increase decision time to account for cyber threats to early warning systems.
- Establish norms to restrict cyber weapons use against nuclear weapons systems.
- Enhance survivability and resilience of nuclear systems and Nuclear Command, Control, and Communications (NC3) processes.

2. Reducing risks to the nuclear deterrent

- Secure and diversify critical systems.
- Prioritize addressing cyber risks in modernization plans.
- Maintain a cadre of experts.

3. Reducing the risk of unauthorized use

- Enhance security of nuclear weapons, and review vulnerabilities of nuclear weapons to blended physical and cyber attacks.

4. Taking a global approach to the cyber threat to nuclear weapons systems

- Initiate bilateral dialogue with Russia.
- Increase international cooperation to reduce the cyber threat.

UNDERSTANDING THE CYBER THREAT TO NUCLEAR WEAPONS AND RELATED SYSTEMS

The Cyber Threat to Nuclear Weapons and Related Systems

Cyber-based threats target all sectors of society—from the financial sector to the entertainment industry, from department stores to insurance companies. Governments face an even more critical challenge when it comes to cyberattacks on their most critical systems. Attacks on critical infrastructure could have extraordinary consequences, but a successful cyberattack³ on a nuclear weapon or related system—a nuclear weapon, a delivery system, or the related Nuclear Command, Control, and Communications (NC3) systems—could have existential consequences. Cyberattacks could lead to false warnings of attack, interrupt critical communications or access to information, compromise nuclear planning or delivery systems, or even allow an adversary to take control of a nuclear weapon.

Given the level of digitization of U.S. systems and the pace of the evolving cyber threat, one *cannot assume that systems with digital components—including nuclear weapons systems—are not or will not be compromised*. Among the reasons: nuclear weapons and delivery systems are periodically upgraded, which may include the incorporation of new digital systems or components. Malware could be introduced into digital systems during fabrication, much of which is not performed in secure foundries. In addition, there are a range of external dependencies, such as connections to the electric grid, that are outside the control of defense officials but directly affect nuclear systems. Finally, the possibility always exists that an insider, either purposefully or accidentally, could enable a cybersecurity lapse by introducing malware into a critical system.

Increased use of digital systems may also adversely affect the survivability of nuclear systems. New technologies can enhance reliability and performance, but they can also lead to new vulnerabilities in traditionally survivable systems, such as submarines or mobile missile launchers.⁴

3 For the purposes of this report, we adopt the following definition: *cyberattack* refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems and networks. See National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William Owens, Kenneth Dam, and Herbert Lin (Washington, DC: National Academies Press, 2009), <https://doi.org/10.17226/12651>.

4 Paul Bracken, “The Intersection of Cyber and Nuclear War,” *Real Clear Defense*, January 17, 2017, https://www.realcleardefense.com/articles/2017/01/17/the_intersection_of_cyber_and_nuclear_war_110646.html.

The Trump administration's Nuclear Posture Review recently recognized the cyber threat to NC3 systems: "The emergence of offensive cyber warfare capabilities has created new challenges and potential vulnerabilities for the NC3 system. Potential adversaries are expending considerable effort to design and use cyber weapons against networked systems. While our NC3 system today remains assured and effective, we are taking steps to address challenges to network defense, authentication, data integrity, and secure, assured, and reliable information flow across a resilient NC3 network."⁵

**ALTHOUGH TECHNICAL
CYBERSECURITY MEASURES
ARE CRITICALLY IMPORTANT
AND ARE BEING PURSUED,
THEY CANNOT ALONE PROVIDE
SUFFICIENT CONFIDENCE
IN THE SECURITY AND
RELIABILITY OF CRITICAL
SYSTEMS, INCLUDING
NUCLEAR WEAPONS SYSTEMS.**

This recognition follows previous work that highlighted the magnitude of the cyber threat to nuclear weapons systems and warned about the ability to address the threat solely through technical means. In 2013, the Defense Science Board (DSB) conducted a major study to provide recommendations to improve the resiliency of Department of Defense systems against cyberattacks. *One of the DSB report's striking conclusions was that "The United States cannot be confident that our critical Information Technology systems will work under attack from a sophisticated and well-resourced opponent."*⁶ The board concluded that no technical approaches are available to "comprehensively" protect the Department of Defense against an adversary determined to inflict harm. The report recommended "immediate action to assess and assure national leadership that the current U.S. nuclear deterrent is also survivable against"⁷ the most significant cyber threats identified in the report.

In January 2017, a second DSB study recommended that the Pentagon undertake a series of initiatives, including planning and conducting tailored deterrence campaigns, creating a cyber resilient "thin line" of key U.S. nuclear and nonnuclear strike systems, and enhancing foundational

capabilities to improve U.S. cyber resilience, including through greater attribution capabilities.⁸

The DSB reports and subsequent discussions with experts led NTI to conclude that the cyber threat is of a character such that *special measures must be taken as a matter of the highest priority to protect nuclear weapons systems, and that although technical cybersecurity measures are critically important and are being pursued, they*

5 U.S. Department of Defense, Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, DC: Department of Defense, February 2018), 57, <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>.

6 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Defense Science Board, January 2013), 1, <https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf>.

7 Defense Science Board (2013), 42.

8 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Defense Science Board, February 2017), https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf.

cannot alone provide sufficient confidence in the security and reliability of critical systems, including nuclear weapons systems.

Notwithstanding the administration's statement in the recently issued Nuclear Posture Review that the "NC3 systems remain assured and effective," this, at best, can only be a point-in-time assessment. We believe that the more realistic view of the cyber danger is contained in the pages of the DSB's 2013 report. The conclusions found therein that the government can no longer assure, now or in the future, that nuclear weapons systems will always operate as designed (or that they can be fully secured against unauthorized use)—coupled with the unavoidable assumption that other states with nuclear weapons face similar challenges—have significant implications. There is no question today that *cyber threats to nuclear weapons systems increase the risk of use as a result of miscalculation; increase the risk of unauthorized use of a nuclear weapon; and, for some, could undermine confidence in the nuclear deterrent, affecting strategic stability.* Addressing those implications will require adjustments to U.S. nuclear policies and posture and, in all likelihood, to the nuclear policies and postures of other states with nuclear weapons.

Is the Threat Real?

No cyberattacks on nuclear weapons systems have been publicly disclosed to date, but historical incidents provide some indication of what could happen. For example, in 1980, warning systems showed missiles headed for the United States.⁹ In the minutes remaining before the president would have had to order a retaliatory strike, the warning was determined to be a false alarm caused by a faulty computer chip. More recently, in 2010, 50 nuclear-armed missiles based in Wyoming were offline for nearly an hour because of a computer hardware failure.¹⁰

Those are the kinds of incidents that, particularly in a crisis or conflict, could bring leaders to the brink of ordering a nuclear attack on the basis of faulty information and could undermine the confidence in military systems that is needed to prevent a grave mistake.

