BUILDING A SAFER WORLD

Transformative Guiding Principles for Implementing Cybersecurity at Nuclear Facilities

Alexandra Van Dine[1], Michael Assante[2], Page Stoutland[3]

Abstract

Ensuring the security of nuclear facilities is a critical element in preventing theft of nuclear materials or sabotage that could result in a radiological release. While the international community has traditionally focused on improving physical security to prevent these outcomes by investing in the “guns, guards, and gates” trifecta, a newer threat has gained attention: the cyber threat. A cyber attack on a nuclear facility could have physical consequences leading to either an act of theft or sabotage—presenting new challenges to facility operators as well as national authorities. Given the increasing use of digital devices and communications for controls, safety, physical security, and supporting functions, it is expected that these challenges will only continue to grow. As the cyber threat becomes more pronounced, these challenges could undermine global confidence in nuclear energy as a safe and reliable resource.

The growing sophistication of cyber threats increasingly taxes the capabilities of governments, national regulators, and facility operators around the world, and necessary progress in this area requires a fresh look at the overarching framework that guides cybersecurity implementation at nuclear facilities. The current approach is one of incremental change that ultimately leads to insufficient security because it can neither keep pace with the threat nor address the ever-widening gap between attackers and defenders. A more effective approach, based on a set of high-level guiding principles, is critical to mitigating the risks associated with our reliance on digital technology. Over the last year, NTI has convened a diverse group of experts to develop a set of ambitious, forward-looking principles to guide cybersecurity at nuclear facilities. This paper will discuss the cyber threat to nuclear facilities, why the current approach is insufficient, and some broad suggestions and questions to consider as the international community moves forward in this area.

[1] 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. She is a graduate of Georgetown University’s Walsh School of Foreign Service.

[2] 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. Mr. Assante 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.

[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 (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.

Introduction

At nuclear facilities, digital technologies are a double-edged sword. On the one hand, they unlock important benefits that improve safety and streamline processes. On the other hand, they increase a facility's vulnerability to cyber attacks with serious consequences. For example, a cyber attack could compromise surveillance systems and alarms to allow a thief to enter a facility, steal weapons-usable nuclear material, and escape, undetected. Or, an adversary could shut down cooling or heating systems with a cyber attack, facilitating an act of sabotage with consequences that, in a worst-case scenario, could rise to the level of those experienced at Fukushima in 2011. A cyber attack that results in the theft of dangerous nuclear materials or sabotage resulting in radiological release would have consequences that reverberate around the world and could seriously harm global confidence in nuclear energy as a safe and reliable resource.

This threat exists in a troubling context; not only are countries around the world unprepared to meet this threat, but traditional methods of cyber defense, such as firewalls, antivirus, and airgaps, have been demonstrated to be fallible. Furthermore, the capabilities that are restricted to states today will not necessarily stay that way in the future; in the words of renowned cryptographer Bruce Schneier, "Today's NSA secrets become tomorrow's PhD theses and the next day's hacker tools."[4] The increasing ease with which non-state actors can access dangerous tools combined with the widespread use of inherently vulnerable digital systems in the operation and security of nuclear facilities amid a global lack of preparedness and expertise in this area present a significant security challenge at nuclear facilities worldwide. National authorities now face the difficult task of mitigating this threat.

The Threat

A cyber attack against a nuclear facility has the potential to manipulate digital systems vital to ensuring the safety and security of nuclear facilities and materials. These include everything from access control systems to materials accounting systems to vital safety systems, such as those that control cooling. Compromising these systems via cyber attack could facilitate the theft of nuclear materials or the sabotage of a facility resulting in a radiological release.

The conventional approach to manage these risks has been prevention-focused—that is, using tools like airgaps, unidirectional information flows, and physical segmentation technologies to prevent outsiders from accessing critical networks. These precautions, while generally effective against non-targeted attacks that simply leverage existing technological vulnerabilities, are simply insufficient to protect against newer, target-focused attacks and threats.[5] The attacks facilities face today tend to rely upon more enduring vulnerabilities such as human behaviors and practices, and sometimes include the development of custom exploits. More concerning, they have a proven track record when it comes to compromising conventional cybersecurity defenses.

[4] Bruce Schneier, "Cyberweapons Have No Allegiance." https://www.schneier.com/essays/archives/2015/02/cyberweapons_have_no.html.

[5] 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/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.

This is a global problem—nuclear materials stolen abroad through a cyber-facilitated operation could be used in an attack anywhere in the world, and a cyber-facilitated act of sabotage would have global consequences for the future of nuclear energy. Either of these events would profoundly shake global confidence in nuclear power as a viable energy source, undoing years of good work in the scientific community and nuclear industry.

