ENHANCING GLOBAL CYBERSECURITY CAPACITY AT NUCLEAR FACILITIES
The Cyber-Nuclear Forum

P.O. STOUTLAND
Nuclear Threat Initiative
Washington, D.C., United States
Email: stoutland@nti.org

E.D. DUMBACHER
Nuclear Threat Initiative
Washington, D.C., United States
Email: dumbacher@nti.org

M.N. MILLER
Nuclear Threat Initiative
Washington, D.C., United States

Abstract

Working with nuclear industry cyber security experts, the Nuclear Threat Initiative has developed the Cyber-Nuclear Forum to strengthen protection of civilian nuclear facilities from cyber-attacks. A successful cyber-attack on a nuclear facility could have serious consequences with global ramifications for human health and safety and the industry. The Forum seeks to support the cyber-nuclear experts working to defend their facilities against the expanding threat.

The Forum provides a venue for dialogue, information exchange, cooperation and problem solving among an international group of operational and technical experts addressing cyber threats at nuclear facilities. The Forum aims to: (a) enhance global cyber security practices and create an international network of experts by enabling engagement among experienced cybersecurity leaders at nuclear research and energy facilities; (b) accelerate and amplify the capabilities of the limited number of skilled, trained cyber-nuclear operators in nuclear facilities, particularly in countries without mature nuclear research or energy programs; and (c) establish an industry-led, self-sustaining vehicle that helps facilities get ahead and stay ahead of constantly evolving cyber-nuclear threats. The paper will discuss the Forum concept and successes to date.

1. INTRODUCTION

Working with nuclear industry cyber security experts, the Nuclear Threat Initiative (NTI) has developed the Cyber-Nuclear Forum to strengthen protection of civilian nuclear facilities from cyber-attacks. Nuclear energy and research facilities, including the sensitive digital systems used for nuclear security and safety, are not immune from cyber-attack. Compromise of a facility's business networks could lead to the loss of sensitive business information, as well as security-sensitive information that could enable future attacks, including sabotage. Compromise of digital control systems could directly affect the safety of a nuclear facility. 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 global demand for such experts, all countries—but particularly countries with emerging nuclear programs that lack the hands-on knowledge gained through operating experience—are struggling to attract the technical talent needed. Even in countries with established nuclear programs, some utilities employ a limited number of experts dedicated to cybersecurity. Given the intense competition for experts, inadequate technical capacity will be an enduring issue and one of the fundamental challenges for the global nuclear industry. To address this issue, the Cyber-Nuclear Forum seeks to promote greater international cooperation by engaging and building a network of cybersecurity experts from operational nuclear facilities. The Forum offers a necessary platform for global nuclear industry experts to cooperate and collectively strengthen defences against cyber threats.

The Cyber-Nuclear Forum has been designed to:

— Enhance global cyber security practices and create an international network of experts by engaging experienced cybersecurity leaders at nuclear research and energy facilities;
— Accelerate and amplify the capabilities of the limited number of skilled, trained cyber-nuclear operators in nuclear facilities, particularly in countries without mature nuclear research or energy programs;
— Establish an industry-led, self-sustaining vehicle that helps facilities get ahead and stay ahead of constantly evolving cyber-nuclear threats.

A private venue for dialogue, information exchange, cooperation, and problem solving, the Cyber-Nuclear Forum gathers international operational and technical experts who can address the shared challenges posed by cyber-attacks and collectively strengthen defences against cyber threats.

2. BUILDING CYBERSECURITY CAPACITY GLOBALLY

Global capacity to mitigate the cyber risk to nuclear facilities is uneven, and nuclear power plants in all countries remain potentially vulnerable to attacks that could compromise sensitive information or affect control systems. This situation is exacerbated by the global shortage of cybersecurity experts, particularly in the nuclear industry. The Cyber-Nuclear Forum seeks to build global capacity to address cyber threats at nuclear facilities by bringing together cybersecurity experts from operational nuclear facilities.

