

OUTPACING CYBER THREATS

PRIORITIES FOR CYBERSECURITY AT NUCLEAR FACILITIES



ABOUT THE AUTHORS

Alexandra Van Dine is a Program Associate with the Scientific and Technical Affairs program at the Nuclear Threat Initiative, where she works on projects related to the cybersecurity of nuclear facilities and nuclear weapons systems and the NTI Nuclear Security Index. She has presented research on cybersecurity at nuclear facilities at U.S. Strategic Command and Los Alamos National Laboratory. She graduated with honors from Georgetown University's Edmund A. Walsh School of Foreign Service, where she received the J. Raymond Trainor Award for outstanding academic achievement in International Politics.

Michael Assante is the Director of Industrial Control System (ICS) security at the SANS Institute and is a Senior Associate with the Center for Strategic and International Studies (CSIS) Strategic Technologies program. He held a number of high-level positions with the Idaho National Laboratory and served as Vice President and Chief Security Officer for American Electric Power. Throughout his career, he has developed and provided briefings on the latest technology and security threats to the National Security Advisor, Chairman of the Joint Chiefs of Staff, Director of the National Security Agency, various chief executive officers and their boards of directors, and other leading private sector and government officials.

Page Stoutland, Ph.D. is NTI's Vice President for Scientific and Technical Affairs, responsible for scientific and technically related projects designed to strengthen nuclear security around the world. His work includes developing the NTI Nuclear Security Index, strengthening technical cooperation with China, and promoting cybersecurity at nuclear facilities. Prior to joining NTI, he held senior positions at Lawrence Livermore National Laboratory (LLNL). 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, Minn., and a doctorate in chemistry from the University of California, Berkeley.

TABLE OF CONTENTS

ACKNOWLEDGMENTS.....	3
FOREWORD BY SAM NUNN	4
EXECUTIVE SUMMARY	5
THREAT AND LANDSCAPE	9
TODAY'S APPROACH.....	17
FOUR PRIORITIES TO DRIVE ACTION.....	19
TAKING ACTION.....	26
THE CYBER PRIORITIES PROCESS	29
APPENDIX: CYBER INCIDENTS AT NUCLEAR FACILITIES	31

© 2016 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 copyright holder. For permissions, send an e-mail request to contact@nti.org.

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

ACKNOWLEDGMENTS

We are grateful to NTI Co-Chairman and Chief Executive Officer Sam Nunn for his leadership on nuclear security and to NTI President Joan Rohlfing and Executive Vice President Deborah Rosenblum for their continued support as we seek to build a safer world.

We owe a special thank you to the group of experts who contributed their thoughts, suggestions, and trove of experiences to this project. NTI is fortunate to work with such outstanding people, and we have made every effort to ensure

that this report reflects their collective wisdom. We would especially like to thank Michael Assante, NTI's technical lead on this project, as well as Anna Ellis and Rob Hoffman. All three contributed papers in support of this report.

Finally, we are indebted to all of our colleagues at NTI who have contributed to this project in ways big and small. In particular, we are grateful to Carmen MacDougall, Mimi Hall, Carter Bates, and Catherine Crary. We also thank NTI's Elsie Bjarnason for her diligence and support.

- Page Stoutland, Ph.D.
Vice President, Scientific and Technical Affairs
Nuclear Threat Initiative
- Alexandra Van Dine
Program Associate, Scientific and Technical Affairs
Nuclear Threat Initiative

FOREWORD BY SAM NUNN

Banks and big-box stores, government agencies and airlines, social media and the news media—all have been victimized by cyberattacks; many have suffered serious breaches. None of those breaches has been catastrophic.

A cyberattack on a nuclear facility, however, could have catastrophic consequences. Terrorists and other hackers today may not have the cyber skills to facilitate the theft of nuclear bomb-making materials, but they will certainly make every effort. They could use stolen materials to detonate a bomb in any country in the world. They could sabotage systems to cause the release of dangerous levels of radiation that would extend beyond state borders. Or they could hold a facility hostage until their sinister demands were met. Beyond the unthinkable potential human toll, a serious cybersecurity breach would profoundly shake global confidence in civilian nuclear power generation.

Governments and industry simply must get ahead of this rapidly evolving global threat.

There's no doubt that nuclear facility operators and regulators are aware of the threat. Unfortunately, many of the traditional methods of cyber defense at nuclear facilities—including firewalls, antivirus technology, and air gaps—are no longer enough to match today's dynamic threats.

As the renowned cryptographer Bruce Schneier said, "Today's NSA secrets become tomorrow's Ph.D. theses and the next day's hacker tools." Increased digitalization at nuclear facilities creates critical efficiencies, including for some security practices. At the same time, digitalization creates new and ever-evolving cyber vulnerabilities that

Beyond the unthinkable potential human toll, a serious cybersecurity breach would profoundly shake global confidence in civilian nuclear power generation.

require a more effective and sustainable response to mitigate risks.

A tremendous amount of good work is being done in government and industry to evaluate and address new entry points for cyberattacks, but we also must take steps to outpace the threat. To help build on the progress being made, NTI convened a diverse international group of technical and operational experts to take a fresh look at cybersecurity at nuclear facilities and to develop a set of ambitious, forward-leaning priorities and recommendations.

Taken alone or in combination, the priorities identified by the group—institutionalizing cybersecurity, mounting active defenses, reducing complexity, and pursuing transformation—would dramatically reduce the risk of damaging cyberattacks on nuclear facilities.

This report is our first contribution to ensuring that no one with malicious intent is able to engage in nuclear sabotage or to gain access to some of the world's most powerful—and most dangerous—materials.

— Sam Nunn, NTI Co-Chairman



EXECUTIVE SUMMARY

The past decade has seen unprecedented progress in the security of nuclear materials and facilities. As key improvements to physical security have been implemented, however, a threat that is potentially even more challenging is endangering these gains: the cyber threat.

Cyberspace provides a new opportunity for determined adversaries to wreak havoc at nuclear facilities—possibly without ever setting foot on-site. Cyberattacks could be used to facilitate the theft of nuclear materials or an act of sabotage that results in radiological release. A successful attack could have consequences that reverberate around the world and undermine global confidence in civilian nuclear power as a safe and reliable energy source.

Given the risk and the stakes, governments and industry must increase their focus on the cyber threat.

Nuclear operators and a range of national and international organizations have recognized the challenge and have begun to accelerate their efforts to strengthen cybersecurity at nuclear facilities. However, the rapidly evolving cyber threat, combined with the proliferation of digital systems, makes it difficult to get ahead of the threat. Case after case—from the Stuxnet attacks on the Natanz uranium enrichment facility in Iran, to the hack of Korea Hydro and Nuclear Power in South Korea, to disturbing revelations of malware found on systems at a German nuclear power plant—demonstrates that the current

approach to cybersecurity at nuclear facilities is not equal to the challenge. Crafting a strategy that protects facilities from dynamic, evolving cyber threats requires a fresh, unconstrained examination of the overarching framework that guides cybersecurity.

To try to get ahead of the threat, the Nuclear Threat Initiative (NTI) assembled an international group of technical and operational experts with backgrounds in computer security, nuclear safety systems, nuclear engineering, industrial control systems, and nuclear facility operations. This group was tasked with identifying the core elements of a new strategy, then with focusing on those elements that would have the greatest possible effect.

Over 12 months, the group identified four overarching priorities, as well as specific actions, that if implemented would dramatically reduce the risk of damaging cyberattacks on nuclear facilities. Similar concepts are being put to use elsewhere, and NTI believes that, either alone or in combination, they would provide considerable leverage on the threat posed to nuclear facilities.

1. Institutionalize cybersecurity. Implementation of robust processes and practices is essential for the effective management of complex systems and is at the heart of long-standing quality management programs used across industry. Given the rapidly evolving cyber threat, however, such practices are generally not yet in place for cybersecurity in nuclear facilities. Nuclear facilities should

learn from and actively integrate the practices employed by safety and physical security programs to strengthen and sustain their cybersecurity programs. Specifically,

- Governments and regulators should work to develop and implement regulatory frameworks, perhaps drawing on lessons learned from progress made in nuclear safety and physical security, that promote the institutionalization and ongoing improvement of cybersecurity at nuclear facilities. Accordingly, efforts should be made to draw talented people into the cyber-nuclear field by investing in education and training programs and providing incentives to take jobs in this critical security sphere.
- Nuclear industry should apply lessons learned from industry experiences with safety and physical security and recruit the expertise necessary to achieve a more secure future.
- International organizations should support, through international dialogue and definition of relevant best practices, international cooperation and an expanded focus on cybersecurity at nuclear facilities.

2. Mount an active defense.¹ The static cybersecurity architectures at today's nuclear facilities are not effective enough on their own to prevent a breach by a determined adversary, nor are they effective enough to respond once a compromise has occurred. Nuclear facilities need to update their prevention and response plans—steps that are essential but that are challenged by the global shortage of technical experts. Specifically,

- Governments and regulators should enhance cyber expertise within governmental and regulatory bodies, share relevant

threat information with industry, consider how to develop and exercise cyber incident response capabilities, and provide additional resources for defense against threats beyond those that facilities could reasonably be expected to handle.

- Nuclear industry should initiate the development of active defense capabilities at the facility level, including providing training opportunities and assistance to boost human capacity, especially in countries with new or expanding civilian nuclear energy programs. This could include developing mutual-aid agreements or other cross-industry resources to allow facilities to access needed skills.
- International organizations should facilitate the sharing of threat information where possible and appropriate.

3. Reduce complexity. Complexity is the enemy of security. Today's nuclear facilities consist of thousands of digital systems. The security effects of these systems, their functionalities, and how they interact are not always fully understood. Although networks may be initially characterized, this information is not always kept up to date. When it comes to the most critical systems, the most advantageous option may be to eliminate digital complexity entirely by transitioning to non-digital systems. Specifically,

- Governments and regulators should support—with financial, personnel, and research resources—facility efforts to characterize networks, understand functionalities and interactions, and ultimately minimize complexity in critical systems.
- Nuclear industry and facilities should characterize systems, identify excess

¹ In other industries, the term *active defense* can sometimes imply that defenders should “hack back” against adversaries. The term is used here merely to indicate a dynamic defense, distinct from “hacking back.”

functionalities and remove them where possible, and work with vendors to develop non-digital systems and secure-by-design products where possible and appropriate.

