GLOBAL ACTION ON CYBERSECURITY AT NUCLEAR FACILITIES: MOVING BEYOND THE STATUS QUO

Michelle Nalabandian[1], Alexandra Van Dine[2], Page Stoutland[3]
Nuclear Threat Initiative
1747 Pennsylvania Avenue NW, Seventh Floor
Washington, D.C. 20006

ABSTRACT

Cyber threats to nuclear facilities are becoming more sophisticated each day, and the technical capacity to address the threat remains limited. This threat is global and undermines the security of nuclear materials and facility operations. Traditional nuclear security practices focus primarily on preventing physical attacks—putting in place "guns, guards, and gates" to prevent theft of materials to build a bomb or sabotage of a nuclear facility—with the assumption that nuclear facilities are air-gapped and safe from traditional cyber attacks. While physical security is of vital importance, the threat of a cyber attack is escalating as is the technical means and capabilities of malicious actors. All countries are vulnerable, and nuclear cybersecurity practices have not kept pace with the threat. The 2016 NTI Nuclear Security Index found that many countries are ill-prepared to protect nuclear facilities against cyber attacks that could facilitate the theft of weapons-usable nuclear materials or even cause a significant radiological release like the accident at Fukushima. Much more needs to be done by governments and the private sector to effectively secure and prevent the theft of nuclear materials or sabotage of nuclear facilities. The paper discusses the 2016 NTI Nuclear Security Index findings, identifies where gaps remain, and provides recommendations for further global action. This paper also highlights actions taken at the 2016 Nuclear Security Summit and the 2016 Nuclear Industry Summit to advance the dialogue on securing nuclear materials and facilities from cyber attack.

---

[1] Michelle Nalabandian serves as program officer in the Scientific and Technical Affairs program at the Nuclear Threat Initiative (NTI), where she manages operational elements of the program and conducts research and analysis that focuses on the security of nuclear and radiological materials globally, cybersecurity for nuclear facilities, and biosecurity threats. She was a 2015 PONI Nuclear Scholar and a 2015 Fellow of the Emerging Leaders in Biosecurity Initiative. She holds a bachelor's degree from George Mason University.

[2] Alexandra Van Dine is a program associate with the Scientific and Technical Affairs team at NTI, where she works on the NTI Nuclear Security Index and cybersecurity-related projects. She has presented research on cybersecurity at nuclear facilities at U.S. Strategic Command and Los Alamos National Laboratory. She is a graduate of Georgetown University's Walsh School of Foreign Service.

[3] Page Stoutland is NTI's vice president for Scientific and Technical Affairs, where he is responsible for NTI's scientific and technically related projects designed to strengthen nuclear security around the world, including the NTI Nuclear Security Index, strengthening technical cooperation with China, and cybersecurity at nuclear facilities. Prior to joining NTI, Stoutland held a number of senior positions at Lawrence Livermore National Laboratory. Previously, he held positions within the U.S. Department of Energy and at Los Alamos National Laboratory. Stoutland holds a bachelor's degree from St. Olaf College in Northfield, Minnesota and a doctorate in chemistry from the University of California, Berkeley.

BACKGROUND

Today, nuclear facilities are increasingly vulnerable to cyber attacks due to the expanded use of digital controls and the growing sophistication of attackers. A cyber attack could facilitate the theft of nuclear material or an act of sabotage of a nuclear facility in a variety of ways, resulting in potentially catastrophic consequences that would have a global impact. This frightening reality highlights the need for a concerted global action aligning efforts for combatting both cyber and physical threats against nuclear facilities.

With evolving global threats in mind, the 2016 NTI Nuclear Security Index (NTI Index) includes an assessment of how states are protecting their nuclear facilities against cyber threats. The NTI Index found that 20 out of 47 countries with weapons-usable nuclear materials or nuclear facilities that, if sabotaged, could cause significant off-site health consequences, do not even have basic requirements to protect nuclear facilities from cyber attacks.