Cyber threats are rapidly evolving—but today, the risks of greatest concern associated with a cyberattack on nuclear weapons systems are:

- **Risk of launch as a result of miscalculation.** When coupled with today's nuclear posture—nearly 1,000 nuclear weapons poised to launch within minutes and a ground-based force vulnerable to a disarming first strike—a cyberattack on early warning systems to credibly spoof an incoming nuclear attack would create a high risk of a miscalculated nuclear response. Similarly, during a conflict, the detection of a malicious code in the command and control system that is assessed or reported to be capable of rendering some or all strategic forces inoperable also could heighten the risk of use. In part because intercontinental ballistic missiles (ICBMs) must be launched quickly

9 Patricia M. Lewis, Heather Williams, Benoît Pelopidas, and Sasan Aghlani, *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Chatham House, 2014), https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20140428TooCloseforComfortNuclearUseLewisWilliamsPelopidasAghlani.pdf.

10 "Air Force Loses Contact with 50 ICBMs at Wyoming Base," Nuclear Threat Initiative, October 27, 2010, <http://www.nti.org/gsn/article/air-force-loses-contact-with-50-icbms-at-wyoming-base/>.

“It is imperative that we regularly assess and address any cyber vulnerabilities in our nuclear arsenal, as it is certain that adversaries are looking for these very same weaknesses. We must make it our priority to find and address them first.”

—*Debra Plunkett*
STUDY GROUP MEMBER

to survive an incoming nuclear first strike, the president would be under extreme pressure to make a decision about whether to launch those weapons based on a warning of an attack, including a potential false warning caused by cyber means or otherwise.

- **Risk of unauthorized use.** Cyberattacks could be used in combination with a physical attack to defeat the security of nuclear weapons, leading to theft or unauthorized use of a nuclear weapon, with potentially catastrophic results. Another possible, although perhaps less credible, scenario would be an illicit or unauthorized order to launch nuclear weapons through a compromised command and control system.
- **Reduction of confidence in the nuclear deterrent and the effect on strategic stability.** In addition to heightening the risk of use as a result of miscalculation or unauthorized launch, cyber threats to nuclear weapons systems could undermine the very foundation of nuclear deterrence and strategic stability. The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not. For example, cyberattacks against communications systems could prevent the flow of information vital for making decisions about the use of nuclear weapons, including responding to warnings of attack; disable the ability to transmit nuclear orders; cut off much-needed de-escalation channels between nations in a crisis; or lead to misinterpretation if dual-use systems are attacked with no way to clarify the adversary’s intentions. In addition, the introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent. Confidence in the ability to use nuclear weapons as intended, and the adversary’s belief that the country’s weapons could be used and would work as intended, are vital ingredients for nuclear deterrence. A loss of confidence in the ability to deter nuclear use by an adversary would have a significant negative effect on strategy stability.

It is important to note that these risks existed before cyber threats became prevalent. False warnings because of human error or technical failures have occurred multiple times in the nearly seven decades since nuclear weapons were developed. The cyber threat exacerbates those risks and creates new ones. The speed, stealth,

unpredictability, and challenges of attribution of any particular cyber threat or attack make it exceedingly difficult, if not impossible, to anticipate, deter, and defend against such an attack. Furthermore, nuclear weapons are dependent on systems with digital components, including those connected to civilian systems.

Because of the unique character and implications of cyber risks, recommendations to address them are more urgent, particularly now as the United States implements policies set forth in the Trump administration's Nuclear Posture Review (NPR). The NPR establishes priorities that affect nuclear use policies, force posture, force structure, and modernization plans for years to come.

Four Illustrative Scenarios

The Study Group examined four scenarios that illustrate the implications of the cyber threat to nuclear weapons and related systems. When considering the scenarios, group members looked beyond the immediate potential risks of a cyberattack against nuclear weapons systems—

that is, an increased risk of use as a result of miscalculation or an unauthorized launch—and analyzed how vulnerabilities and risks affect strategic stability and nuclear deterrence because of a loss of confidence in the nuclear deterrent. Deliberations within the Study Group revealed that cyber threats could potentially compromise confidence in nuclear weapons systems.

The scenarios are considered plausible and representative of the most significant threats and vulnerabilities facing nuclear weapons systems. Addressing those threats and vulnerabilities would have broad implications for protecting critical nuclear weapons systems from cyberattack, including other, less catastrophic scenarios. The likelihood that any of the scenarios described below could be initiated by state or nonstate actors varies and will continue to evolve. Insiders could also play a role (either inadvertently or maliciously) and therefore must be taken into account.

Scenario 1: Warning systems provide false indications of a nuclear attack during a crisis.

At a time when tensions with Russia are as high as at any time since the Cold War, screens light up at North American Aerospace Defense Command (NORAD) with warnings of incoming missiles—many of them. It's the middle of the night, and when the call comes into the White House that a devastating attack may be under way, the president and his military aides have only minutes to decide whether and how to respond. They know it's possible that our early warning systems have been



Technicians prepare a Space Tracking and Surveillance Satellite for launch in 2008.

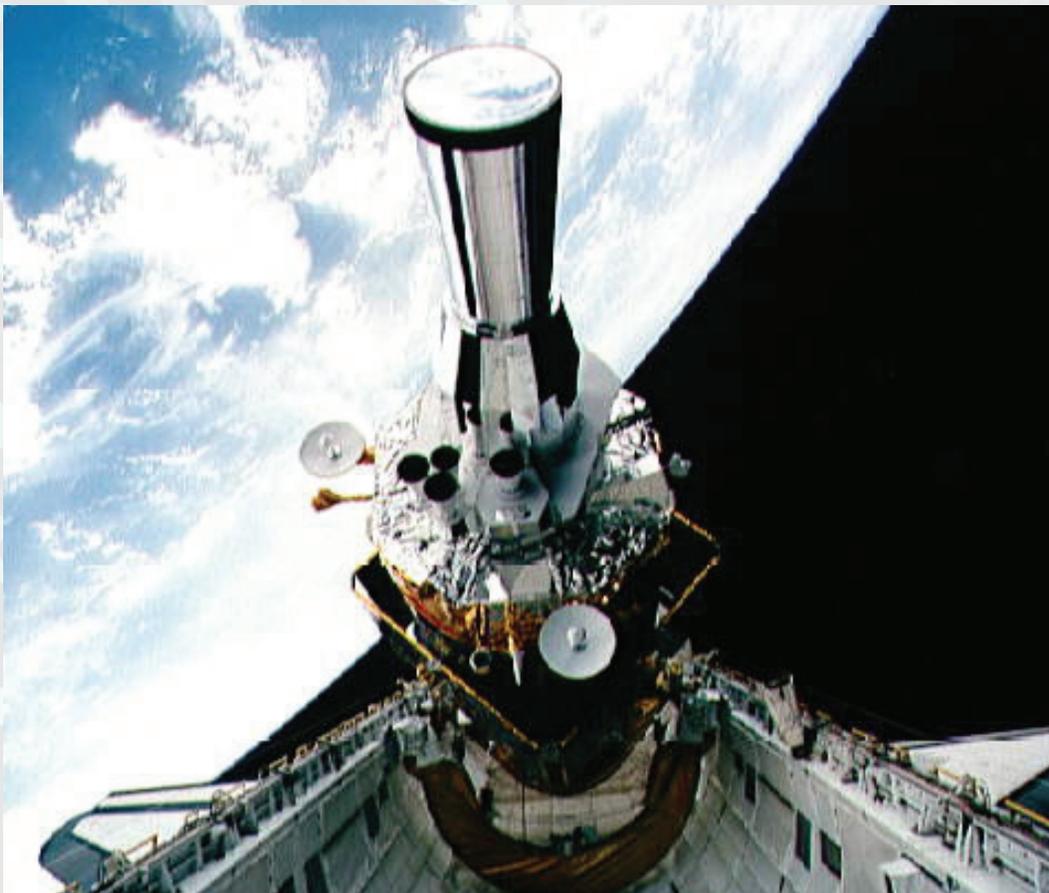
DUAL-USE CAPABILITIES AND THE CHALLENGE OF RISK MITIGATION

The dual-use nature of Communication, Command, and Control (C3) systems—for example, satellites that support both conventional and nuclear capabilities—heightens the risks posed by cyberattacks. Attacks on C3 systems, historically used early in a conventional conflict, could be perceived as an attack to undermine a country's ability to use its nuclear weapons.