- International organizations should provide platforms for discussing and developing solutions for reducing complexity.

4. Pursue transformation. The global community is in the early stages of understanding the magnitude of the cyber threat. In many ways, humans have created systems that are too complex to manage; in most cases, risks cannot even be quantified. As a result, there is a fundamental need for transformative research to develop hard-to-hack systems for critical applications. Specifically,

- Governments and regulators should undertake or fund transformative research into the technologies, methods, and approaches that will be necessary to get ahead of the threat.
- Nuclear industry should support the cybersecurity efforts of relevant organizations, including the International Atomic Energy Agency (IAEA), the World Nuclear Association (WNA), the World Association of Nuclear Operators (WANO), and the Institute of Nuclear Power Operations (INPO), in an effort to continue internation-

**Given the risk and the stakes,
governments and industry must
increase their focus on the
cyber threat.**

al dialogue and contribute to key research and development necessary to improving cybersecurity.

- International organizations should foster innovation and continue to think creatively about how to mitigate this threat and should recruit a variety of voices and perspectives to join the conversation.
- Governments, industry, and international organizations alike should strive to boost human capacity across the cyber-nuclear field, especially in countries with new or expanding civilian nuclear energy programs.

Taken together, the priorities listed represent a new approach to getting ahead of the urgent and evolving cyber threat. Implementing them will be a multiyear effort and will not be easy, but the risk is far too great to accept the status quo.

CYBER PRIORITIES, STAKEHOLDERS, AND ACTIONS

STAKEHOLDERS



**Governments
and Regulators**



**Nuclear
Industry**



**International
Organizations**

PRIORITIES

Institutionalize Cybersecurity

- Prioritize development and implementation of regulatory frameworks
- Draw talented people into the cyber-nuclear field
- Apply lessons learned from institutionalizing safety and physical security to cybersecurity
- Recruit the expertise necessary to achieve a more secure future
- Support, through international dialogue and definition of relevant best practices, international cooperation and an expanded focus on cybersecurity at nuclear facilities
- Develop and provide guidance and training to governments and facilities, as requested

Mount an Active Defense

- Enhance cyber expertise within governmental and regulatory bodies
- Consider how to develop and exercise cyber incident response capabilities
- Support efforts to re-tool defense strategies and promote information sharing between governments and industry
- Initiate the development of active defense capabilities at the facility level
- Develop cross-industry defense resources
- Provide training opportunities and assistance to boost human capacity
- Facilitate sharing of threat information, where possible and as appropriate

Reduce Complexity

- Provide financial, personnel, and research support to efforts to minimize complexity in critical facility systems
- Characterize facility systems and networks and understand device functionalities
- Demand more secure, less complex products from vendors
- Provide platforms for discussing and developing solutions for reducing complexity

Pursue Transformation

- Invest in augmenting human capacity, research, and development in the cyber-nuclear space
- Support the cybersecurity efforts of relevant organizations in an effort to continue international dialogue and contribute to key research and development
- Foster innovation and continue to think creatively about how to mitigate this threat
- Enlist a variety of voices and perspectives to join the conversation



THREAT AND LANDSCAPE

The cyber threat has become more urgent in recent years, as illustrated by a series of damaging, high-profile attacks that have made headlines around the world. Case after case has demonstrated that critical infrastructure is not immune. That includes nuclear facilities, where a cyberattack could have consequences on par with a serious safety incident or physical security breach and could even facilitate an act of sabotage or the theft of nuclear materials. Cyberattacks are a powerful tool for those who are determined to terrorize the public, undermine confidence in civilian nuclear power, or both.

Today, both safety and physical protection systems rely on digital components that could be compromised by a determined adversary. For example, researchers have shown that a cyber-attack could be used to disable physical protection measures, such as closed-circuit television cameras, to allow an intruder unfettered access to sensitive areas of a facility.² Additionally, an attacker could manipulate nuclear reactor control systems—which could potentially lead to a radiological release—thereby directly undermining years of important progress in strengthening safety systems and safety culture at nuclear facilities. Finally, the threat is not only from outsiders, for damaging actions could be taken with the assistance of an insider, either consciously or not.³

Cyberattacks are a powerful tool for those who are determined to terrorize the public, undermine confidence in civilian nuclear power, or both.

Recent history is filled with examples demonstrating that critical infrastructure and even nuclear facilities are vulnerable—both to untargeted malware and to targeted cyberattacks. As is now well known, the Natanz uranium enrichment facility in Iran was attacked with the Stuxnet virus between 2009 and 2010; the virus led to damaged centrifuges and also delayed enrichment activities.⁴ This case is particularly notable because the facility was well defended and isolated from the Internet.

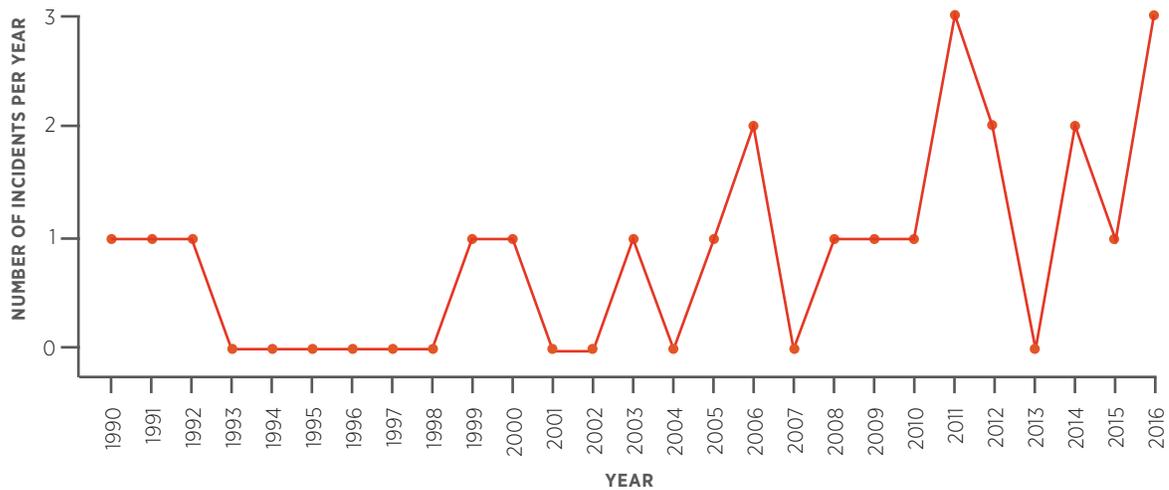
Since news of Stuxnet broke in 2010, revelations of malware found in nuclear facilities and critical infrastructure have only increased in frequency. In 2014 alone, a cyberattack against a German steel mill caused massive physical damage, malware

2 Rodolfo Quevenco, “Secure Computer Systems Essential to Nuclear Security, Conference Finds,” International Atomic Energy Agency website, June 8, 2015, available at www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds.

3 Raj Samani and Charles McFarland, “Hacking the Human Operating System: The Role of Social Engineering within Cybersecurity,” McAfee Labs, 2015, available at www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf.

4 Joby Warrick, “Iran’s Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack,” *Washington Post*, February 16, 2011, available at www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html.

Frequency of Cyber Incidents at Nuclear Facilities Increasing



The incidents pictured above represent publicly disclosed cyber incidents at nuclear facilities since 1990. It is possible that more incidents have occurred that have not been publicly disclosed or for which the details are classified or otherwise unavailable.

was introduced into the control room at Japan's Monju nuclear power plant, and the Korea Hydro and Nuclear Power in South Korea was hacked. The Japanese and South Korean cases resulted in the release of technical data online.⁵ The year 2015 saw a sophisticated, troubling cyberattack—one that is not hard to imagine being used against a nuclear facility—against the Ukrainian power grid that turned out the lights in parts of that country for three to six hours. Also in that year, a Japanese facility that handles plutonium and other nuclear materials revealed that it had discovered malware in its systems.⁶ In 2016, a German nuclear power plant was found to be infected with malware, and

officials discovered a spear-phishing campaign that had been exfiltrating data from a Japanese research center for months.⁷

Nuclear facilities are vulnerable to a variety of cyberattacks by a variety of malevolent actors. Among them are the following:

- **Terrorist groups** have stated their desire to build and use weapons of mass destruction. These groups have, in the past, sought to acquire nuclear materials and even actively surveilled a senior nuclear scientist who had access to sensitive areas of a Belgian nuclear

5 For more information on the German steel mill hack, see Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, January 8, 2015, available at www.wired.com/2015/01/german-steel-mill-hack-destruction/. For more information on the Monju nuclear power plant, see Pierluigi Paganini, "IT Administrator at Monju Nuclear Power Plant Discovered That a Malware-Based Attack Infected a System in the Reactor Control Room," *Security Affairs*, January 10, 2014, available at www.securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html. For more information on the Korea Hydro and Nuclear Power hack, see Meeyoung Cho and Jack Kim, "South Korea Nuclear Plant Operator Says Hacked, Raising Alarm," *Reuters*, December 22, 2014, available at www.reuters.com/article/us-southkorea-nuclear-idUSKBN0K008E20141222.

6 For more information on the attack in Ukraine, see Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, available at www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; see also Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," Electricity Information Sharing and Analysis Center, March 18, 2016, available at www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf. For more information on the Japanese infection, please see "Nuclear Center Waits over a Year to Report Cyber-Attack," *The Asahi Shimbun*, May 19, 2016, available at www.asahi.com/ajw/articles/AJ201605190028.html.

7 For more on the German case, see "German Nuclear Plant Infected with Computer Viruses, Operator Says," *Reuters*, April 27, 2016, available at <http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN20S>. For more on the Japanese case, see "Cyber-Attacks 'Targeted Nuclear Lab,'" *Chicago Tribune*, October 11, 2016, available at <http://www.chicagotribune.com/sns-wp-japan-cyberattack-49bfc78-8fce-11e6-a6a3-d50061aa9fae-20161011-story.html>; see also Catalin Cimpanu, "Hackers Steal Research and User Data from Japanese Nuclear Research Lab," *Softpedia*, October 17, 2016, available at <http://news.softpedia.com/news/hackers-steal-research-and-user-data-from-japanese-nuclear-research-lab-509380.shtml#ixzz4NYnWS8hw>.