Regulatory agencies and facility operators are struggling to understand the threat, and this is evidenced by a global lack of preparedness in this area. For example, the NTI Nuclear Security Index, a ranking of countries according to their nuclear security conditions, found that[6]:

- Out of 47 countries with weapons-usable nuclear materials or high-consequence nuclear facilities, 20 did not require that nuclear facilities be protected from cyber attack.
- Of 24 countries with weapons-usable nuclear materials, 9 received a maximum score on the cybersecurity indicator and 7 received a score of 0.
- Of 23 countries with high-consequences nuclear facilities but no weapons-usable nuclear materials, 4 received a maximum score while 13 scored 0—including some countries expanding the use of nuclear power.

The data revealed that although some countries have been taking steps to protect nuclear facilities from cyber attack, many do not yet have the laws and regulations needed to provide effective cybersecurity. Furthermore, the actions that *are* taken at the regulatory and operator level often fail to address root vulnerabilities.

The challenge of ensuring effective cybersecurity at nuclear facilities is exacerbated by a shortage of technical expertise in the cyber-nuclear space. The experts that do exist tend to be concentrated in North America, Europe, and Russia, leaving other countries—especially those new to nuclear—without the necessary expertise to develop and implement the measures necessary to secure their facilities.

Nuclear facilities have already fallen victim to a variety of non-targeted cyber attacks that exploit widespread technological vulnerabilities. If existing security measures and practices are insufficient to prevent these basic attacks, it is unlikely that they will be able to stand up to the kind of targeted, well-resourced cyber attack that could cause significant physical consequences at a nuclear facility

The Current Strategy

The current strategy for addressing the cyber threat to nuclear facilities is oriented toward attacks leveraging widespread technological vulnerabilities, and fails to account for targeted attacks carried out by well-resourced, determined adversaries. When it comes to attacks like these, the current approach is too incremental to be truly effective.

Although some countries have started to take the steps necessary for better security, the world writ large is largely unprepared. Most facilities rely upon traditional cybersecurity tools such as firewalls, antivirus, and airgaps for security—tools that have been defeated or circumvented in the past by determined adversaries. More concerning, as these security measures fail in the face of a new threat, the implementation of digital technologies across the nuclear enterprise increases the potential

[6] For more information about the NTI Nuclear Security Index, please visit www.ntiindex.org

vulnerabilities. While traditional cybersecurity approaches may be adequate for individual home computers, they are simply not sufficient for high-consequence systems like those found in nuclear power plants and fuel cycle facilities.

A new strategy that moves beyond the current approach is needed in order to address the dynamic and evolving cyber threat to nuclear facilities and prevent an incident that could shake collective confidence in the safety of the nuclear industry.

Developing Guiding Principles

Over the past two years, the Nuclear Threat Initiative undertook research and hosted expert discussions on the cyber threat to nuclear facilities. During this time, it became apparent that a fresh, unconstrained look at cybersecurity at nuclear facilities is required to keep pace with this dynamic threat.

Recognizing that any transformative principles must be grounded in strong technical understanding, NTI gathered a small group of technical experts to achieve several goals. The first was to develop a common understanding of the threat. The second was to discuss the state of the current approach to the threat. The third was to agree, at a very high level, on the broad strokes of a few possible solutions.

Next Steps

Currently, NTI is working to refine a set of principles to serve as the basis for a report to be released in autumn of 2016. The expert group is examining several key questions, including:

- What lessons can be drawn from the experience of fully integrating safety-related concerns into the regulation and operation of nuclear facilities for the cyber case? How could such lessons be applied and ultimately implemented?
- Should the most critical systems at nuclear facilities be either kept in or reverted to a non-programmable state—making them impenetrable? What measures can be taken overall to reduce complexity (and, hence, vulnerabilities) at nuclear facilities?
- Given that experience suggests that full prevention of all cyber attacks is impossible, should facilities undertake a new defense strategy that defends against attacks instead of relying solely on tools like airgaps and firewalls? What could this look like?
- How can this community avoid playing catch-up in the future? What research, innovation, and other intellectual investments must be made to change how the world thinks about this problem?

Conclusion

Today, nuclear facilities around the world face the threat of a targeted cyber attack perpetrated by a determined, well-resourced adversary that could very well have serious physical consequences. These consequences could include the theft of weapons-usable nuclear materials or an act of sabotage that results in radiological release and serious off-site health consequences. The current strategy for cybersecurity was created to meet a different threat—that of technology- or vulnerability-based cyber exploitation. A new challenge requires a new strategy, but regulators and operators around the world have not yet been able to adapt to this dynamic and evolving threat.

Efforts to improve cybersecurity at nuclear facilities are hampered by a lack of qualified personnel, resources, and understanding. Global expertise in this area is short, and the list of challenges is long. Progress will be no easy task, but the stakes are too high to simply maintain the status quo.

In order to overcome these obstacles and prevent a cyber attack on a nuclear facility with catastrophic consequences, NTI, supported by a small working group of technical experts, is re-thinking the current approach and developing a new, forward-looking strategy. A transformational threat merits a transformational response—incremental change, while a necessary component of a larger strategy, is no longer sufficient on its own.

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 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.

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. Mr. Assante 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 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.