Integration of conventional and nuclear C3 systems has multiple drivers. In some cases, it is motivated by a desire to minimize the number of distinct systems or to lower costs. In other cases, some countries may do it as a way to deter attacks on their systems. Regardless, the result is that an attack on such systems, whether intentional or not, would potentially be perceived as undermining a

country's nuclear deterrent.

To reduce those risks, the United States and other countries with nuclear weapons could pledge not to attack C3 systems supporting a country's nuclear deterrent. Given the highly integrated nature of some of those systems, however, such an agreement would be difficult to reach—and even if it could be reached, it would be essentially impossible to verify. As an alternative, countries could agree to separate their conventional and nuclear systems and make clear that any attack on a nuclear system would lead to serious consequences. That agreement could be valuable over time, but it would require a sustained effort to ensure that no unintended connections exist between conventional and nuclear systems.



A Defense Support Program early-warning satellite is placed into orbit during Space Shuttle Mission STS-44 in 1991.

“The cyber threat to nuclear weapons is an international problem and will require concerted global engagement. A cyberattack that either causes a nuclear launch or explosion, or precipitates, exacerbates, and deepens a nuclear crisis is something that everyone has an interest in preventing. The most pressing challenge is therefore to bring together nuclear-armed states and seek agreement on preventing the most dangerous dynamics presented by the new cyber threat.”

—Andrew Futter
STUDY GROUP MEMBER

spoofed, but they have insufficient time to determine whether that is the case before deciding to launch a counterattack or risk losing a significant percentage of the U.S. nuclear deterrent.¹¹

Could it happen?

Absolutely. Although warning systems are well protected, this scenario is plausible, as evidenced in at least two cases: the 1980 failure of a NORAD computer chip that resulted in false warnings of an incoming nuclear attack,¹² and the 1983 Soviet misperception of sunlight reflecting off clouds as five incoming missiles.¹³ Those incidents were caused by human or technical error, not malfeasance, but similar incidents could be caused deliberately. For example, infrared sensors—which detect the plumes of ballistic missiles—could be tampered with at some point in the supply chain through which the missile systems are acquired. Alternatively, false alerts of an incoming attack could be spoofed and communicated through early warning computer systems.¹⁴

Such a scenario most plausibly would be initiated by a nonstate or third-party actor.

11 An alternative scenario, one that is more likely in the case of a state action, is an adversary using a cyberattack to disrupt early warning systems to mask an incoming nuclear attack.

12 “The 3 A.M. Phone Call,” The Nuclear Vault, *The National Security Archive*, March 1, 2012, <https://nsarchive.gwu.edu/nukevault/ebb371/>.

13 Anthony M. Barrett, “False Alarms, True Dangers? Current and Future Risks of Inadvertent U.S.-Russian Nuclear War,” (Santa Monica, CA: Rand Corporation, 2016), https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE191/RAND_PE191.pdf.

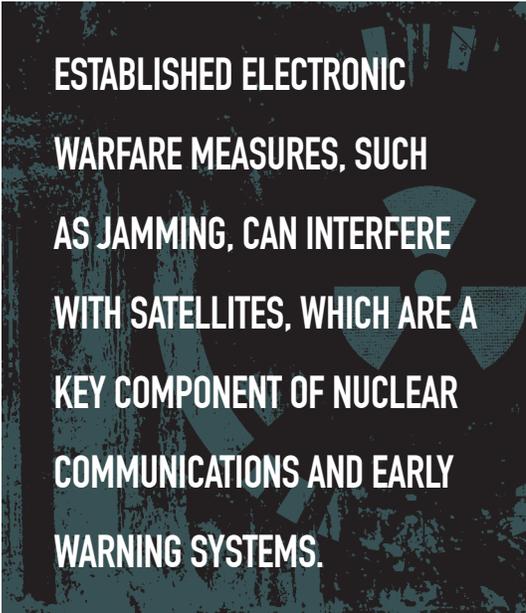
14 Lee Billings, “War in Space May Be Closer Than Ever,” *Scientific American*, August 10, 2015, <https://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/>; Colin Clark, “US Challengers Can Spoof, Dazzle, Cyber Attack US Satellites: DepSecDef,” *Breaking Defense*, April 13, 2016, <https://breakingdefense.com/2016/04/us-challengers-can-spoof-dazzle-cyber-attack-us-satellites-depsecdef/>; Patricia Lewis and David Livingstone, “The Cyber Threat in Outer Space,” *Bulletin of the Atomic Scientists*, November 21, 2016, <https://thebulletin.org/cyber-threat-outer-space10178>.

Scenario 2: A cyberattack disrupts communications between officials, operators and nuclear systems, and/or international counterparts in a potential crisis.

In the middle of a political crisis between Russia and the United States, Russian military commanders try frantically to reach their U.S. counterparts to determine whether what would seem to be an unlikely warning of incoming missiles is real. The Russians are aware that hackers have tried to infiltrate their systems in recent months, but they have no way of knowing whether the warnings they are receiving are real or fake—and the communications systems they rely on to de-escalate a crisis are down.

This scenario, which involves the disruption of vital communications in a nuclear crisis, could unfold in a number of ways to break communications channels between officials, between operators and nuclear systems, or between international counterparts. An adversary also could use a cyberattack to do the following:

- Disrupt or sever communications between political decision makers and the military leaders and communications systems that convey launch orders, preventing the flow of information necessary to make an informed decision about how to respond to a nuclear attack and to execute that response;
- Disrupt or sever communications between operators and nuclear systems, preventing those operators from obtaining information about those systems that are needed by decision makers or from relaying information to those systems;
- Disrupt dual-use (conventional and nuclear) communications as part of a strategy to disable conventional U.S. warfighting capabilities in the early stages of a conflict; or
- Disrupt or sever communications between international military and/or political counterparts, preventing the use of channels to de-escalate a crisis.



ESTABLISHED ELECTRONIC WARFARE MEASURES, SUCH AS JAMMING, CAN INTERFERE WITH SATELLITES, WHICH ARE A KEY COMPONENT OF NUCLEAR COMMUNICATIONS AND EARLY WARNING SYSTEMS.

Could it happen?