8 Samuel Osborne, "ISIS Suspects Secretly Monitored Belgian Nuclear Scientist, Raising Dirty Bomb Fears," *Independent*, February 19, 2016, available at www.independent.co.uk/news/world/europe/isis-dirty-bomb-nuclear-scientists-paris-attacks-a6884146.html.

research facility.⁸ Although such groups are not currently believed to possess a sophisticated cyber capability, their desire to obtain nuclear materials could lead them to develop or hire the skills necessary to do so. This makes the need to improve cybersecurity at nuclear facilities all the more urgent.

- ▶ **Nation-states** are developing unprecedented offensive cyber capabilities. And despite an emerging norm that states should not attack civilian infrastructure,⁹ including nuclear facilities, it could happen. Recent events in Ukraine have highlighted the risks posed to the electric grid—it's not inconceivable that a nuclear power plant could be attacked for similar reasons.
- ▶ **Ransomware hackers** could infect a facility network and hold it hostage until a ransom is paid. Such hackers could infiltrate systems and position themselves to cause significant problems ranging from leaking sensitive data, to shutting down critical systems, to causing a radiological release. Although such an attack has not yet happened in the nuclear sector, it is far from impossible; similar attacks have been perpetrated against Israel's Electric Authority and a series of California hospitals in the United States.¹⁰
- ▶ **"Hacktivists,"** or hackers motivated by a particular social or political cause, also could victimize a nuclear facility. For example, an anti-nuclear activist group might choose to launch cyberattacks against a nuclear facility

9 See, for example, Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations, 2015.

10 For more on the attack against the Israel Electric Authority, see Darlene Storm, "No, Israel's Power Grid Wasn't Hacked, but Ransomware Hit Israel's Electric Authority," *Computerworld*, January 27, 2016, available at www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html. For more on the attack against California hospitals, see Jazmine Ulloa, "Why Lawmakers Are Trying to Make Ransomware a Crime in California," *Los Angeles Times*, July 12, 2016, available at www.latimes.com/politics/la-pol-sac-crime-ransomware-bill-20160712-snap-story.html.

In the past 30 years, an increasing number of publicly disclosed cyber incidents have occurred at nuclear facilities. The number of unreported or undiscovered incidents may well be much higher. These examples, gathered from news and other reports, illustrate the cyber threat to nuclear security and teach important lessons.

2003 CYBER INCIDENT

UNITED STATES Davis-Besse Nuclear Power Station



The Davis-Besse nuclear power plant in Ohio was infected with the Slammer worm—along with 75,000 servers worldwide within 10 minutes of its release in 2003—after a consultant connected to the plant's corporate network. The worm did not carry a malicious payload; rather, it overwhelmed the server by scanning random IP addresses in search of new hosts in which to propagate.

Because the corporate network was connected to the plant process control system without any type of firewall, the worm was able to jump onto plant systems and take up huge amounts of bandwidth. This shut down the safety parameter display system (SPDS) for nearly five hours, and prevented operators from seeing sensitive information about the reactor core. Fortunately, the plant was not running—however, had it been operating, this malfunction could have caused a serious problem.

A patch for the Microsoft SQL 2000 database server software vulnerability that the Slammer worm exploited had been released six months earlier, but neither the corporate network nor the control system had been patched. After the event, the plant installed a firewall between the plant process control system and the corporate network.

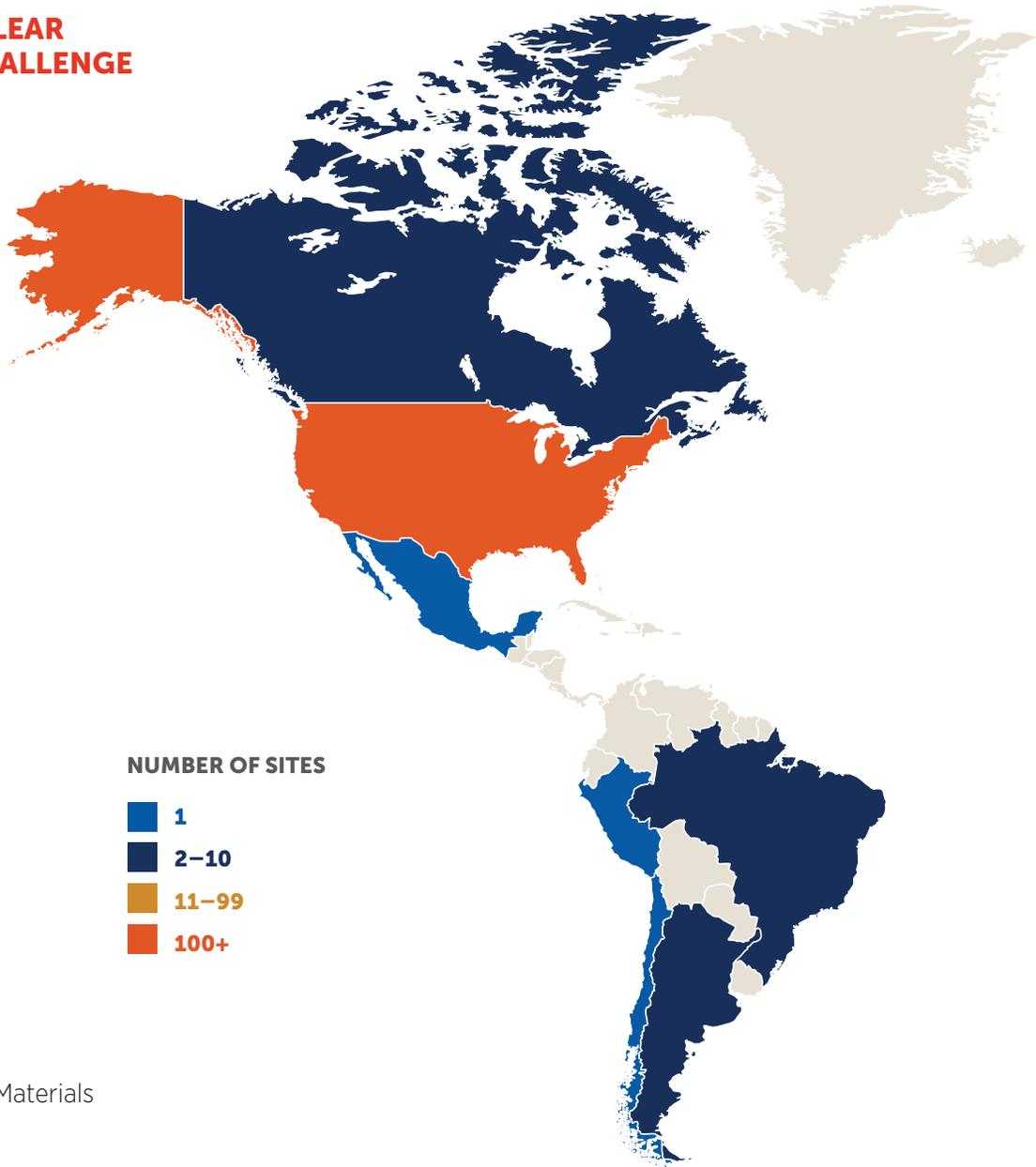
This incident highlights the dangers of linking plant monitoring and operating systems with corporate networks, as well as connecting computers from outside the plant to systems inside.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

CYBERSECURITY AT NUCLEAR FACILITIES: A GLOBAL CHALLENGE

There are hundreds of nuclear facilities around the world. Each type of facility is potentially vulnerable to a cyberattack that may result in theft or sabotage. The map below shows the range and quantity of different types of nuclear facilities in each country.

These data come from the 2016 edition of the NTI Nuclear Security Index.



KEY

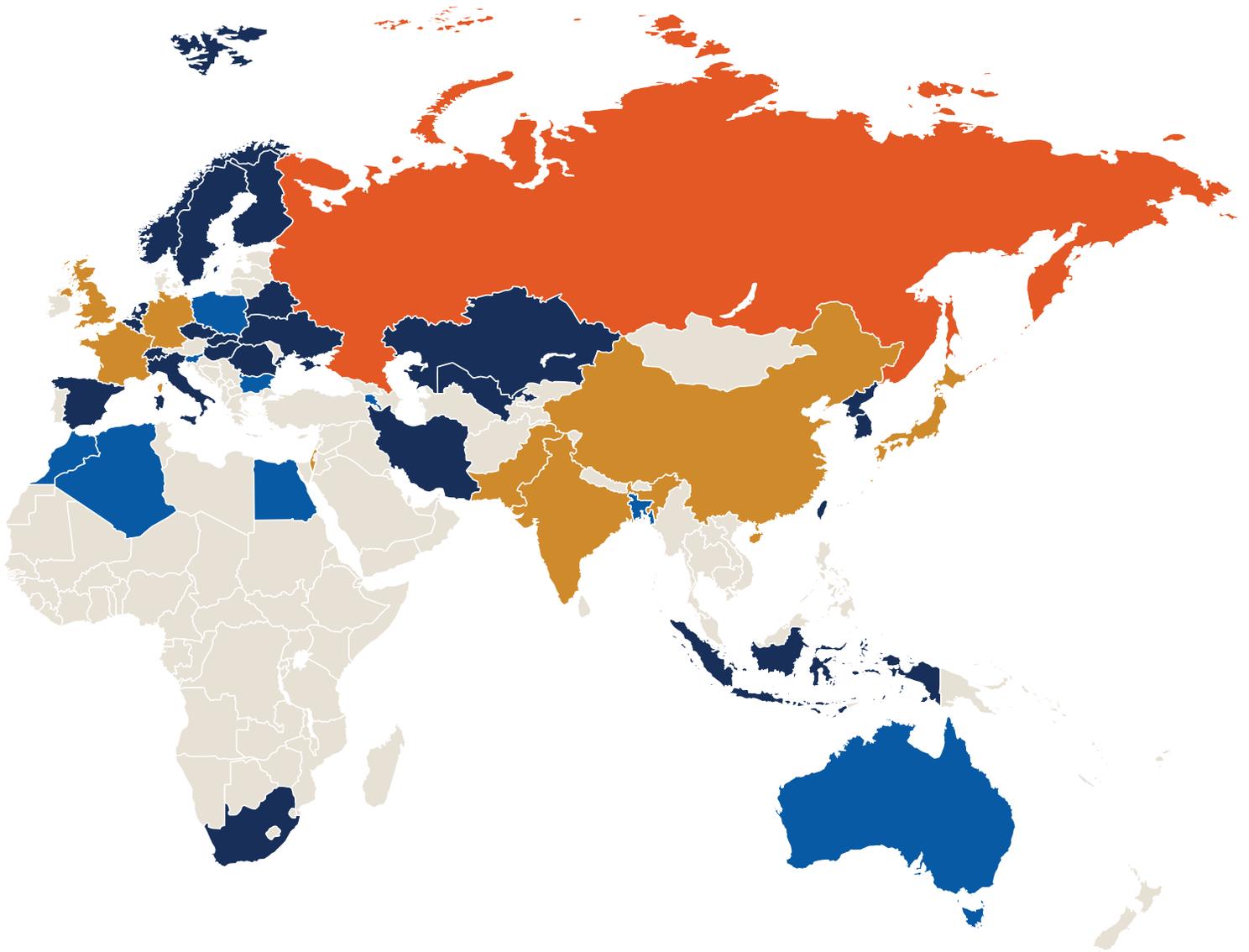
-  Power Reactor
-  Research Reactor
-  Reprocessing
-  Wet Spent Fuel Storage
-  Weapons-Usable Nuclear Materials