2.1. Nuclear facilities are vulnerable to cyber-attacks

Commercial nuclear power plants are vulnerable to cyber threats that could result in theft of nuclear materials or sabotage. Terrorist groups, nation-states, ransomware hackers, and “hacktivists” could all target nuclear facilities with cyber-attacks for political or financial purposes. Cyber espionage could compromise sensitive information and pose a proliferation risk. Nuclear data at nuclear energy and research facilities have been targeted in past cyber-attacks. A successful cyber-attack could even impact critical control systems and pose a risk to nuclear security and safety, with a worst-case scenario resulting in the release of radioactive or nuclear material. For instance, access control systems or accounting systems could be compromised to facilitate unauthorized access to a facility or theft of nuclear materials. In all cases, insider threats remain one of the most plausible risk scenarios for nuclear power plants—and one of the most difficult to mitigate [1].

Efforts to address cyber vulnerabilities at nuclear facilities have been uneven and, at times, ineffective. Physically separating critical systems from the internet and unsecure networks – air-gapping – does not guarantee security, notably demonstrated in the Stuxnet cyber-attack on the Iranian nuclear program [1]. Globally, national capacity varies. In NTI’s 2018 edition of its Nuclear Security Index, one-third of countries with weapons-usable nuclear materials or nuclear facilities still lacked all basic cybersecurity regulations [2]. Two-thirds of countries and Taiwan lacked a cyber-incident response plan, indicating that most countries have not prepared for inevitable failures in existing cybersecurity measures [2].

Recent incidents (see Table 1) demonstrate the urgency of addressing the cyber threat to nuclear power plants. For instance, multiple nuclear facilities have experienced recent accidental incidents due to employees connecting secure systems to the internet to mine cryptocurrency. (For a list of cyber incidents at nuclear facilities from 1990 to 2016, see Appendix in [1]).

TABLE 1. COMPUTER INCIDENTS AT NUCLEAR FACILITIES SINCE 2017

Year	Name	Location	Brief description	Category
2017*	Wolf Creek Nuclear Generating Station	Kansas, U.S.	Hackers compromised business systems of power plant [3]	Intentional
2017	Chernobyl radiation monitors	Ukraine	Petya ransomware attack affected monitors [4]	Unknown
2018	Russian Federal Nuclear Center	Sarov, Russia	Employees mining cryptocurrency with supercomputer connected to internet [5]	Accidental
2019*	Cooper Nuclear Station	Nebraska, U.S.	Conflicting reports that the power plant communications systems were compromised [6, 7]	Unknown

2019	Yuzhoukrainsk Nuclear Power Plant	Ukraine	Plant employees connected computer networks to internet for bitcoin mining [8]	Accidental
2019	Kudankulam Nuclear Power Plant	India	Malware detected in administrative systems [9]	Unknown

***** indicates year discovered/leaked

The frequency of reported computer incidents at nuclear facilities (see Fig. 1) is , increasing. Both state and non-state actors have infiltrated secure systems, and accidental breaches could still have serious consequences. A number of incidents at nuclear power plants remain uncertain in nature, as attributing cyber-attacks is notoriously difficult. Moreover, information about attacks is often disputed [6, 7] or becomes public long after the fact.