These scenarios are plausible, as evidenced by several cases. In 2010, a technical malfunction caused a 45-minute loss of communication with a squadron of 50 nuclear-tipped ICBMs in Wyoming.¹⁵ A cyberattack could have done the same. Other distributed denial-of-service (DDoS) attacks show that compromising key communications infrastructure can prevent one party from reaching another. In 2015, a DDoS cyberattack involving Ukraine's power grid cut service to the power company's customer service phone lines, preventing the transmission of information about the

¹⁵ Bruce Blair, "Could Terrorists Launch America's Nuclear Missiles?" *Time*, November 11, 2010, <http://content.time.com/time/nation/article/0,8599,2030685,00.html>.

KEY CYBER VULNERABILITIES AND POTENTIAL CONSEQUENCES

	POINT OF VULNERABILITY	TYPE OF ATTACK	POTENTIAL CONSEQUENCE
	Early Warning Systems: Radars and Satellites	Spoof of an incoming nuclear attack	Nuclear launch based on false warning
	Communications Systems	Cyberattack disrupts or disables communication channels between officials, operators/systems, international counterparts	Nuclear launch based on misinterpretation of information/inability to de-escalate crisis OR Loss of confidence in ability to issue launch orders to respond to nuclear attack
	Supply Chain	Malware or malicious code introduced into a nuclear weapon component	Loss of confidence in nuclear weapon operating as intended
	Security Systems	Cyberattack disables or defeats physical security measures	Theft of nuclear weapon

power outage.¹⁶ Another attack was caused by the Slammer worm, which overloads networks and disables database servers, severing internet connectivity for websites as the worm consumes all available bandwidth.¹⁷ This worm was able to infect Ohio's Davis-Besse nuclear power station in 2003, shutting down safety parameter display systems for five hours and preventing operators from seeing sensitive information about the reactor core. It may be possible to use similar techniques to overload key communications networks related to nuclear command and control, preventing their use in a crisis. Additionally, established electronic warfare measures, such as jamming, can interfere with satellites, which are a key component of nuclear communications and early warning systems.¹⁸

16 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

17 David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "Inside the Slammer Worm," *Security & Privacy Magazine*, IEEE Computer Society, July/August 2003, <http://www.icsi.berkeley.edu/pubs/networking/insidetheslammerworm03.pdf>.

18 Robert K. Ackerman, "Space Vulnerabilities Threaten U.S. Edge in Battle," *Signal*, AFCEA, June 2005, <http://www.afcea.org/content/?q=space-vulnerabilities-threaten-us-edge-battle>; FAS Panel on Weapons in Space, "United States Space Systems: Vulnerabilities and Threats," in *Ensuring America's Space Security: Report of the FAS Panel on Weapons in Space* (Washington, DC: Federation of American Scientists, September 2004), https://fas.org/pubs/_docs/10072004163734.pdf.



A cascade of gas centrifuges at a U.S. enrichment plant

Scenario 3: An adversary introduces a flaw or malevolent code into nuclear weapons through the supply chain or otherwise in a way that could compromise the effectiveness of those weapons.

As digital components of nuclear weapons or delivery systems are being assembled, an adversary who has evaded detection through the company's background checks is able to introduce malicious code or malware into the components. The malware could be activated at any time (including at the height of a crisis), undermining confidence in nuclear weapons systems and, indeed, their operational effectiveness, leading to escalation of the crisis. In fact, even a false—but credible—claim

of having introduced malware could have the same effect.

Perhaps more likely and most dangerous, the discovery of a flaw or malevolent code—before or after it is used offensively—could be destabilizing during a crisis when the intent of the adversary may be unclear. This is particularly the case when the code is embedded in dual-use systems with both conventional and nuclear applications (e.g., U.S. early warning and NC3 satellites). Decision makers would have to consider whether and how to react, whether the problem is targeted or widespread, and whether additional flaws or follow-on attacks may be coming. Finally, in the most extreme but least likely case, revealed compromises could embolden an adversary to strike or force the United States into a use-or-lose posture because of diminishing confidence in its nuclear weapons capabilities.

Could it happen?

Concern over supply chain security has been highlighted in other related industries. The Air Force Studies Board studied the issue in 2016 as it relates to electronic components procurement. At a workshop, presenters from across industry confirmed that the defense supply chain can be compromised and that serious concerns exist about malware insertion into manufactured parts.¹⁹

Although many key nuclear weapons components are produced in secure foundries, it is not safe to assume that components used in NC3 systems would be immune from supply chain vulnerabilities. The National Nuclear Security Administration has warned, "The trend toward a non-domestic supply chain for components of nuclear weapons systems may pose risks to these weapons and systems."²⁰ Because of the sheer complexity of those systems, vulnerabilities may exist at numerous places along the line.

19 *Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components: Proceedings of a Workshop* (Washington, DC: National Academies Press, 2016), <https://www.nap.edu/read/23561/chapter/2>.

20 "DOE Should Assess Circumstances for Using Enhanced Procurement Authority to Manage Risk," *GAO Highlights*, August 2016, <http://www.gao.gov/assets/680/678999.pdf>.

“Nuclear weapons systems are likely to remain vulnerable to cyber threats regardless of what cybersecurity improvements are made in the future, so much so that changes in nuclear posture are necessary to compensate for risks introduced by the cyber threat.”

—Herb Lin
STUDY GROUP MEMBER

Similarly, an adversary could place a dormant code somewhere in a critical system for use later in a conflict. In early 2017, reports indicated that the Obama administration had a plan to covertly plant cyber weapons in Russian critical infrastructure.²¹ In early 2018, U.S. officials reported that Russian hackers had established a foothold in U.S. and European critical infrastructure.²² Although it is unclear whether the program moved forward, the reports indicate an interest in a latent cyber capability available for future use. In addition, the United States and other countries, such as Russia and China, are widely reported to use a range of offensive cyber capabilities to support military operations, including counterterrorism.²³

Finally, there is uncertainty about the degree to which critical nuclear weapons systems can be isolated from conventional systems, so the risks and trade-offs associated with disrupting or attacking dual-use nuclear/conventional systems may not be clear to an adversary.

Scenario 4: An adversary is able to achieve unauthorized control of a nuclear weapon through cyber-assisted theft and/or defeating of security devices.

During a period of dramatic political unrest in a European country where U.S. forward-deployed nuclear weapons are stored, base commanders temporarily lose control of the facilities housing the weapons when the base security systems go down. Weeks later, at least one weapon is determined to be missing.

Could it happen?

This scenario involves an adversary’s ability to steal or otherwise gain unauthorized control of a nuclear weapon or weapons component, potentially leading to use of that weapon. Although a spoofed authorization to deploy nuclear weapons through a compromised command and control system that would result in the unauthorized launch of a nuclear weapon is less credible than other scenarios, this risk may increase in the future.

21 Greg Miller, Ellen Nakashima, and Adam Entous, “Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault,” *Washington Post*, June 23, 2017, <https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/>.

22 See, for example, Nicole Perloth and David E. Sanger, “Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says,” *New York Times*, March 15, 2018, <https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html>.

23 David E. Sanger, “U.S. Cyberattacks Target ISIS in a New Line of Combat,” *New York Times*, April 24, 2016, <https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html>.