NUMBER OF SITES

-  1
-  2-10
-  11-99
-  100+

					
Algeria		●			
Argentina	●	●		●	
Armenia	●				
Australia		●			●
Bangladesh		●			
Belarus					●
Belgium	●	●		●	●
Brazil	●	●			
Bulgaria	●			●	
Canada	●	●			●
Chile		●			
China	●	●	●	●	●

					
Czech Republic	●	●			
Egypt		●			
Finland		●		●	
France	●	●	●	●	●
Germany	●	●		●	●
Hungary	●	●		●	
India	●	●	●	●	●
Indonesia		●			
Iran	●	●			●
Israel		●			●
Italy					●
Japan	●	●	●	●	●



Kazakhstan		●			●
Mexico	●				
Morocco		●			
Netherlands	●	●			●
North Korea		●	●		●
Norway		●			●
Pakistan	●	●	●	●	●
Peru		●			
Poland		●			
Romania	●	●			
Russia	●	●	●	●	●
Slovakia	●			●	



Slovenia	●				
South Africa	●	●			●
South Korea	●	●			
Spain	●				
Sweden	●			●	
Switzerland	●				●
Taiwan	●	●			
Ukraine	●	●			
United Kingdom	●		●	●	●
United States	●	●	●	●	●
Uzbekistan		●			

NTI NUCLEAR SECURITY INDEX HIGHLIGHTS CYBER GAPS

The NTI Nuclear Security Index highlights the important gap in cybersecurity at nuclear facilities. For the first time in 2016, the Index assessed how countries are protecting their nuclear facilities against cyber threats, and the results were troubling.

The Index posed four questions about cybersecurity at nuclear facilities in 47 countries with 1 kilogram or more of weapons-usable nuclear materials or facilities that, if sabotaged, could result in radiological release. These were

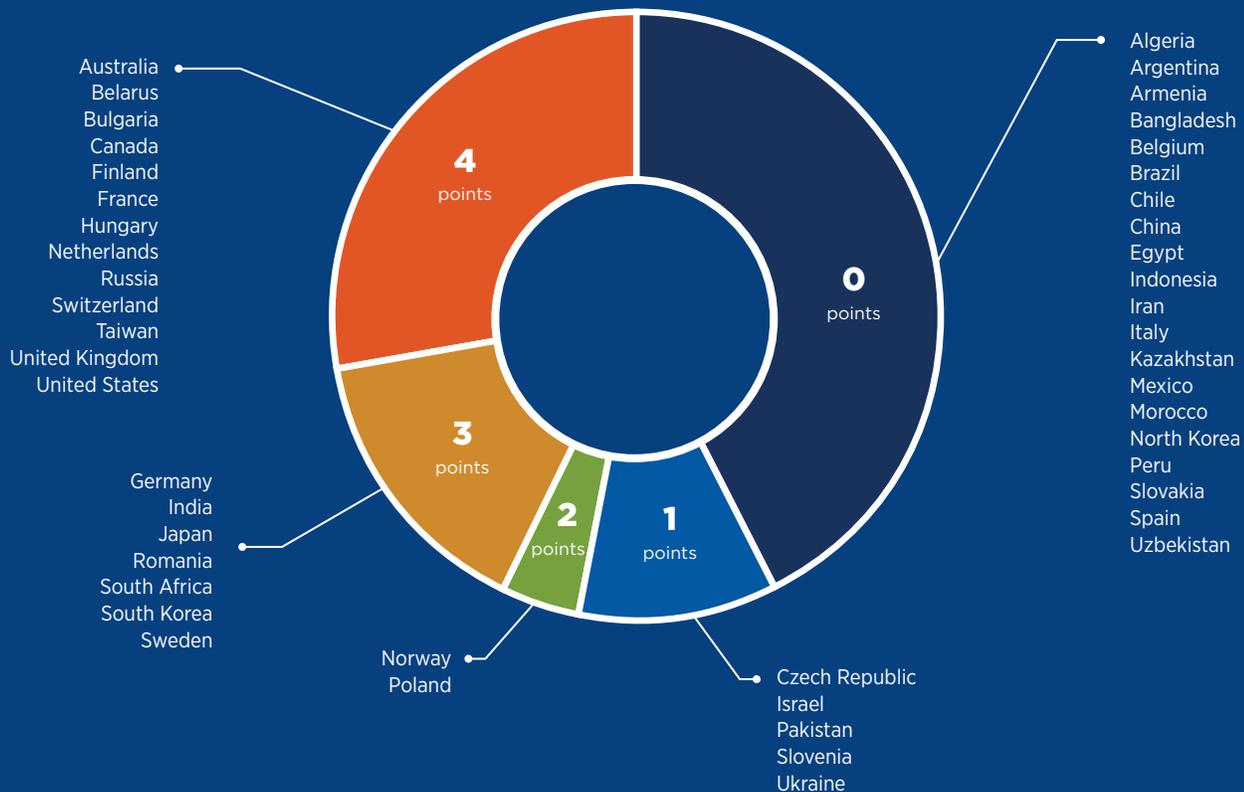
- Does the country require nuclear facilities to be protected from cyberattack?

- Does the country require nuclear facilities to identify critical digital assets?
- Does the country incorporate cyber threats into its design basis threat or other threat assessment?
- Does the country require performance-based testing of its cybersecurity measures?

Scoring was based on publicly available laws and regulations, and did not measure implementation. Therefore, a high score does not necessarily translate to ideal security—although it certainly suggests how seriously a given country takes the cyber threat.

Overall, the results show that too many countries require virtually no security measures at nuclear facilities to address the threat posed by cyber criminals or malicious actors. Although some countries have been taking steps to strengthen cybersecurity requirements at nuclear facilities, such as passing new laws and regulations or updating existing ones, many countries lack these crucial frameworks. Ultimately, the lack of a framework leaves facilities unprepared for the growing cyber threat. For more information on the NTI Index, a first-of-its-kind ranking measuring global nuclear security conditions, go to www.ntiindex.org.

NTI Nuclear Security Index Cyber Scores



to achieve political goals. When Korea Hydro and Nuclear Power (KHNP), South Korea's nuclear operator, was hacked in December 2014, it initially appeared as though hacktivism was the primary motivation. In an online message claiming credit for the attack, the hacker claimed to be the head of an anti-nuclear group and promised that leaks would continue until all 23 of South Korea's nuclear reactors were shut down.¹¹ Although South Korean authorities ultimately attributed the attack to North Korea, it was initially investigated as an act of hacktivism.

It may be only a matter of time before the world experiences a catastrophic event—whether a theft of nuclear material, or the sabotage of a nuclear facility—facilitated by a cyberattack deployed by a determined, well-resourced adversary. Those responsible for security, from policymakers to regulators to industry leaders to facility operators, face the significant challenge of getting ahead of the fast-moving threat.

CYBER-NUCLEAR LANDSCAPE

Digital systems are integral to nuclear facilities—from enrichment facilities and reprocessing plants to spent fuel storage and nuclear power plants—throughout the fuel cycle. They perform a range of functions, including access control, materials control and accounting, and the safe and secure operation of the facility. A sophisticated, targeted cyberattack against a nuclear facility would have the potential to knock out digital systems vital to ensuring safety and security and could result in significant physical consequences.

To date, the approach for managing cyber risks has focused on preventing access to critical systems by using tools such as firewalls, anti-virus programs, air gaps, and unidirectional gateways.¹² This approach has generally proved

AIR GAP MYTH

An air gap is the concept of physically isolating critical computers or networks from unsecure networks (such as the public Internet). In theory, devices on either side of this gap are unable to communicate, making an air gap an attractive option for securing the most important networks—including the industrial control systems present in many nuclear facilities.

Air gaps were used as one of the first means of preventing attacks on critical computer systems from the untargeted cyber threats that plagued computer users more than a decade ago. However, even against these older threats, the air gap was no panacea. Security inspections often found unintended network connections to systems that were meant to be isolated. Additionally, evidence of malware infections on air-gapped computer systems was often discovered years after the initial infection.

Although air gaps provide some level of protection, in practice they create a sense of complacency and are insufficient to meet the threat currently faced by the nuclear industry: that of a targeted attack perpetrated by a determined, well-resourced adversary. Such attacks are constructed on the basis of extensive research of targeted systems and go beyond network connections—generally by leveraging witting or unwitting humans, or a long and difficult-to-defend supply chain, to deliver the attack. The most commonly described compromises of air-gapped systems are through the use of removable media (e.g., USB drives). This has been demonstrated in high-profile cases, most notably in the Stuxnet malware that destroyed centrifuges inside an air-gapped uranium enrichment facility in Iran.

effective against untargeted cyberattacks—the cyber threat that has plagued computer users for the last decade—but it is not sufficient to protect against newer, target-focused attacks and

¹¹ Cho and Kim, "South Korea Nuclear Plant."