Though the Nuclear Security Summits (NSS) and the Nuclear Industry Summits (NIS) played a valuable role in raising awareness about the global threat posed by nuclear and radiological materials, cyber attacks at nuclear facilities went largely unaddressed until the 2016 NSS and NIS. Given that cybersecurity at nuclear facilities is an evolving and emerging threat, the Summits should be credited for attempting to make progress in this area, regardless of how incremental the progress may be.

THE THREAT

At present, 24 countries have one kilogram or more of weapons-usable nuclear materials and nearly 2,000 metric tons of weapons-usable nuclear materials are stored at hundreds of sites around the world. Although this amount has decreased over the past few years, much of it remains too vulnerable to theft. Terrorist organizations have publicly declared their desire to acquire and use nuclear weapons, and given the vast quantity of nuclear materials that exists worldwide, the path to a terrorist bomb is not hard to imagine. Such an attack would result in catastrophic, global consequences with implications for economies, commerce, militaries, public health, the environment, civil liberties, and the stability of governments. An additional 23 countries with nuclear facilities remain vulnerable to sabotage, which could result in a significant radiological release causing serious off-site health consequences. Looking ahead, a growing number of countries are exploring nuclear energy even though many lack the legal, regulatory, and security frameworks to ensure that their facilities are safe as well as secure.

Meanwhile, the cyber threat has expanded exponentially in recent years, with a series of damaging, high-profile attacks that have made headlines around the world. Recent attacks against banking and commerce systems, private companies, and national governments highlight the growing gap between the threat and the ability to respond to or manage it. Like all critical infrastructure, nuclear facilities are not immune to a cyber attack—a particular concern, given the potentially catastrophic consequences. For example, in 2012, a power reactor at the Susquehanna Nuclear Power Plant in Pennsylvania was shut down when operators realized that

the computer system that controlled the water level of the reactor was not functioning correctly.[4] If a reactor cooling system could be deliberately disabled, it could potentially result in a disaster similar to the events at Fukushima, Japan.

A cyber attack against a nuclear facility has the potential to disrupt vital digital safety systems and manipulate nuclear facility security. Such attacks could facilitate the theft of nuclear materials or an act of sabotage against a nuclear facility. For example, access control and accounting systems could be compromised, allowing the entry of unauthorized persons seeking to obtain nuclear material or to damage the facility. Contrary to popular belief, critical systems that are not connected to the internet (i.e., air-gapped) are still vulnerable to cyber attack. An example is the infamous Stuxnet attack, where the sabotage of a nuclear facility was perpetrated by introducing a malicious computer worm via an infected USB flash drive.

A recent example of a targeted attack on the nuclear industry occurred in December 2014 on the Korea Hydro and Nuclear Power Company (KHNP), showcasing a hacker group's ability to introduce malware into a commercial network to gain sensitive information regarding the power plant schematics and vital personnel. [5] This example of data exfiltration highlights how a malicious attacker can gain access to sensitive information to later exploit the nuclear power plant control systems.

Similarly, other attacks could manipulate nuclear material accounting systems so that the theft of material goes unnoticed. In 1999, faulty software was provided to the Russian Kurchatov Institute for their nuclear materials accounting. The flaw led to the loss of material database records, which, if exploited, could have resulted in loss of nuclear material without anyone noticing.[6] While this incident was not a cyber attack, similar results could be achieved with one.

Government authorities and facility operators are struggling to keep pace with this new threat, and national and international guidance is still being developed. Given the increasing use of digital (and connected) systems, such challenges will only continue to grow.

NTI NUCLEAR SECURITY INDEX

Background

The NTI Index is a first-of-its-kind public assessment of nuclear security conditions on a country-by-country basis in 176 countries. Initially launched in 2012 and currently in its third edition, the NTI Index helps spark international discussions about priorities required to strengthen security and most important, encourages governments to provide assurances and take actions to reduce risks. Developed with the Economist Intelligence Unit (EIU) and with input from a respected international panel of nuclear security experts, the NTI Index draws on NTI's

[4] Unit 2 at Susquehanna Nuclear Power Plant Returns to Service, PR Newswire, 19 November 2012. Available at http://www.prnewswire.com/news-releases/unit-2-at-susquehanna-nuclear-power-plant-returns-to-service-180075671.html.