Meanwhile, past incidents in which the security or control of forward-deployed nuclear weapons was compromised, combined with established instances of cyber measures used to defeat access controls, suggest that this scenario should be of concern.

In 2016, U.S. forward-deployed nuclear weapons stored at Turkey's Incirlik Air Base in support of extended deterrence for NATO were under serious risk as a result of a military coup in that country. During the coup, power was cut to the base, U.S. Air Force planes were grounded, and the Turkish base commander was detained under suspicion of involvement in the coup. Clearly, chaotic situations, especially where weapons are forward deployed, can and do arise. Cyber tools could be used to compromise the access controls in place to protect these weapons from unauthorized individuals.



POLICY RECOMMENDATIONS

Guiding Principles

Using the four scenarios as a framework for discussion and debate, NTI, with input from the Study Group, developed recommendations to reduce the risk that a cyberattack on nuclear weapons systems could lead to catastrophic consequences. The recommendations were developed based on the following guiding principles:

1. The United States will continue to require a safe, secure, and reliable nuclear deterrent as long as nuclear weapons remain a central element of its security strategy.

As long as nuclear weapons remain relevant to deterrence, measures must be pursued to reduce the cyber threat to nuclear weapons systems as much as possible, even if the risk cannot be entirely eliminated. The cyber threat will continue to evolve so rapidly that significant changes in nuclear weapons policy, posture, and structure will be necessary to mitigate cyber risks to nuclear weapons systems.

2. Technical measures alone are unable to completely eliminate the cyber threat to nuclear weapons.

Although technical cybersecurity measures are critically important and should be pursued, they alone will not provide sufficient confidence in the security and reliability of critical systems, including nuclear weapons systems. Instead, the government must operate under the assumption that given the level of digitization of our systems and the pace of the evolving cyber threat, systems with digital components, including nuclear weapons systems, may already be compromised.²⁴

3. The cyber challenge is global, and a unilateral approach is not sufficient.

The cyber threat affects all nuclear-armed states; therefore, bilateral and multilateral actions are necessary. Although this report focuses on examining threats and vulnerabilities in the United States and most of the recommendations are intended for the U.S. government, U.S. unilateral actions alone are insufficient. In some cases, unilateral actions might lead to greater instability if efforts to secure U.S. systems create significant asymmetries in states' ability to secure and have confidence in their systems.

²⁴ Richard Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies," *Center for a New American Security*, July 21, 2014, <https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies>.

CURRENT U.S. EFFORTS TO ADDRESS THE CYBER THREAT TO NUCLEAR WEAPONS

Publicly available information suggests that the United States is increasing its emphasis on addressing cyber threats to nuclear weapons systems. Although the specifics are not publicly available, some details on new and ongoing cyber resilience modernization priorities can be derived from U.S. defense budgets.

For example, the U.S. Navy and Air Force are each spending approximately \$500 million to make improvements to strategic command and control. Those improvements include upgrading communications links between all elements of the nuclear triad with the National Command Authority. Within several independent program justifications, improving cybersecurity is listed as a priority. In addition, in its FY 2018 Congressional Budget Justification, the National Nuclear Security Administration (NNSA) requested more than \$186 million from its weapons activities budget for enhancements to crosscutting NNSA information technology and cybersecurity efforts. Although this budget may cut across efforts to reduce cyber vulnerabilities on nuclear weapons systems, it cannot be specifically attributed to those efforts.

Other indications that improving cybersecurity of NC3 systems is becoming a priority can be found in the FY 2018 National Defense Authorization Act, which became law on December 12, 2017.

Section 1651 of that Act calls for the commander of the United States Strategic Command and the commander of the United States Cyber Command to conduct an annual joint assessment of the cyber resiliency of the nuclear command and control system. In addition, Section 1640 calls on the Secretary of Defense, in consultation with the director of the National Security Agency, to provide a plan to establish a Department of Defense (DoD) “Strategic Cybersecurity Program,” which will assist the department in improving the cybersecurity of systems, including (a) offensive cyber systems, (b) long-range strike systems, (c) nuclear deterrent systems, (d) national security systems, and (e) critical infrastructure of the DoD. This is consistent with the recommendations of the 2017 Defense Science Board report on cyber deterrence, which recommended the establishment of a “thin line” of cyber-resilient systems in nearly those same categories.

These and other efforts will be important to minimize the risk of cyberattacks on nuclear weapons systems. As highlighted in this report, however, although technical efforts are critical, no technological solution alone will be wholly effective; nuclear policy and posture changes must be implemented as well.

Recommendations

The recommendations in this section represent a high-level set of priorities for measures to mitigate the cyber threat to nuclear weapons systems. Some of these measures are already being implemented in some form and should continue to be prioritized. The following proposals can serve as a starting point for additional in-depth analysis.

Reducing the Risk of Launch as a Result of Miscalculation

New policies and postures are needed to decrease the risk of a nuclear launch as a result of miscalculation.

- **Develop options to increase decision time to account for cyber threats to early warning systems.** Cyber interference with nuclear weapons systems increases the potential for false warning of nuclear attack and a loss of confidence in the information available for national leaders to make a launch decision. No plausible improvements in the cybersecurity of these systems will allow leaders to ignore the possibility of the cyber threat. Increasing decision time (including potential changes in alert status) may be the only way to compensate for risks introduced by the cyber threat.

Today, U.S. and Russian ballistic missiles armed with nuclear warheads deployed on prompt-launch alert status can be fired and hit their targets within minutes. Once fired, a nuclear ballistic missile cannot be recalled before it reaches its target. Leaders may have only minutes between warning of an attack and nuclear detonations on their territory, which puts enormous pressure on leaders to maintain “launch on warning/launch under attack” options. In a crisis or at a time of heightened mutual tensions, this short interval increases the risk that a decision to use nuclear weapons will be made in haste after a false warning, and it multiplies the risk of use as a result of miscalculation—blundering into nuclear catastrophe.

The emergence of the cyber threat to nuclear weapons systems exacerbates that risk because of the increased potential for false warning and loss of confidence in information. The military should develop options for political leaders to increase decision time while retaining the ability to effectively respond to a nuclear attack if necessary. Those options should ensure that systems and processes are in place to verify or refute early warning data and other information necessary to determine an appropriate response. The United States should also work with other nations to develop understanding and mutual steps to increase decision time.

- **Establish norms to restrict cyber weapons use against nuclear weapons systems.** A cyber intrusion into another nation’s nuclear weapons system, even an unintentional intrusion, could prompt a crisis, potentially leading to nuclear use if another nation believed that the intrusion was a precursor to decapitating its nuclear deterrent. Given the stakes and risk of

miscalculation involved, civilian and military leaders, as well as lower-level officials, must be made aware of and act on the knowledge that cyberattacks on nuclear systems could have unintended and catastrophic consequences. The establishment of norms, although difficult to verify, to limit state cyber activity against nuclear weapons systems would reduce the potential for this type of crisis, particularly in periods of growing adversity. The establishment of such norms, however, is made considerably more difficult by the underlying dual-use nature of some nuclear weapons systems that may be vulnerable to the cyber threat and the integration and colocation of nuclear and conventional systems (see sidebar on p. 14). In addition, although norms are less likely to be effective in deterring or modifying the behavior of nonstate actors, the existence of norms could still be beneficial. With such norms in place, a cyberattack on nuclear systems—in violation of the norm—could more readily be assumed by states to be the work of a nonstate actor and could therefore help avoid potentially dangerous escalation.