¹² Unidirectional security gateways are replacing the overly restrictive air gap in the form of data diode technologies.

2009 CYBER INCIDENT

UNITED STATES Energy Future Holdings



After an employee of the Dallas-based power company that operates the Comanche Peak Nuclear Power Plant was terminated for poor performance in March 2009, the employee, Dong Chul Shin, logged onto the company's corporate network, modified and deleted files, and e-mailed sensitive information to himself. He also e-mailed the operators of the Comanche Peak nuclear reactor with unsettling questions about the safety of the reactor, such as what would happen if the load were "increased to 99.7 percent of capacity."

The only damages that resulted from this incident were economic, estimated at \$26,000. However, this incident highlighted the dangers posed by the insider threat in the cyber-nuclear space.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

threats. Targeted attacks tend to rely on more enduring vulnerabilities, such as human behaviors and practices, and may require the creation of new cyber weapons.¹³

In contrast to unsophisticated attackers, determined adversaries are known to use targeted, adaptive strategies and customized cyber tools and may even consider compromising the supply chain—meaning equipment could be infected before it is even installed at a nuclear facility. In

practice, targeted attacks have proved effective in compromising conventional cybersecurity defenses, and it is evident that well-resourced, persistent adversaries can defeat even technologically advanced security solutions.¹⁴

In the context of nuclear facilities, it is also important to recognize not just the potential consequences of what digital systems are designed to do but also what they are *capable* of doing. System engineers often think in terms of what the system is *designed* to do, but adversaries tend to think in terms of what the system can be *made* to do. Because this difference is only beginning to be realized, many of the potential outcomes of a cyberattack on a nuclear facility have yet to be analyzed.

Protecting nuclear facilities from damaging cyberattacks is made more difficult by their complexity. A typical facility might include more than a thousand digital components, including legacy systems with no built-in security. Moreover, older facilities are transitioning to digital systems that often bring greater reliability and safety, but also increase vulnerability to cyberattacks. In addition to making defense more difficult, complexity increases attack pathways, including the creation of unanalyzed failure modes that would never occur naturally.

Finally, challenges to addressing the cyber threat are exacerbated by a shortage of technical expertise in the cyber-nuclear space. Finding experts with specific knowledge of digital control systems in a nuclear environment is no easy feat. What expertise does exist tends to be overwhelmingly concentrated in North America, Europe, and Russia—leaving many countries with new or expanding nuclear energy programs grasping for solutions.

¹³ The ability to exploit weaknesses in the complex system-of-systems that comprise modern organizations has invented underground markets, empowered activists, and transformed intelligence gathering and war fighting. Many enterprises have mastered the art and science of maneuvering through the expected noise and less structured threats that come with global public networks. The adversarial "cyber" threat actors that engage in targeted attacks continue to expand at an alarming rate, defeating security prevention and detection technology and controls, challenging conventional analysis, and invalidating existing reliability and safety design methods. Examples include campaigns and malware such as Snake, Ice Fog, Black Energy, Duqu, MiniDuke, Stuxnet, Regin, Night Dragon, etc.

¹⁴ Rob O'Regan, "3 of the Biggest Concerns about External Cyber Threats," *Art of the Hack*, July 6, 2016, available at www.theartofthehack.com/3-of-the-biggest-concerns-about-external-cyber-threats/; Steve Ragan, "Researcher Discloses Zero-Day Vulnerability in FireEye," *CSO Online*, September 6, 2015, available at www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html.



TODAY'S APPROACH

Nuclear operators and a range of national and international organizations have recognized the challenge and begun to accelerate their efforts to strengthen cybersecurity at nuclear facilities. For example, in the United States, the Nuclear Regulatory Commission (NRC) and the Department of Homeland Security (DHS) have clearly defined roles in protecting nuclear facilities from cyberattacks. At the international level, important efforts have been undertaken by the International Atomic Energy Agency (IAEA) and the World Institute for Nuclear Security (WINS). The IAEA, for instance, provides hands-on training in cybersecurity at nuclear facilities to member states. Moreover, it has worked to develop and publish guidance for developing and implementing cybersecurity plans at nuclear facilities.¹⁵ Finally, the importance of cybersecurity at nuclear facilities was highlighted at the 2016 Nuclear Security Summit and the Nuclear Industry Summit.

The nuclear industry, recognizing the urgency of the cyber threat, also has taken steps to improve security at nuclear facilities. The U.S.-based Nuclear Energy Institute, for example, has created

a policy brief on cybersecurity at nuclear power plants, has developed implementation guidance for nuclear facilities, and actively works with industry partners to chart a path forward in this area.¹⁶ Furthermore, as part of the Nuclear Industry Summit, an international working group of industry representatives was convened specifically to bring high-level attention to this threat and to develop recommendations for mitigating it within the industry context.¹⁷ This group will continue to meet, even in the absence of future Nuclear Security Summits, demonstrating the nuclear industry's commitment to addressing cyber threats to nuclear facilities.

These efforts are important steps toward more secure nuclear facilities and should be continued. However, the rapidly evolving cyber threat, combined with the expanded use of digital systems at nuclear facilities around the world, has left the nuclear industry ill equipped to get ahead of the adversary it faces. Today's defenses are no longer adequate, and a fresh look at how to best protect nuclear facilities from cyberattack is needed. The threat is too great, and the potential consequences are too high, to remain comfortable with the status quo.

15 The IAEA has published several relevant documents and is continuing to work to assemble guidance on this issue. The documents are International Atomic Energy Agency, *Technical Guidance Reference Manual: Computer Security at Nuclear Facilities*, IAEA Nuclear Security Series No. 17 (Vienna: IAEA, 2011), available at www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf; International Atomic Energy Agency, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, IAEA Specific Safety Guide No. SSG-39 (Vienna: IAEA, 2016), available at www-pub.iaea.org/MTCD/publications/PDF/Pub1694_web.pdf; International Atomic Energy Agency, *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants*, IAEA Nuclear Energy Series No. NP-T-3.12 (Vienna: IAEA, 2011), available at www-pub.iaea.org/MTCD/Publications/PDF/Pub1495_web.pdf; International Atomic Energy Agency, *Conducting Computer Security Assessments at Nuclear Facilities* (Vienna: IAEA, 2016), available at www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf; and International Atomic Energy Agency, *Computer Security Incident Response Planning at Nuclear Facilities* (Vienna: IAEA, 2016), available at www-pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf.

16 "Policy Briefs: Cyber Security for Nuclear Power Plants," Nuclear Energy Institute, July 2016, available at www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit.

17 Nuclear Industry Summit 2016 Working Group, "Working Group 1 Report: Managing Cyber Threats," presented at the Nuclear Industry Summit, March 30, 2016, available at www.nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf.

DON'T CYBERSECURITY REGULATIONS AND GUIDANCE DOCUMENTS ALREADY EXIST?

Yes. Numerous cybersecurity documents already exist, even for the specialized field of cybersecurity at nuclear facilities. These documents range from those specifically guiding the implementation of regulations to those giving general guidance that can be applied on a global scale. Although such documents are helpful in reducing the risk from non-targeted attacks, they fail to address the root cause of why many of these problems exist in the first place. Furthermore, development of these *frameworks* is constrained in various ways—for example, the IAEA operates by consensus, often leading to delays, and regulatory agencies are often reluctant to impose undo financial burdens.

NTI's *Cyber Priorities* project is unique in that it takes a different approach. Instead of a long checklist of tasks that need to be completed by everyone from technicians to management, it is a simple list of four strategic priorities. These priorities were determined by experts to be the foundational issues that, if addressed, would significantly reduce the cybersecurity risks surrounding nuclear facilities. Because these *priorities* are the key pillars of a strategy, not simply a checklist, implementation will not happen overnight. They are intended to help frame the conversation about the most effective ways not only to reduce the risk today, but also to get ahead in the future.

Existing Guidance and Regulatory Documents. The existing U.S. nuclear-specific cybersecurity *guidance and regulatory guidance* can be grouped into four general categories: NRC, IAEA, DHS, and commercial.¹⁸

Additional *frameworks* have been developed for the critical infrastructure sector, such as the National Institute of Standards and Technology (NIST) National Institute of Standards and Technology Cybersecurity Framework.

NRC Regulatory Guide 5.71 was developed specifically to assist nuclear facilities in complying with the NRC regulation (10 CFR 73.54) that requires NRC licensees to verify that their computers, digital communication systems, and networks are protected from cyberattacks. This guide covers forming a cybersecurity team; identifying critical digital assets; designing and implementing defense-in-depth protective strategies, controls, incident response, and contingency planning; and incorporating cybersecurity into physical security. The cybersecurity regulations in this guide are largely based on NIST cybersecurity standards (NIST SP 800-53 and 800-82).¹⁹

IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual: Computer Security at Nuclear Facilities provides general cybersecurity guidance for the nuclear industry. Intended to be used on a global scale, it is a compilation of “special provisions, best practices, and lessons learned” that apply to nuclear facilities and other critical infrastructure. It recognizes that regulation is the responsibility of state-level regulatory bodies and includes two main parts: a management guide and an implementation guide. The management guide covers regulatory and management considerations, management systems, and organizational issues. The implementation guide provides a basic overview of threats, vulnerabili-

ties, and risk management strategies, and it states how these specifically apply to nuclear facilities. The guide is largely based on the ISO 27000 series by the International Organization for Standardization.²⁰

Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors was produced by DHS to assist the nuclear sector in complying with the 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity. This framework is based on cybersecurity standards and best practices. It includes general guidance on risk management principles, and it provides a structure for organizations to improve cybersecurity risk management.²¹

Cybersecurity Plan for Nuclear Power Reactors, or NEI 08-09, is a document produced by the U.S.-based Nuclear Energy Institute to assist licensees in developing and implementing the Cybersecurity Plan required by the NRC as a license condition. This comprehensive guidance details key elements of an appropriate cybersecurity plan and provides a template for licensees to use to achieve compliance with U.S. regulation 10 CFR 73.54.