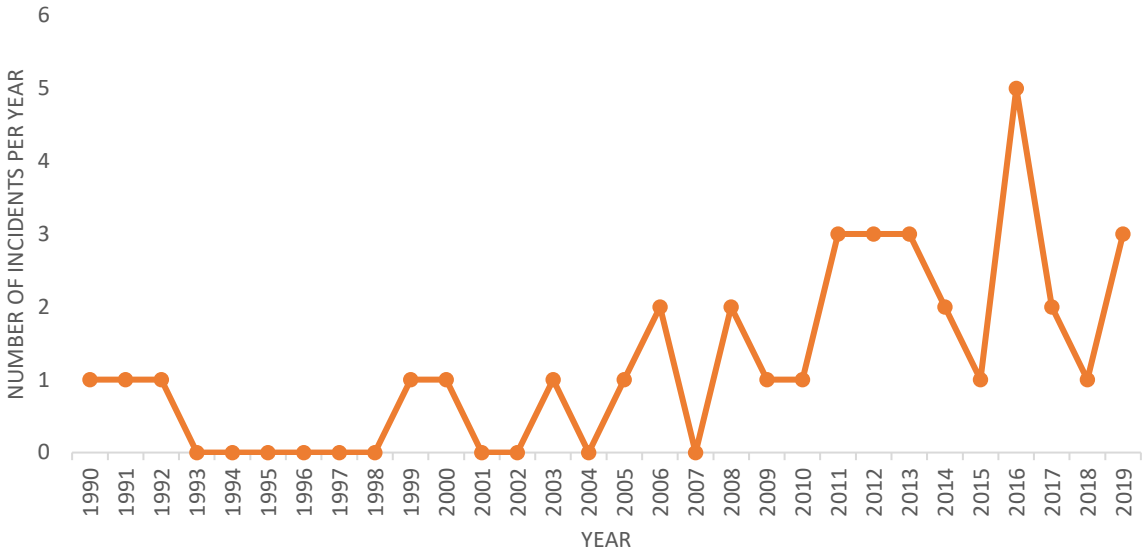

FIG. 1. Publicly disclosed cyber incidents at nuclear facilities since 1990. Incidents are classified for the year they occurred or were publicly disclosed.

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

2.2. Nuclear facilities struggle to attract technical talent

The Cyber-Nuclear Forum is addressing the critical capability deficits that exist globally. There are not enough highly trained experts with the unique knowledge of both industrial cybersecurity and nuclear facilities. Moreover, this challenge is exacerbated by the low profit margin of many nuclear power plants compared to industries like finance that can devote more resources to hiring and training cybersecurity staff. Together, the limited resources and experts dedicated solely to the cyber-nuclear threat make it more likely that attacks could be successful.

The nuclear industry is not unique in dealing with labor and staffing challenges, as the information security workforce overall lacks enough well-trained employees. Cisco reported in 2015 that one million security jobs were empty, and there remains a “stubbornly stagnant” low proportion of women in information security that compounds existing workforce challenges [10]. Salaries are rising across both developed and developing countries for cyber experts due to information security professional scarcity [11]. Suby and Dickson explain that the increase in pay “can be explained by basic economics. The demand for security professionals is growing, but the supply of security professionals is not growing at the same rate. The result is growing salaries” [11].

Multiple studies have documented the same shift from budget constraints to a talent gap that prevents the employment of a sufficient number of security experts. In 2013, survey respondents in the information security field identified business conditions and funding as the limiting factor in hiring enough personnel, yet in 2015 respondents increasingly said "it is difficult to find the qualified personnel we require" [11]. A 2018 Cisco survey similarly found that budget constraints and compatibility issues with legacy systems have decreased as obstacles to security each year from 2015 to 2017, while lack of trained personnel has grown as a limiting factor [12]. In 2018, more than half of surveyed industrial control system professionals said that "hiring ICS cybersecurity employees with the right skills" is "a major challenge," and another third said it was a minor challenge [13].

The nuclear industry faces particular challenges recruiting the necessary cyber talent. Companies operating commercial nuclear power plants typically have narrow profit margins, which limits their ability to compete for top talent and hire adequate teams. A 2018 Union of Concerned Scientists report found that "More than one-third of existing plants, representing 22 percent of total US nuclear capacity, are unprofitable or scheduled to close" [14]. The report found that in the United States, "On average, projected operating costs exceed revenues between 2018 and 2022 for 16 nuclear plants in addition to five plants scheduled for retirement" [14]. In a worst-case scenario, organizations may accept higher risk or deficient security postures due to the higher wages for security talent and lack of qualified professionals available [11].

This threat extends to the regulation and oversight of the nuclear industry as well. The Nuclear Regulatory Commission (NRC) conducted a 2019 audit of U.S. nuclear power plants and found that the inspection program for cybersecurity at plants "faces future staffing challenges, because demographic and resource constraints work against optimal staffing. If this is not addressed, challenges in maintaining cyber security expertise among the inspectors could hinder NRC's ability to manage cyber security risk" [15]. Challenges staffing cyber experts identified by the NRC are likely to extend to regulatory organizations in other countries and multilateral bodies and could make addressing the cyber-nuclear threat even more difficult.