- **Enhance survivability and resilience of nuclear systems and NC3 processes.** Nuclear deterrence requires a credible threat of retaliation, either through the ability to retaliate under attack or an ensured second-strike capability. The cyber threat, however, makes survivability—of nuclear weapons, delivery systems, and NC3 systems—even more challenging and

DECIDE UNDER ATTACK?

One option to reduce the pressure of decision time that was debated in the Study Group would be for the president to “decide under attack”—in other words, on being advised of an incoming nuclear attack, the president could order a nuclear response to be implemented after a specified period of time (e.g., 10 hours), perhaps in combination with another condition being met, such as confirmation and attribution of a nuclear attack. Proponents of this option argued that it would allow for the possibility of reversal if the incoming attack were determined to be a false warning, but it would ensure a nuclear response if it were not false and would therefore strengthen deterrence. Others voiced deep concerns that this option could lower the bar for a president to order

a nuclear attack, albeit a delayed one; that there could be technical and procedural challenges to successfully reversing a delayed launch order; and even that public leaks about the order could trigger a nuclear attack from another country. Moreover, some were generally uncomfortable with the idea of removing the human from the loop, arguing that if the order were carried out on this basis, it would preclude other options for response proportional to the actual scope of the attack and raise legal and chain-of-command issues, assuming the president who ordered the response was incapacitated before the order was executed. This option requires additional study and debate. Additional decision time options must also be developed.

“Nuclear command and control is the under-appreciated ‘fourth leg’ of the nuclear triad. Without highly reliable, high speed communications among the President, his advisors, and those who execute the nuclear deterrence mission, the other three legs are of no use. Thus, in a world of increasingly acute cyber threats, it is only fitting that due regard be given to the threat that cyberattacks could potentially pose to this vital fourth leg.”

—Adm. James A. Winnefeld, USN, Retired
STUDY GROUP MEMBER

important. NC3 systems must be resilient to the cyber threat to ensure that decision makers can communicate with the nuclear systems (both receiving and sending information), with each other to ensure the ability to consider appropriate responses, and with foreign counterparts (to de-escalate a crisis).

Reducing Cyber Risks to the Nuclear Deterrent

Many of the following measures to reduce risks to nuclear weapons systems already are being addressed in the United States (see sidebar on p. 22), and they should continue to be prioritized and advanced with adequate resources. This is crucial to sustaining confidence in the nuclear arsenal and maintaining strategic stability.

- **Secure and diversify critical systems.** The United States is investing significant resources in measures to defend against the cyber threat to its critical infrastructure, including nuclear weapons systems. Although there is no 100 percent effective technical solution for the cyber threat to nuclear weapons systems, every effort should be made to enhance the security and resiliency of those systems. It is important to take steps to increase the likelihood of prompt detection of a cyber breach and decrease the likelihood that an attack could disable a critical system. Priorities include avoiding the risk of failures that could compromise multiple systems or platforms.

The focus must therefore be on the diversity of systems and components (nuclear weapons, delivery systems, and communications systems) within and across systems and on examining how cyber threats could affect new, upgraded, networked, or automated systems as the nuclear force is modernized. Possible measures could include maintaining and enhancing reliance on nondigital systems, reducing complexity, hardening satellite and other communications systems, securing and diversifying the supply chain, and increasing diagnostic testing of components. Additional measures could include using dynamic solutions that increase resilience of critical communications systems.

“No complex systems are as consequential as nine nations’ systems of nuclear command and control. Leaders have an obligation to emphasize and illuminate the problems that result when the irresistible force of digitization meets the thought-to-be immovable objects of nuclear command and control.”

—Richard Danzig, former U.S. Secretary of the Navy
STUDY GROUP MEMBER

- **Prioritize addressing cyber risks in modernization plans.** The U.S. nuclear arsenal is in the initial stages of a decades-long modernization and recapitalization program to field new and updated delivery systems across all three legs of the nuclear triad of ground-based intercontinental ballistic missiles, sea-based ballistic missiles and their submarines, and strategic bombers. Additional plans include refurbishing U.S. nuclear warheads, recapitalizing aging nuclear infrastructure, upgrading U.S. NC3, and improving the management of the overall nuclear enterprise. As systems are increasingly networked and automated, cyber risks will be exacerbated. Therefore, the decision to automate and network key critical systems within the nuclear complex will require balancing the functionality benefits of modernization with the potential increase in cyber vulnerabilities. As the modernization and recapitalization process proceeds, it will be vital to examine in depth the effect of cyber threats on new and upgraded systems. That includes modernization of digital nuclear systems that are old by technological standards. As the systems are modernized, creative and rigorous measures should be employed to ensure the integrity of those systems and to identify threats to them. Such measures should include requiring new participants in the supply chain to ensure adequate security measures.
- **Maintain a cadre of experts.** Even with enhanced security measures, nuclear weapons systems could be compromised by cyber means. In the case of a cyber compromise of critical nuclear systems, resolving the issue and returning the systems to fully operational status will be the highest priority. The skills necessary to diagnose and respond to cyberattacks on nuclear weapons systems are unique, and doing so requires both a range of cyber skills and knowledge of nuclear weapons systems. The government should invest in and maintain trained and experienced experts, including a roster of rapid-recall personnel, to promptly detect and resolve cyberattacks on nuclear weapons systems. Establishing a pipeline of future experts can start with courses and training at the college level and could include workforce development. The government should ensure that resources are committed to train all operators in the broader nuclear weapons complex about the importance of cybersecurity. Humans will remain one of the major

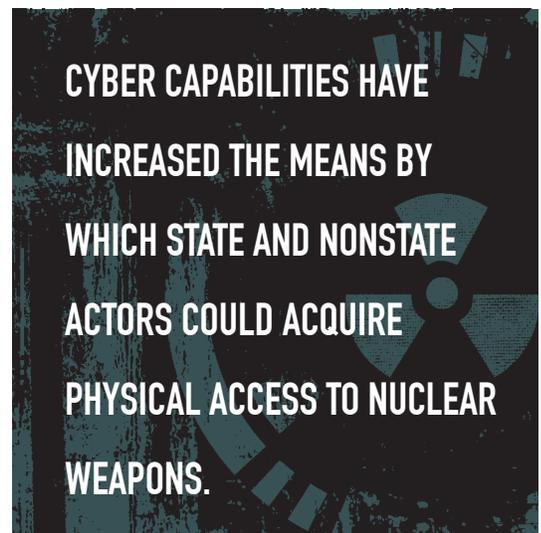
vulnerabilities for any would-be attacker. Therefore, in addition to ensuring a future pipeline of trained personnel, personnel vetting and other enhanced personnel security measures to address the insider threat will be key in mitigating cyber threats to nuclear weapons systems.