Commercial products to protect critical infrastructure against cyberattacks are available. One example of a commercial product is the RIPE Framework by Ralph Langner, which is based on application of quality management concepts for industrial control systems. Other commercial efforts to assist with the implementation of cybersecurity of critical infrastructure also exist.²²

18 Other countries have similar types of documents (where they exist).

19 Available online at www.nrc.gov/docs/ML0903/ML090340159.pdf.

20 Available online at www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.

21 Available online at www.us-cert.gov/sites/default/files/c3vp/framework_guidance/nuclear-framework-implementation-guide-2015-508.pdf.

22 For example, see Ralph Langner, “The RIPE Framework: A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security,” Langner Communications Whitepaper, available at www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf.



FOUR PRIORITIES TO DRIVE ACTION

In response to current realities and challenges, NTI assembled an international group of technical and operational experts with backgrounds in computer security, nuclear safety systems, nuclear engineering, industrial control systems, and nuclear facility operations. This group was tasked with identifying the core elements of a new strategy, then with focusing on those elements that would have the greatest possible effect.

Over 12 months, the group identified four overarching priorities that, if implemented, would dramatically reduce the risk of damaging cyberattacks on nuclear facilities. In many ways, these priorities are not novel—similar concepts are being put to use elsewhere. Alone or in combination, however, each would provide considerable leverage on the threat posed to nuclear facilities.

1. Institutionalize cybersecurity. Implementation of robust processes and practices is essential for the effective management of complex systems and is at the heart of long-standing quality management programs used across industry. Given the rapidly evolving cyber threat, however, such practices are generally not yet in place for cybersecurity in nuclear facilities. Nuclear facilities should learn from and actively integrate the practices employed by safety and physical security programs to strengthen and sustain their cybersecurity programs.

2. Mount an active defense.²³ The static cybersecurity architectures at today's nuclear facilities are neither effective enough on their own to prevent a breach by a determined adversary, nor are they effective enough to respond once a compromise has occurred. Nuclear facilities need to update their prevention and response plans—steps that are essential but that are challenged by the global shortage of technical experts.

3. Reduce complexity. Complexity is the enemy of security. Today's nuclear facilities consist of thousands of digital systems. The security effects of these systems, their functionalities, and how they interact are not always fully understood. Although networks may be initially characterized, this information is not always kept up to date. When it comes to the most critical systems, the most advantageous option may be to eliminate digital complexity entirely by transitioning to non-digital systems.

4. Pursue transformation. The global community is in the early stages of understanding the magnitude of the cyber threat. In many ways, humans have created systems that are too complex to manage; in most cases, risks cannot even be quantified. As a result, there is a fundamental need for transformative research to develop hard-to-hack systems for critical applications.

²³ In other industries, the term *active defense* can sometimes imply that defenders should “hack back” against adversaries. The term is used here merely to indicate a dynamic defense, distinct from “hacking back.”

The priorities listed are complementary and offer differing benefits as well as implementation challenges. For example, an initial active defense capability could be put into place relatively quickly. Implementation of robust processes could occur over the mid term, and reduction of complexity will undoubtedly be a multiyear process. In the following sections, each of these strategic priorities is described in more detail.

PRIORITY: INSTITUTIONALIZE CYBERSECURITY

Since the partial nuclear reactor meltdown at Three Mile Island in 1979, and more recently the terrorist attacks of September 11, 2001, nuclear facilities have focused much of their attention on preventing accidents and physical security lapses. Today, safety and security programs are largely institutionalized and are part of daily operations. Such programs address plant design and choice of technologies, hiring, management and training of the people hired to work at a facility, and processes that govern operations.

Although safety and security are generally considered separate concerns, the increasingly widespread use of digital technologies at nuclear facilities has virtually eliminated the gap between them. A cyberattack, after all, can have implications for nuclear safety or security—and in a worst-case scenario, perhaps both. Recognizing that cyberattacks may have serious physical consequences on par with a safety or security incident, cybersecurity must be treated with at least the same rigor and attention as are safety and physical security. Specifically, cybersecurity must be embedded in the daily operations of a nuclear facility in three key areas:

- ▶ **People and organizational culture.** Awareness of the importance of cybersecurity should be embedded throughout the organization, from the chief executive officer to the most junior employees. Lessons learned from both safety and physical security demonstrate

A universal understanding of the importance of cybersecurity at any given facility would help reduce one of the vulnerabilities most often exploited by adversaries—humans.

that program effectiveness depends on having personnel understand their role and how it fits into a larger context. This understanding should also apply to personnel outside of the facility, such as suppliers and vendors. Leadership should reinforce this priority in identifying roles, in hiring and training staff, and in performing personnel assessments. General awareness training should be provided for all staff members. A universal understanding of the importance of cybersecurity at any given facility would help reduce one of the vulnerabilities most often exploited by adversaries—humans.

- ▶ **Design solutions.** Systems at nuclear facilities must be designed and defended appropriately. Lessons learned from the graded application of safety and physical security measures can be applied to cybersecurity to ensure that the systems performing the most important functions are engineered to be the least likely to fail. Under this graded approach, options for designing the most critical systems would be significantly constrained and subject to more stringent requirements in an effort to minimize the likelihood of intentional or accidental failure, or of malicious operation. Similarly, facilities would be limited in the products they could purchase for these systems, and vendors would have to demonstrate that their products and processes are appropriate for secure design.

► **Facility processes and practices.** Effective processes and practices are essential for the safe and secure operation of nuclear facilities. Supervisors must ensure that digital systems are designed, operated, and maintained appropriately in accordance with the significance of the cyber threat. For example, these practices should include classifying digital systems, outlining permissible system architectures, defining change and review processes, and updating procedures for response to severe incidents. Developing and implementing processes and practices to ensure cybersecurity—just as the industry already has done to ensure safety and physical security—is crucial.

In addition to these efforts, facilities must conduct the appropriate analyses and preparations for emergency response in the event of a cyber incident. This investment in emergency preparedness figured prominently in the institutionalization of safety and physical security at nuclear facilities and is just as important in the cyber realm.

PRIORITY: MOUNT AN ACTIVE CYBER DEFENSE

As digital technologies have spread, cyber vulnerabilities have grown—often without the full awareness of those charged with defending nuclear systems. Cyber defense strategies at nuclear facilities tend to rely on the concept of static prevention—that building the right walls in the right places will prevent even the most serious attacks. Unfortunately, recent examples of malware found in even the most secure nuclear facilities suggest that this assumption may no longer be true.²⁴ Cases mentioned earlier demonstrate that commonly relied-upon measures such as air gaps, firewalls, and antivirus programs fail against even untargeted viruses and likely would crumble in the face of a well-resourced, determined adversary.

²⁴ For example, the Stuxnet virus infected a highly sensitive uranium enrichment facility that was air gapped. For more information, see the appendix.

2010

CYBER INCIDENT

IRAN **Natanz Fuel-Enrichment Plant**



The United States and Israel are reported to have jointly developed the Stuxnet virus, which was deployed in two stages and destroyed nearly 1,000 of Iran's 9,000 IR-1-type gas centrifuges. The first stage, reportedly released as early as 2005, was active between 2007 and 2009. This version targeted Siemens programmable logic controllers (PLCs) at the Iranian Natanz uranium-enrichment facility and attempted to disrupt uranium enrichment by closing the valves that fed uranium hexafluoride gas into the centrifuges. This version of Stuxnet ceased operation in July 2009.

The second version of the Stuxnet virus was reportedly released into Natanz in June 2009 and was revealed in 2010. This version attempted to disrupt uranium enrichment by altering the rotational speed of the gas centrifuges at Natanz. It is likely that this version of Stuxnet was introduced to a computer at the Iranian Natanz uranium enrichment facility through a USB stick, demonstrating that even facilities disconnected from the Internet are vulnerable to attack.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

Facility operators should work to reduce complexity wherever possible in systems controlling critical functions of nuclear processes.

An effective “active defense” capability is essential to developing stronger cyber defenses. For the purposes of this report, *active defense* is defined as *the continuous process of analysts monitoring for, responding to, learning from, and applying their knowledge of threats internal to the network in order to detect, block, and expel adversaries.*²⁵ Such a strategy incorporates the lessons learned from recent attacks on critical infrastructure and is based on the assumption that it is not possible to prevent all cyberattacks before they occur. The ultimate goal is to develop and implement a capability that allows facility staff members to detect and disrupt cyber intrusions as they happen—a pragmatic approach to cyber defense.

Implementation will require several steps. Facilities will need to characterize their systems and conduct risk analyses and engineering evaluations to determine which systems and data are most important and vulnerable—and therefore have the greatest need of protection. Armed with an understanding of which systems are most critical and how systems function and interact, the cybersecurity team can focus on detecting attackers, anticipating their next moves, and eliminating their attack opportunities.

This mission requires team members with a variety of skill sets, including threat intelligence analysts, intrusion analysts, incident responders, forensic analysts, malware reverse engineers,

and team directors. Team members could be present either on- or off-site. A key challenge to this approach is the difficulty associated with hiring and retaining highly technical staff. One solution could be for national governments to make experts available to the industry or to develop shared technical resources.

PRIORITY: REDUCE COMPLEXITY

The increased digitization and automation of technologies and processes at nuclear facilities in recent years have created a highly complex system of devices, networks, and systems that is often difficult to characterize. Complexity can compromise cybersecurity in two key ways. First, it heightens the likelihood that various components have unknown functionalities or interactions that can serve as entry points for an adversary. Second, it leads to higher levels of activity and “noise” on the network, which can be used as camouflage to allow an adversary to operate virtually undetected.

As an example, as modern nuclear power reactors have replaced their predecessors in nuclear energy programs all over the world, industry has seen an increasing demand for precise control of internal processes. This demand has been met with increased digitization, and additional instrumentation, sensors, controls, and communications have been implemented across fundamental plant networks.

Although digitization has brought many benefits, it also has made systems more complex. These systems, built on top of one another over time, are too often not fully understood by any one individual or operational entity. Thousands of nodes communicate across multiple layers in a variety of protocols, operating systems, and shared applications. Technologies offered by vendors often include a variety of modes of connectivity, ranging from non-declared radio

²⁵ To reiterate, the authors do not advocate the “hack back” approach sometimes associated with this term. The authors also acknowledge that, for attacks of a certain magnitude, governmental organizations and even the diplomatic corps could be brought in to find a resolution.

communications devices to Bluetooth and Wi-Fi.²⁶ Moreover, generic system designs in use in facilities around the world can include intricate layers of enhanced features and functionalities that are very difficult to understand—especially when crafted without security as a primary consideration.