[5] J.M. Park and M. Cho, "South Korea blames North Korea for December hack on nuclear operator," Available at http://www.reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317.

[6] B. Blair, "Nukes: A Lesson from Russia," *The Washington Post*, 11 July 11 2001.

nuclear expertise, the EIU's experience in constructing indices, and the reach of the EIU's global network analysts and contributors.

Goals of the NTI Index

The 2016 NTI Index is the third edition of a country-by-country assessment of nuclear security conditions around the world, with three primary goals: (1) Catalyze a discussion on priorities for nuclear security by putting forward a framework of the most important aspects of nuclear security; (2) Promote action to strengthen security; and (3) Track progress on nuclear security over time to help identify areas for improvement.

NTI Index Framework

The NTI Index assesses nuclear materials security conditions in 24 countries with one kilogram or more of weapons-usable nuclear materials across a broad framework capturing policies, actions, and other conditions that shape their nuclear security. The framework is made up of five categories of indicators that are weighted to reflect their relative importance.[7] An additional 152 countries with less than one kilogram of weapons-usable nuclear materials or none at all are assessed across a subset of the framework.

The 2016 NTI Index also looks at a third set of countries in a new sabotage ranking. This assessment reviews the nuclear security conditions of 45 countries with respect to the protection of nuclear facilities against sabotage. Importantly, this new assessment provides a first-time look at the security conditions of countries with less than one kilogram of or no weapons-usable nuclear materials but that have one or more of the following facilities: operating nuclear power reactors or nuclear power reactors that have been shut down within the last five years; research reactors with a capacity of two megawatts or greater; reprocessing facilities; and spent fuel pools (only if the fuel has been discharged in the last five years and if not associated with an operating reactor).

Cybersecurity at Nuclear Facilities

Given the vulnerabilities of nuclear facilities and potentially serious consequences, cybersecurity at nuclear facilities has recently received greater attention by the international community, among national regulators and facility operators, and within the NSS process. In recognition of this evolving global threat, the NTI Index includes a cybersecurity indicator to provide a more complete picture of nuclear security around the world.

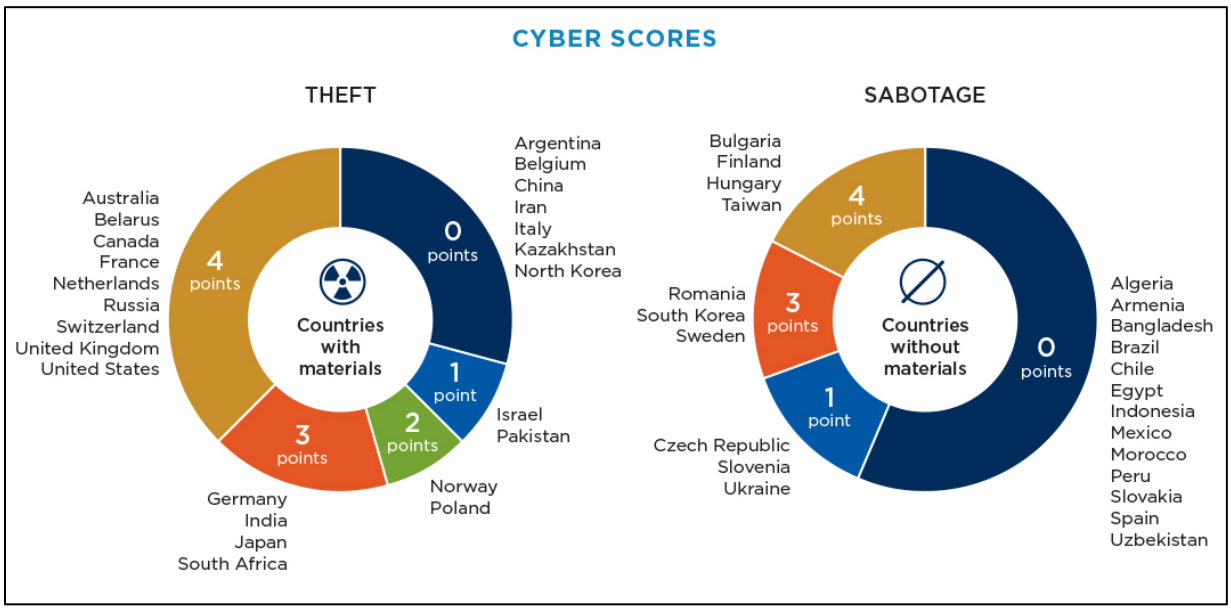
The cybersecurity indicator in the NTI Index includes a set of basic questions about a country's legal and regulatory requirements for securing nuclear facilities against cyber attacks, such as whether domestic laws require nuclear facilities to have protection from a cyber attack and if a country considers cyber threats in its threat assessment for nuclear facilities.[8]