Reducing the Risk of Unauthorized Use

Cyber capabilities have increased the means by which state and nonstate actors could acquire physical access to nuclear weapons, leading to theft or unauthorized use of a nuclear weapon, with potentially catastrophic results.

- **Enhance security of nuclear weapons, and review the vulnerabilities of nuclear weapons to combined physical and cyber attacks.** The United States should continue to take steps to enhance the security, both physical and cyber, of nuclear weapons and delivery systems, including forward-based nuclear weapons in Europe. As long as such weapons remain in place, they will be uniquely vulnerable to theft through combined physical and cyber attacks.

As part of enhanced security, the United States should conduct comprehensive and regular reviews of how cyber threats could exacerbate existing physical threats to nuclear weapons. The reviews should determine the severity of the threat—both now and in the future, as potential adversaries' cyber capabilities evolve—and identify what additional security measures are needed to mitigate that threat. Other countries with nuclear weapons should do the same.



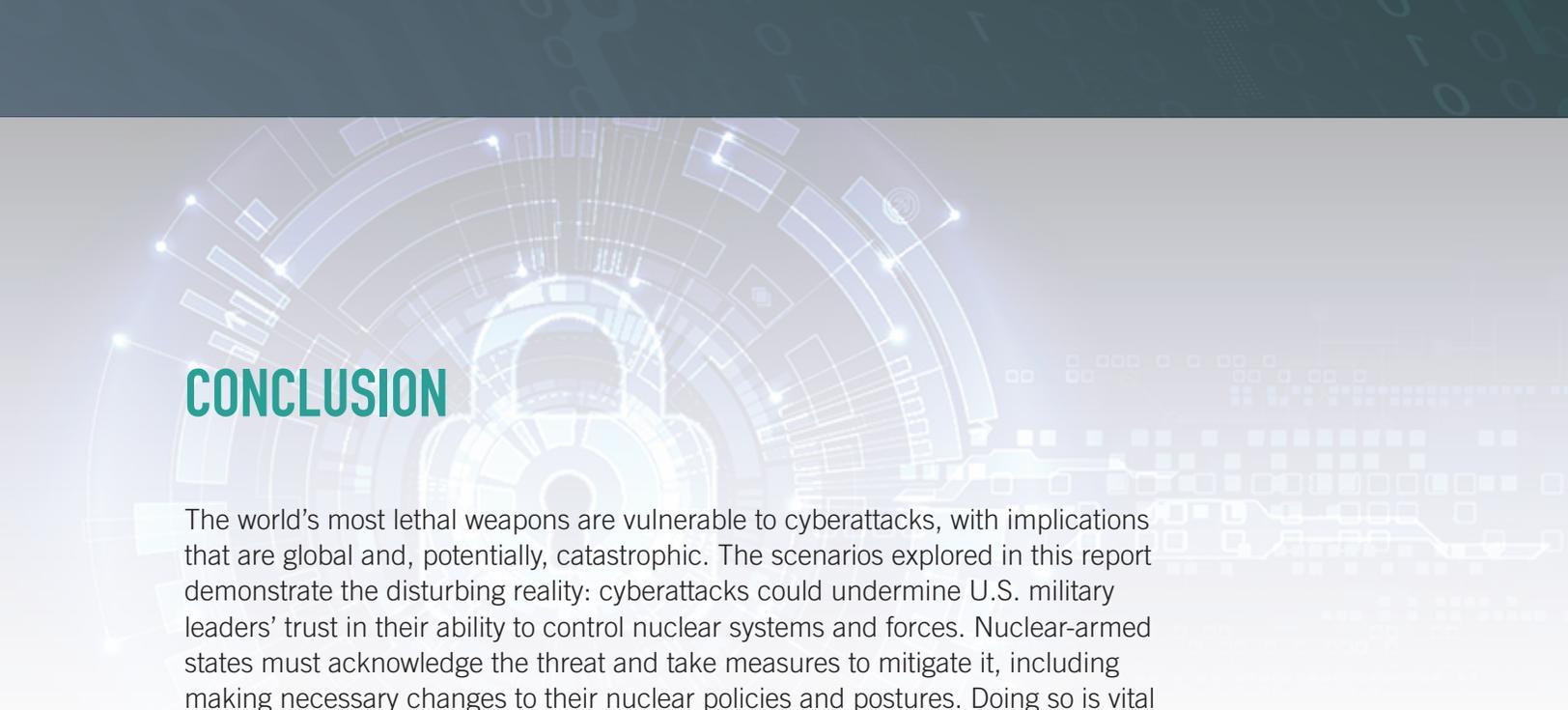
Taking a Global Approach to the Cyber Threat to Nuclear Weapons Systems

Cyber threats to nuclear weapons systems require a global response. All countries with nuclear weapons are vulnerable to cyberattacks, and the potential consequences of any nuclear launch due to miscalculation, unauthorized use, or a failure of nuclear deterrence would have global consequences. The following actions should be taken to build a better understanding of the global nature of the threat and to develop cooperative approaches to reducing the threat.

- **Initiate bilateral dialogue with Russia.** As a priority first step, the United States should seek to initiate a bilateral dialogue with Russia on cyber-nuclear threats (including the threat of third-party interference) to develop mutual understanding on how cyber threats can affect deterrence and strategic stability. Talks should be held with a view toward developing a shared understanding of our mutual interest in minimizing that risk and identifying practical ways to address it bilaterally and multilaterally. Such steps could include development of norms against cyberattacks on nuclear weapons systems and agreement on practical steps to enhance stability.

- **Increase international cooperation to reduce the cyber threat.** Without bilateral and multilateral engagement on the cyber threat, unilateral efforts to enhance the security of nuclear weapons systems might be considered destabilizing by other nations. Bilateral and multilateral dialogue with countries with and without nuclear weapons, with an initial priority on Russia and China, is crucial. To be sure, discussing these issues with countries from whom the cyber threat also emanates does present political and technical challenges, but the cyber threat is too great—and affects both the United States and its adversaries—to avoid dialogue about this existential common interest.

Bilateral and multilateral dialogues should consider norms and rules of the road—for example, agreement to refrain from using cyberattacks against nuclear weapons systems. Those dialogues also should consider unilateral or reciprocal actions to reduce the risk of nuclear weapons use that could result from cyberattacks. As an example, the United States should seek ways to cooperate internationally to improve early warning systems—including through military-to-military cooperation—to further reduce the possibility of a cyber-induced false warning. The United States also should work independently and with other states to explore and develop improved verification tools that could be used to enhance confidence in future cyber arms control or confidence-building agreements and measures.



CONCLUSION

The world's most lethal weapons are vulnerable to cyberattacks, with implications that are global and, potentially, catastrophic. The scenarios explored in this report demonstrate the disturbing reality: cyberattacks could undermine U.S. military leaders' trust in their ability to control nuclear systems and forces. Nuclear-armed states must acknowledge the threat and take measures to mitigate it, including making necessary changes to their nuclear policies and postures. Doing so is vital to ensure that states can have confidence in their ability to control their nuclear weapons and related systems.