In addition to the high levels of complexity at the facility level, regulators, vendors, and operators alike face a significant challenge in the supply chain from which all facility technologies are sourced. Vendors in the supply chain are not held accountable for the security of the products and services they provide—and in many cases, would not even be capable of assuring security.²⁷ Operators and vendors are driven by market forces when awarding contracts and rarely have access to important information about the myriad individuals, companies, and organizations involved in designing, manufacturing, and transporting final products to the customer. Because each stage of information exchange—from design to delivery—provides a new opportunity for exploitation, the supply chain exacerbates the complexity conundrum and can even introduce new and undetected cyber vulnerabilities to nuclear facilities.

System complexity also has made defense more challenging, but regulators and operators alike have continued to use outdated physical security models for threat, response, and deterrence in cyberspace and rely primarily on regulations to address the cyber threat. Unfortunately, this strategy can only manage the cyber threat—not eliminate it.

26 Michael J. Assante, Tim Roxey, and Andy Bochman, “The Case for Simplicity in Energy Infrastructure—for Economic and National Security,” Center for Strategic and International Studies, Washington, D.C., October 2015, available at www.csis.org/publication/case-simplicity-energy-infrastructure.

27 Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*, (Washington, D.C.: Center for a New American Security, 2014), available at www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.

2011 CYBER INCIDENT

UNITED STATES Oak Ridge National Lab



Oak Ridge National Laboratory in Tennessee was victimized by a sophisticated cyberattack that exploited a zero-day, or previously undiscovered, vulnerability in Internet Explorer that allowed attackers to infect computers when users visited malicious websites. The attack was first delivered via a spear-phishing e-mail sent in April 2011 that was disguised as an e-mail from the human resources department. The e-mail contained a link to a malicious website; when users visited the site, malware took advantage of the vulnerability in Internet Explorer to download the malware to various computers. About 530 of 5,000 employees at Oak Ridge received the e-mail; only 57 clicked on the link, and only two computers were infected.

Although the lab started blocking malicious e-mails soon after they started coming in, administrators quickly discovered that a server had been breached when they noticed data leaving the network. This system was cleaned up, but then other servers began experiencing similar effects; the malware had camouflaged itself on systems and had been designed to self-eradicate if attempts to compromise a given system were unsuccessful. Ultimately, a few megabytes of data were taken before the lab shut down Internet access to prevent further data loss.

This incident highlights the ways in which attackers leverage any access gained through spear-phishing e-mails, and it shows that even facilities keenly aware of the cyber threat are still vulnerable to it.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

To address this problem, facility operators should work to reduce complexity wherever possible in systems controlling critical functions of nuclear processes. Where complexity must exist, it should be commensurate with the level required to accomplish only the system's immediate task, and it should be appropriately documented. Those systems performing the most important functions should be engineered to be the least likely to fail. In some cases, recognizing the trade-offs, it may be appropriate to transition to non-digital systems to greatly reduce the cyber threat.

PRIORITY: PURSUE TRANSFORMATION

Today's targeted attacks reveal significant shortfalls in the means used to defend and the methods used to minimize consequences. Reducing complexity, institutionalizing cybersecurity, and establishing an active defense are pillars of a more robust strategy. Over the longer term, however, getting ahead of the growing threat will require new approaches, methods, and technologies. That need is particularly pressing for cyber-physical systems, including nuclear facilities, in which safety and security are intertwined. In addition to the nuclear industry, these systems are pervasive and are found in the aviation and automobile industries, in power generation and distribution, and in the military. Although development of high-assurance and resilient systems is becoming an increasingly active area of research, much more is needed.²⁸

Digital systems historically have been designed for functionality, not security. That has been particularly true for hardware and software that controls industrial processes. Because they were usually stand-alone systems, isolated from busi-

Digital systems historically have been designed for functionality, not security. That has been particularly true for hardware and software that controls industrial processes.

ness networks and the Internet, these devices typically had limited built-in security. Unfortunately, in today's interconnected world, this isolation, even of legacy systems, can no longer be assured. With the development of ever-more sophisticated hacking tools, "security through obscurity" no longer holds true.

Building robust and secure systems (i.e., trustworthy and defensible systems) for critical applications will require rigorous software and hardware development, as well as means to assess and verify that trustworthiness and security. As an example, research is underway on the application of formal methods to ensure that software and hardware are functionally correct and also meet the safety and security goals.²⁹ This approach is already used for critical National Aeronautics and Space Administration (NASA) applications and automated train safety systems and is being improved through existing research and development programs,³⁰ but it must be developed and applied more broadly for critical applications.

In addition to hardened hardware and software, improved models are needed to simulate the behavior of these complex cyber-physical

28 For example, within the U.S. Department of Defense, the Defense Advanced Research Projects Agency has a research program to develop High-Assurance Cyber Military Systems. See www.darpa.mil/program/high-assurance-cyber-military-systems. In addition, see Department of Homeland Security, *A Roadmap for Cybersecurity Research* (Washington, D.C.: DHS, 2009), available at www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf.

29 See, for example, Jeffrey Voas and Kim Schaffer, "Insights on Formal Methods in Cybersecurity," *Computer*, vol. 49, no. 5 (2016): 102-5, doi:10.1109/MC.2016.131.

30 See, for example, "Atelier B," Clearsy Engineering website, available at www.atelierb.eu/en/.

systems and to understand the potential implications of a cyberattack. When developed, such models could provide a basis for cyber-induced safety analysis when existing risk models are not applicable. Models exist to simulate the behavior of safety-related failures; they are typically unable to consider multiple operations, failures, or widespread loss of data integrity that would never occur naturally but could be induced via a concerted cyberattack.

Research also should pursue the development of *21st-century non-digital solutions* that would be inherently secure. Yesterday's analog technologies were not vulnerable to cyberattacks, and many nuclear facilities continue to benefit from those systems. As those systems become obsolete, they are being replaced with digital systems that offer increased performance and reliability but also cyber vulnerabilities. It may be possible, however, to develop new, non-digital approaches that are cybersecure and that have the improved performance characteristics necessary. For example, a solid-state analog solution³¹ was recently announced to eliminate vulnerability to Aurora-type attacks.³² In the future, one can envision using modern technologies to construct high-performance, verifiable, non-digital solutions for critical safety and security functions.

31 Timothy Roxey, North American Electric Reliability Corporation, personal communication.

32 Aurora attacks, first discovered in 2006, are asynchronous attacks against rotating machines that result in catastrophic failure. See Michael Swearingen et al., "What You Need to Know (and Don't) About the AURORA Vulnerability," *Power*, September 1, 2013, available at www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/.

2014 CYBER INCIDENT

SOUTH KOREA Korea Hydro and Nuclear Power Company



Korea Hydro and Nuclear Power Co., which operates 23 of South Korea's nuclear reactors, was hacked in December 2014. The hackers, claiming to be an anti-nuclear group based in Hawaii, used phishing e-mails to introduce malware into the commercial network. They then were able to steal the blueprints and manuals for two nuclear power plants, believed to be the Gori and Wolsong plants in South Korea. The hackers also obtained radiation-exposure estimates for surrounding areas, personal data for 10,000 employees, and electricity flow charts. These data were leaked via Twitter, and the hackers threatened "destruction" if Korea Hydro and Nuclear Power Co. did not shut down three reactors. The company ignored the threat, and nothing came of it.

In March 2015, more files, including blueprints and test data, were leaked via Twitter, and the hackers demanded money to not hand over additional information to countries that they claimed were interested in purchasing the information. South Korea publicly blamed North Korea for the attack because the phishing attacks could be traced to North Korean IP addresses; North Korea vehemently denied the claims.

This incident highlights the complexities of attribution in cyberspace, as well as concerns about the exfiltration of data from nuclear facilities.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.



TAKING ACTION

In the last several years, countries have made great strides in improving physical security at nuclear facilities in the name of preventing a catastrophic act of nuclear terrorism. Many of the same outcomes can be achieved in the cyber realm—making it more important than ever to pursue an ambitious, forward-looking strategy grounded in technically sound priorities for improving cybersecurity at nuclear facilities. Because an investment of time, focus, and resources is required, it is crucial to begin now. Actions for governments, regulators, and industry follow.

GOVERNMENTS AND REGULATORS

Governments, and particularly nuclear regulators, play a key role in setting requirements for security at nuclear facilities. In an effort to better reflect these priorities in national requirements for licensees, governments and regulators should

- ▶ **Work to develop and implement regulatory frameworks** that promote the institutionalization and ongoing improvement of cybersecurity at nuclear facilities; these frameworks might draw on lessons learned from progress made in nuclear safety and physical security;
- ▶ **Promote the development of active defense strategies and capabilities** by enhancing cyber expertise within governmental and regulatory bodies, sharing relevant threat information with industry, considering how to develop and exercise cyber incident response capabilities, and providing additional resources

for defense against threats beyond those that facilities could reasonably be expected to handle;

- ▶ **Support—with financial, personnel, and research resources**—facility efforts to characterize networks, understand functionalities and interactions, and ultimately minimize complexity in critical systems;
- ▶ **Undertake or fund transformative research** into the technologies, methods, and approaches that will be necessary to get ahead of the threat; and
- ▶ **Draw talented people into the cyber-nuclear field** by investing in education and training programs and by providing incentives to take jobs in this critical security sphere.

NUCLEAR INDUSTRY

Nuclear facilities, and the industry in general, are the first line of defense when addressing the cyber threat. In the near term, industry should

- ▶ **Apply lessons learned** from industry experiences with safety and physical security to institutionalize and promote ongoing improvements in cybersecurity at nuclear facilities;
- ▶ **Initiate the development** of active defense capabilities at the facility level, including perhaps developing mutual-aid agreements or other cross-industry resources to allow facilities to access needed skills;

- ▶ **Work to reduce system complexity** at nuclear facilities by characterizing systems, identifying excess functionalities and removing them where possible, and working with vendors to develop non-digital systems and secure-by-design products where appropriate;
- ▶ **Support the cybersecurity efforts** of relevant organizations, including the IAEA, the WNA, WANO, and INPO in an effort to continue the international dialogue and contribute to key research and development necessary to improve cybersecurity; and
- ▶ **Provide training opportunities** and assistance to boost human capacity across the cyber-nuclear field, especially in countries with new or expanding civilian nuclear energy programs.