---

[7] For further details on the NTI Index framework and methodology as well as all data collected, see the NTI Index website: www.ntiindex.org.

[8] The cybersecurity indicator asks the following four questions: Do domestic laws, regulations, or licensing requirements require nuclear facilities to have protection from a cyber attack? Do domestic laws, regulations, or licensing requirements require nuclear facilities to protect critical digital assets from a cyber attack? Does the state consider cyber threats in its threat assessment or design basis threat for nuclear facilities? Does the regulator require a performance-based program, which includes tests and assessments of cybersecurity at nuclear facilities?

The following chart shows the breakdown in cybersecurity scores for the 24 countries with materials in the theft ranking and the 23 countries without materials, but with nuclear facilities, in the sabotage ranking:



The 2016 NTI Index results show that of the 24 countries with weapons-usable nuclear materials, only 9 countries received a maximum score for the cybersecurity indicator while 7 countries scored 0.

Of the 23 countries that have nuclear facilities but with less than one kilogram of or no weapons-usable nuclear materials, the NTI Index revealed the following results:

- Only 4 countries received the maximum score for the cybersecurity indicator;
- Thirteen countries scored 0, including some that are considering expanding their use of nuclear power or beginning new programs; and
- Fifteen do not have even a basic requirement to protect nuclear facilities from a cyber attack.

The NTI Index 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 facilities are not prepared for the growing cyber threat. That reality is particularly worrisome, however, given that an attack on a nuclear facility anywhere could have global consequences.

NUCLEAR SECURITY SUMMITS

In 2010, President Obama initiated the first in a series of Nuclear Security Summits to focus high-level attention on the global threat posed by nuclear terrorism – it was the largest gathering of heads of government in nearly 50 years. At this Summit, and at the subsequent three,

participating countries made various commitments to strengthen nuclear security, but there is still no global system in place for tracking, accounting for, managing, and securing nuclear materials and facilities.

Although the Summits resulted in meaningful action to improve security and to enhance cooperation, it was not until the 2016 Summit that cybersecurity related to nuclear materials and facilities was addressed in a meaningful way. The 2012 and 2014 Summit communiqués briefly mention the growing threat of cyber attacks and possible risk mitigation measures, but the steps that governments have taken are not sufficient in the face of this evolving threat.

At the 2016 Summit, 28 countries and the United Nations committed to a Gift Basket on Cyber Security of Industrial Control and Plant Systems at Nuclear Facilities (also known as the Joint Statement on Cyber Security); all countries that signed up will attend two international workshops in 2016 aimed at sharing and improving the integrity of industrial controls at nuclear facilities. While previous efforts have sought to strengthen the security of data systems that contain sensitive nuclear information, this represents a milestone effort focused solely on cyber attacks with explicit physical implications. The workshops will focus on various topics such as cyber threats and vulnerabilities; technical and management challenges of managing cyber risks; and incident response and recovery, among others. Although this is a positive step, this Joint Statement on Cyber Security commits countries to only limited action aside from participating, as resources permit, in the international workshops.