Technical measures alone are insufficient to effectively reduce the threat. The cyber threat to nuclear systems also demands policy changes that reduce both the cyber-induced risk of use as a result of miscalculation and the risk of unauthorized use of a nuclear weapon, and the policy changes also must maintain confidence in nuclear deterrence. This report recommends a range of measures that represent high-level priorities to mitigate the cyber threat to nuclear weapons systems, and it can serve as the starting point for additional in-depth analysis. The recommendations include increasing decision time to account for cyber threats to early warning systems, developing norms against the use of cyber weapons, securing and diversifying critical systems, and exploring global cooperative approaches.

The cyber threat and the cyber capabilities of state and nonstate adversaries are constantly evolving, requiring a dynamic and evolving strategy in response. Governments must therefore closely and continuously review cyber threats to nuclear weapons systems, including analyzing the effect of modernization of nuclear systems. Perhaps more important, governments must be willing to question the continued viability of nuclear deterrence strategy, asking whether it is becoming obsolete—particularly if confidence levels in nuclear weapons systems can no longer be sustained. This report offers a starting point for how governments can grapple with these questions.

MEMBERS OF THE STUDY GROUP

Experts participating in the Study Group did not represent the views or interests of their countries or organizations. Instead, they played an advisory role in their personal capacities. Participation in the Study Group does not imply concurrence with every aspect of the report or its recommendations. The views expressed in this report do not reflect those of the institutions with which the members are associated; their affiliations are listed for the purpose of identification only.

Study Group Co-Chairs

Ernest J. Moniz, Co-Chair and Chief Executive Officer, NTI

Sam Nunn, Co-Chair, NTI

Des Browne, Lord Browne of Ladyton, Vice Chair, NTI

Study Group Members

James Acton, Jessica T. Mathews Chair and Co-Director, Nuclear Policy Program, Carnegie Endowment for International Peace

Brooke Anderson, Partner, The Hyalite Group

Steven Andreasen, National Security Consultant, NTI

General James Cartwright, United States Marine Corps (Retired), Harold Brown Chair in Defense Policy Studies, Center for Strategic & International Studies

Richard Clarke, Chairman and CEO, Good Harbor Security Risk Management

Charles B. Curtis, NTI President Emeritus and Emeritus NTI Board Member

Richard Danzig, Senior Advisor, Johns Hopkins Applied Physics Laboratory

Erin Dumbacher, Program Officer, Scientific and Technical Affairs, NTI

Chris Finan, CEO, Co-Founder, Director, Manifold Technology

Andrew Futter, Senior Lecturer in International Politics, University of Leicester

James Gosler, Senior Fellow, Johns Hopkins Applied Physics Laboratory; Member, Defense Science Board

General Eugene E. Habiger, United States Air Force (Retired), Former Commander in Chief, U.S. Strategic Command

Melissa Hathaway, President, Hathaway Global Strategies LLC; Senior Advisor, Cyber Security Project, Belfer Center for Science and International Affairs, Harvard University

Aaron Hughes, Senior Associate, Center for Strategic and International Studies; Former Deputy Assistant Secretary of Defense for Cyber Policy

Herb Lin, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University; Research Fellow, Hoover Institution

Joseph Nye, Harvard University Distinguished Service Professor, Emeritus, Harvard Kennedy School

Samantha Pitts-Kiefer, Senior Director, Global Nuclear Policy Program, NTI

Debora Plunkett, Principal, Plunkett Associates LLC

Joan Rohlfing, President and Chief Operating Officer, NTI

Brian Rose, Program Officer, Global Nuclear Policy Program, NTI

Deborah Rosenblum, Executive Vice President, NTI

Lynn Rusten, Senior Advisor, Global Nuclear Policy Program, NTI

Scott Sagan, Senior Fellow, Freeman Spogli Institute for International Studies, Stanford University; Senior Fellow, Center for International Security and Cooperation, Stanford University; Caroline S. G. Munro Professor of Political Science, Stanford University

Admiral James G. Stavridis, United States Navy (Retired); Dean, Fletcher School of Law and Diplomacy, Tufts University

Page O. Stoutland, PhD, Vice President, Scientific and Technical Affairs, NTI

Michael Sulmeyer, Director, Cyber Security Project, Belfer Center for Science and International Affairs, Harvard University

William Tobey, Senior Fellow, Belfer Center for Science and International Affairs, Harvard University

Sir Mark Welland, Professor of Nanotechnology, Nanoscience Centre, University of Cambridge

Isabelle Williams, Senior Advisor, Global Nuclear Policy Program, NTI

Admiral James A. "Sandy" Winnefeld, United States Navy (Retired); Distinguished Professor of International Affairs, Sam Nunn School of International Affairs, Georgia Institute of Technology; Senior Non-Resident Fellow, Belfer Center for Science and International Affairs, Harvard University

ABOUT THE AUTHORS

Page O. Stoutland, PhD, NTI's Vice President for Scientific and Technical Affairs is responsible for scientific and technically related projects designed to strengthen nuclear security around the world. Before joining NTI, he held senior positions at Lawrence Livermore National Laboratory. Previously, he held positions within the U.S. Department of Energy, where he served as the director of the Chemical and Biological National Security Program, and at Los Alamos National Laboratory. He holds a bachelor's degree from St. Olaf College in Northfield, Minnesota, and a doctorate in chemistry from the University of California, Berkeley.

Samantha Pitts-Kiefer is Senior Director of NTI's Global Nuclear Policy Program, where she is responsible for NTI's projects related to U.S.-Russia relations, U.S. nuclear policy, North Korea, and disarmament. In 2012, Pitts-Kiefer completed a master of public administration degree at the Harvard Kennedy School. She served as a research assistant for David Sanger on his book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Pitts-Kiefer practiced law at Simpson Thacher & Bartlett LLP and clerked for the Honorable Maryanne Trump Barry on the U.S. Court of Appeals for the Third Circuit. She holds a bachelor's degree from St. Olaf College and a juris doctor degree from Villanova University School of Law, where she was elected to the Order of the Coif.

From the Foreword by Ernest J. Moniz, Sam Nunn, and Des Browne

“This new report, *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group*, addresses cyber risks to nuclear weapons systems and offers recommendations developed by a group of high-level former and retired government officials, military leaders, and experts in nuclear systems, nuclear policy, and cyber threats.

As we work to improve technical security measures, all nuclear-armed states should be asking some bigger questions. If ultimately we cannot be confident that systems will work under attack from a sophisticated opponent, and if we cannot have full confidence in our ability to control nuclear weapons systems, what does this say about the continued viability of nuclear deterrence? In an age of cyberwarfare, has the nuclear deterrence strategy that helped guide the West and the Soviet Union through the Cold War become dangerously obsolete? Should our nuclear policies and force deployments be changed to mitigate the potential consequences of cyberattacks?

We believe the United States has an obligation to be a leader on addressing cyber threats to nuclear systems of all kinds, but especially to nuclear weapons systems. That is why this report is primarily U.S. focused. A subsequent effort will more directly address vulnerabilities in other countries because preventing nuclear use, whether by terrorists or by states, whether intentionally or by miscalculation, is a global issue. All countries with nuclear weapons and facilities must do more—much more—to protect their nuclear weapons and related systems. A weak link anywhere can result in catastrophe.”