INTERNATIONAL ORGANIZATIONS

The magnitude of the threat can overwhelm already overtaxed governments and can strain limited resources. International organizations can help lessen this burden. In the short term, international organizations should

- ▶ **Support, through international dialogue,** provision of guidance and training to governments and facilities, and definition of relevant best practices, international cooperation and an expanded focus on cybersecurity at nuclear facilities;
- ▶ **Facilitate sharing** of threat information where possible and appropriate;
- ▶ **Provide platforms** for discussing and developing solutions for reducing complexity; and
- ▶ **Foster innovation** and continue to think creatively about how to mitigate the threat and recruit a variety of voices and perspectives to join the conversation.

2016 CYBER INCIDENT

JAPAN University of Toyama Hydrogen Isotope Research Center



In June 2016, it was discovered that hackers had used a spear-phishing attack to steal research and personal data from the University of Toyama Hydrogen Isotope Research Center. This research center is a world leader in research into tritium, a radioactive isotope of hydrogen that serves as fuel for controlled nuclear fusion and is an integral part of hydrogen bombs.

The hackers had posed as curious Tokyo university students with questions for several researchers, and they transmitted the malware through infected documents attached to e-mails sent to the researchers. Only one researcher's computer was compromised, with the first data exfiltration occurring in November 2015. Large amounts of data—more than 1,000 compressed files—were collected and transmitted to an online server before attackers stopped collection in late December 2015. More compressed files were transmitted in March 2016. When a third batch of files was stolen in June 2016, an outside entity noticed the suspicious transfers and notified the lab.

In addition to research results regarding the discharge of contaminated water from the Fukushima No. 1 nuclear power plant, personal information for nearly 1,500 individuals who collaborated with the university also may have been stolen. Investigators believe the attackers managed to steal more than 59,000 files in total, and they noted that the malware samples they examined were programmed to search for the term “IAEA,” an acronym for the International Atomic Energy Agency. This attack highlights the degree to which hackers targeting nuclear facilities are successfully using spear-phishing to compromise networks and exfiltrate data.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

The consequences of a cyberattack on a nuclear facility would be serious and far reaching. Institutionalizing cybersecurity at nuclear facilities, implementing active defense strategies, and minimizing complexity would address many of the serious vulnerabilities the world faces today, and investing in transformative research and

development will lay the groundwork for an even more secure future.

Governments, industry, and international organizations all have a role to play in addressing and outpacing this threat. The risk is too great to accept the status quo.

THE CYBER PRIORITIES PROCESS

NTI began examining the cyber threat to nuclear facilities in 2014. Recognizing the importance of grounding any proposals or recommendations in a strong technical foundation, NTI solicited input from an international group of experts in all technical aspects of this question—from nuclear engineering, to industrial control and instrumentation, to system design and engineering, to digital instrumentation and control, to cybersecurity. This breadth of experience allowed NTI to more completely understand the threat—and to develop the fresh, forward-looking solutions required to outpace it.

NTI hosted two initial meetings in 2015, the first in Washington, D.C., and the second in Vienna, Austria. These meetings allowed NTI to refine its thinking on this question and to come to the conclusion that defining a set of high-level priorities that respond directly to the threat—and not to the constraints and concerns that can sometimes cloud it—would be useful to policymakers, regulators, and operators alike.

Armed with this mission, NTI convened a group of interested technical experts (listed below) to discuss the nature of the threat, to evaluate the utility of the current strategy for addressing it, and to develop recommendations as to the measures that are actually required to not only mitigate the threat, but also get ahead of it. Additionally, NTI commissioned papers from three participants—the SANS Institute’s Michael As-sante, Indigon Consulting’s Anna Ellis, and Idaho National Laboratory’s Rob Hoffman—to outline the technical foundations for three priorities.

2016 CYBER INCIDENT

GERMANY Gundremmingen Nuclear Power Plant



In April 2016, reports surfaced that the Gundremmingen Nuclear Power Plant in Bavaria was infected with malware. The discovery was made in the plant’s B unit, in a computer system that had been retrofitted in 2008 with data-visualization software accompanying equipment for moving nuclear fuel rods. Viruses had also infected 18 removable data drives associated with computers not connected to the plant’s operating systems. There was no apparent damage.

Two of the viruses found on the plant’s fuel rod-monitoring system and on the removable data drives were W32.Ramnit and Conficker. W32.Ramnit targets Microsoft Windows software systems and is designed to steal files and allow an attacker to remotely control a system that is connected to the Internet. It is often spread using removable data sticks. Conficker, which can spread through networks and jump onto removable data drives, was designed to obtain login information and financial data. The station’s operator stated that the viruses “appear not to have posed a threat to the facility’s operations because it is isolated from the Internet.” This statement raises questions about how the “isolated” plant became infected and why the malware went undetected for so long.

For a longer list of incidents, as well as sourcing information, please visit www.nti.org/cyberpriorities.

GROUP MEMBERS

Michael Assante*[§]

Director, Critical Infrastructure
Curriculum Lead, ICS/SCADA SANS
Institute
United States of America

Robert Anderson

Senior Controls Consultant
Idaho National Laboratory
United States of America

Sunha Bae

Researcher
National Security Research Institute
Republic of Korea

Ian Buffey, Ph.D.

Technical Director
Atkins Global
United Kingdom

Jor-Shan Choi

Consultant/Visiting Scientist
Lawrence Livermore National
Laboratory
Affiliated Associate Director
UC Berkeley Nuclear Research Center
United States of America

Anna Ellis[§]

Co-Founder
Indigon Consulting Ltd.
United Kingdom

Guido Gluschke

Director, Institute for Security and
Safety (ISS)
Managing Co-Director, ISS
Brandenburg University
of Applied Sciences
Germany

Roger Green

Chief Executive Officer
Disruption Forum Inc.
United States of America

Robert Hoffman[§]

Cyber Security Consultant
Idaho National Laboratory
United States of America

Gary Johnson

Independent Consultant
United States of America

Anno Keizer[†]

Security Manager
URENCO Nederland B.V.
The Netherlands

Dr. So Jeong Kim

Head, Cybersecurity Policy
and Resilience Program
National Security Research Institute
South Korea

Phil Litherland

Design Authority Electrical &
Industrial Control Systems
CISO Operational Technology
EDF Energy Nuclear New Build
United Kingdom

Timothy Roxey

Chief Security Officer
North American Electric Reliability
Corporation
United States of America

Ron Southworth

Director, Australian Operations
Lofty Perch Inc.
Australia

Chris Stevens

IT Security Advisor
Australian Nuclear Science and
Technology Organization
Australia

Dr. Ferenc Suba

Cybersecurity Consultant
Cybersecurity Solutions LLC
Hungary

Jean-Luc Trollé

Nuclear Security Information Advisor
EDF
France

Arthur van der Weerd

Security Specialist,
National Cyber Security Centre
The Netherlands

Timo Wiander

Information Security Manager
Fennovoima
Finland

* NTI Project Technical Lead

[§] Author of supporting technical paper

[†] Vice Chair, Nuclear Industry Summit Working Group on Managing Cyber Threats

APPENDIX: CYBER INCIDENTS AT NUCLEAR FACILITIES

This table lists 23 publicly disclosed cyber incidents that have occurred at nuclear facilities around the world since 1990. It is possible that

more incidents have occurred that have not been publicly disclosed or for which the details are classified or otherwise unavailable.

For more information on these incidents and sourcing, please see www.nti.org/cyberpriorities

#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
1	January 1990	Bruce Nuclear Generating Station	Canada	Software error leading to release of radioactive water	Accidental
2	September 1991	Sellafield reprocessing plant	United Kingdom	Software bug leading to unauthorized opening of doors; widespread software errors	Accidental
3	February 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
4	June 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
5	January 2000*	Kurchatov Institute	Russian Federation	Bug in nuclear materials accounting software	Accidental
6	January 2003	Davis-Besse Nuclear Power Station	United States	Virus blocked operator access to reactor core information	Accidental
7	June 2005*	Japanese Nuclear Power Plants	Japan	Data release	Unknown
8	August 2006	Browns Ferry Nuclear Plant	United States	Technical failure	Accidental
9	December 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
10	March 2008	Edwin I. Hatch Nuclear Power Plant	United States	Shutdown caused by software update	Accidental
11	March 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
12	June 2010*	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
13	April 2011	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
14	September 2011	Areva	France	Network intrusions	Unknown
15	October 2011*	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
16	May 2012*	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
17	November 2012	Susquehanna Nuclear Power Plant	United States	Technical failure	Accidental

* Indicates date of discovery or public disclosure, where appropriate

#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
18	January 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
19	December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
20	February 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyberattack	Unknown
21	February 2016*	Nuclear Regulatory Commission/U.S. Department of Energy	United States	Employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
22	April 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered plant's fuel rod monitoring system	Unknown
23	June 2016*	University of Toyama, Hydrogen Isotope Research Center	Japan	Data theft via spear-phishing	Intentional

* Indicates date of discovery or public disclosure, where appropriate

ABOUT NTI

The Nuclear Threat Initiative 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, NTI is guided by a prestigious, international board of directors. Sam Nunn serves as chief executive officer, Des Browne is vice chairman, and Joan Rohlfing serves as president.

For more information, visit www.nti.org.

The past decade has seen unprecedented progress in the security of nuclear materials and facilities. As key improvements to physical security have been implemented, however, a threat that is potentially even more challenging is endangering these gains: the cyber threat.

Cyberspace provides a new opportunity for determined adversaries to wreak havoc at nuclear facilities—possibly without ever setting foot on-site. Cyberattacks could be used to facilitate the theft of nuclear materials or an act of sabotage that results in radiological release. A successful attack could have consequences that reverberate around the world and undermine global confidence in civilian nuclear power as a safe and reliable energy source.

Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities takes a fresh look at cybersecurity at nuclear facilities and offers a set of ambitious, forward-leaning priorities and recommendations.



Nuclear Threat Initiative
1747 Pennsylvania Ave NW, Seventh Floor
Washington, DC 20006
www.nti.org/cyberpriorities