Of the 28 countries that signed up to the Joint Statement on Cyber Security:

- Nine countries received the highest possible score for the NTI Index cybersecurity indicator.[9]
- Four countries received more than half the full score for this indicator.[10]
- Six countries are not evaluated in the theft ranking with materials or the sabotage ranking, showing positive engagement among countries that do not possess weapons-usable nuclear material or that have facilities.[11]

Unfortunately, six participating Summit countries without weapons or facilities (but who have planned or expressed an interest in nuclear power programs), did not sign on to the Joint Statement on Cyber Security.[12] There are also several notable omissions from this gift basket related to development of unique technical solutions as well as the need for a dedicated focus on information sharing. In addition, much of the language in the official gift basket statement only identifies the need for countries to ensure adequate cybersecurity measures at nuclear facilities, but does not clearly specify how to implement it. Thus, despite useful recognition of cybersecurity at the 2016 Summit, progress on protecting against a dynamic threat remains challenging and current government initiatives on cybersecurity leave much to be desired.

[9] Australia, Canada, Finland, France, Hungary, Netherlands, Switzerland, the United Kingdom, and the United States.
[10] Germany, Japan, Republic of Korea, and Sweden.
[11] Denmark, Georgia, Jordan, Philippines, Turkey, and the United Arab Emirates.
[12] Lithuania, Malaysia, Nigeria, Saudi Arabia, Thailand, and Vietnam.

NUCLEAR INDUSTRY SUMMIT

The 2016 Nuclear Industry Summit brought together hundreds of nuclear industry and policy experts from around the world to discuss the industry's global role in securing the nuclear materials and installations from theft and sabotage. Coordinated by the Nuclear Energy Institute, it was an official side event of the 2016 NSS.

The NIS participants issued a joint statement committing to, among other actions, improving the state of cybersecurity across all nuclear facilities and applications by: sharing best practices and information sharing; further developing technological approaches to cybersecurity; promoting peer reviews that include a cybersecurity module; and working to minimize vulnerabilities in the supply chain. This commitment brings the industry community one step closer to enhancing cyber-nuclear security.

The 2016 NIS also convened a working group to evaluate progress at the previous Nuclear Security and Industry Summits, and build upon this progress to develop a platform for the response to cyber threats and to develop comprehensive and integrated nuclear security programs. The outcomes of the working group include a set of 25 recommendations for industry, international organizations, governments, academia, research centers, and vendors, as well as a joint statement.

One of the greatest challenges of the final NIS was to establish a follow-on architecture for the international community to continue work on nuclear security in the absence of the Summit process. The NIS has struggled with the same issue of sustaining attention and momentum on the remaining challenges related to cybersecurity at nuclear facilities. A possible approach being considered is the establishment of a nuclear industry steering group focused on various aspects of nuclear security, though much work still needs to be done to demonstrate progress.

KEY CHALLENGES

Based on the NTI Index results, it is clear that several global challenges remain for combatting the cyber threat at nuclear facilities. Since a cyber attack against a nuclear facility could facilitate the theft of nuclear materials or an act of sabotage leading to a catastrophic radiation release, all countries must work aggressively to ensure that their nuclear facilities are protected from these type of attacks. Governments should include the cyber threat within the national threat assessment for their nuclear facilities, and should put in place a clear set of laws, regulations, standards, and licensing requirements for all nuclear facilities that require protection of digital systems from cyber attack. At the facility-level, leadership must prioritize cybersecurity, determine potential consequences, and implement a program that ensures that digital assets and networks are characterized and secured and that the security is routinely tested. This includes enforcing mechanisms to provide appropriate training and awareness to staff at nuclear facilities.

Countries planning new nuclear energy programs must first put in place the legal and regulatory frameworks necessary to ensure effective security of their nuclear facilities. Countries should take advantage of the International Atomic Energy Agency (IAEA) guidance on computer security at nuclear facilities as well as best practice documents developed by the World Institute

for Nuclear Security (WINS). Countries should also seek assistance from international partners and other countries with well-established nuclear programs before embarking on their own to ensure the secure operation of new nuclear facilities.

Due to the potential for blended cyber-physical attacks (whereby a cyber attack and a physical attack could together defeat physical security systems), cybersecurity and physical security programs and personnel should be integrated. Countries should assist nuclear facility operators with strengthening understanding of weaknesses and vulnerabilities related to the correlation of cyber-physical attacks. Similarly, security personnel and operators should receive appropriate training to understand the types of threats that exist (e.g., social engineering, phishing attacks, etc.) and how to better defend against them.

Further, recognizing the challenge of finding technically trained and competent cybersecurity personnel, countries should take advantage of existing institutions, such as the IAEA and WINS as well as other means to strengthen awareness and to develop the capacity necessary to protect and respond to cyber attacks. Protection of nuclear facilities from cyber attacks requires a diverse blend of technical skills (both operational technology- and information technology-related) that includes knowledge of a wide range of commercial and custom computer systems and digital controllers as well as the processes and equipment within the facility—a far more extensive skill set than is broadly recognized or available at many facilities. Therefore, consideration should be given to the development of alternative means of filling gaps in national capacities.

Finally, although the Nuclear Security Summits and Nuclear Industry Summits have contributed greatly to security improvements and awareness, many commitments have yet to be fulfilled, including important pledges related to ensuring adequate cybersecurity at nuclear facilities to prevent theft of materials or sabotage. Since the Summit process has now concluded, governments should recommit to delivering on their Summit commitments and provide information on their progress. The nuclear industry should focus attention on sustaining momentum from the Summit process and following through on the commitments made through the NIS joint statement as well as the 25 recommendations from the working group. Establishing a steering group to deal with these issues would be a good start.

CONCLUSION

As previously discussed, much more needs to be done by governments and the private sector to effectively secure nuclear facilities from cyber attack and prevent the theft of nuclear materials or sabotage of facilities. As the sophistication of attacks against nuclear facilities continues to grow, the required response and preventative measures to protect these facilities will need to mature accordingly. The 2016 NTI Index results provide countries with areas for improvement and where attention should be focused to keep nuclear materials and facilities safe from theft and sabotage.

Though the NSS and NIS processes played an important role in highlighting the threat and providing support for—and accelerating—national efforts to secure nuclear materials, more must be done to improve cybersecurity at nuclear facilities. Countries must explore methods to

continue advancing the dialogue on securing nuclear materials and facilities from cyber attack beyond 2016.

ABOUT THE AUTHORS

Michelle Nalabandian joined the Nuclear Threat Initiative (NTI) in 2009 and serves as program officer for the Scientific and Technical Affairs program. In this role, she manages operational elements of the program and conducts research and analysis that focuses on the security of nuclear and radiological materials globally, cybersecurity for nuclear facilities, and biosecurity threats. Prior to joining NTI, Nalabandian worked in the financial sector for asset management firms Global Environment Fund and Sciens Capital Management. Nalabandian holds a bachelor's degree in biology from George Mason University and received a certificate of mastery from the John F. Kennedy School of Government at Harvard University. She was a 2015 PONI Nuclear Scholar and a 2015 Fellow of the Emerging Leaders in Biosecurity Initiative (ELBI). She is also a member of Women in International Security (WIIS) and the Institute of Nuclear Materials Management (INMM).

Alexandra Van Dine is a program associate with the Scientific and Technical Affairs program at the Nuclear Threat Initiative, where she works on the NTI Nuclear Security Index and cybersecurity-related projects. She has presented research on cybersecurity at nuclear facilities at U.S. Strategic Command and Los Alamos National Laboratory. Ms. Van Dine is a member of the Center for Strategic and International Studies Project on Nuclear Issues Nuclear Scholars Initiative Class of 2016. She is a graduate of 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 at Georgetown and earned honors on her thesis, which explored why individuals choose to proliferate.

Page Stoutland is NTI's vice president for Scientific and Technical Affairs, where he is responsible for NTI's scientific and technically related projects designed to strengthen nuclear security around the world, including the NTI Nuclear Security Index, strengthening technical cooperation with China and cybersecurity at nuclear facilities. Prior to joining NTI, Stoutland held a number of 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. Stoutland holds a bachelor's degree from St. Olaf College in Northfield, Minnesota and a doctorate in chemistry from the University of California, Berkeley.

ABOUT THE NUCLEAR THREAT INITIATIVE

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.