2.3. The Forum enhances global cyber-nuclear capacity

Cyber experts at nuclear facilities may not have access to training and advancement opportunities specific to their field. Forums that address nuclear security rarely provide in-depth training about cybersecurity, while cybersecurity training even in industrial control fields is unlikely to address the specific conditions of operational nuclear power plants. Moreover, academic or military research addressing these threats may not incorporate operators at commercial plants—particularly those in developing countries. The Cyber-Nuclear Forum provides a venue for sharing of best practices among participants in bi-annual meetings.

Further, professionals in information security identify a range of 'soft' skills as critical for success in their field, including communication skills, leadership skills, and a broad understanding of the security field [11]. Creating opportunities for cyber-nuclear professionals to network, and to discuss specific problems in their field will strengthen cybersecurity at facilities around the world. The Forum has already demonstrated that participants desire to be involved in subsequent meetings and often refer colleagues or request to bring other professionals they believe would benefit and contribute.

3. CYBER-NUCLEAR FORUM EVENTS

The Cyber-Nuclear Forum brings together cyber-nuclear leaders to share experiences and practices to strengthen cybersecurity at nuclear facilities. Meetings are by invitation only, with up to forty attendees, to provide an environment for substantive engagement. Specifically, the Forum is:

(a) Facilitating the sharing of best practices. The Forum brings together experts from industry-leading organizations, as well as new or small nuclear facilities. Participants include chief information security officers, lead computer security engineers, cyber-nuclear security managers, and others who can share best practices and lay the groundwork for a global cyber-nuclear expert network.
(b) Creating a self-sustaining entity. In partnership with the nuclear industry, international organizations, and industry groups, the Forum is working to develop the appropriate partnerships and funding sources for ongoing Forum support.

(c) Guided by a steering group. NTI has created a Forum steering group to guide the overall effort, including its sustainability, drawing members from key nuclear companies from around the world.

Agenda topics include developing risk frameworks, embedding cybersecurity into organizational culture, recruiting and retaining talent, and the identification of technical subgroups.

3.1. Cyber-Nuclear Forum meeting in Paris, France

In July 2018, 31 experts gathered in Paris, France for the first meeting of the Cyber-Nuclear Forum. Twelve countries were represented: United States, United Kingdom, Ukraine, Republic of Korea, South Africa, Russia, Netherlands, Germany, France, Finland, Canada, and Belarus, plus Taiwan. Overall, participants said described the meeting as "a great first forum to build trust amongst the group" and said the Forum was an "excellent collaborative initiative to develop best practices against the cyber threat."

After the meeting, participants highlighted three key topics to discuss at the next Forum event:

(a) Supply chain management – identifying potential risks in product suppliers and methods to mitigate the threat introduced to plant operations;
(b) Risk quantification – discussing methods to systematically analyze potential threats to nuclear facilities;
(c) Education and training for cyber-nuclear skills – sharing best practices to develop the highly specialized skill set necessary for cyber experts working at operational nuclear facilities.

3.2. Cyber-Nuclear Forum meeting in Krems, Austria

From February 8 – 11, 2020, NTI convened the second meeting of the Cyber-Nuclear Forum in Krems, Austria. Many of the participants from the Paris meeting returned to participate in the second Forum meeting, indicating their level of commitment and interest in the Forum's work.

In addition, the Forum was expanded from approximately thirty participants to around forty professionals. Fourteen countries were represented: the twelve countries and Taiwan from the July 2018 meeting, with the addition of Argentina and Brazil. This controlled expansion is intended to facilitate the involvement of new experts and expansion of the cyber-nuclear expert network. As previously identified, the capacity gaps in cyber-nuclear expertise worldwide are wide-reaching and systematic, so greater involvement with new experts will only help address this deficit. Still, meetings remain a manageable small size to permit the conversations and trust building that make the Forum so successful.

3.3. Sustainability of the Cyber-Nuclear Forum

Ensuring the sustainability of the Forum is necessary as the Forum goals will take some time to achieve. To date, we have been fortunate to have the financial support from several nuclear utilities, as well as the UK government. Looking forward, we plan to broaden the financial support base and to ensure appropriate organizational support.

4. DISCUSSION AND CONCLUSION

Nuclear facilities, including commercial power plants and research centers, are potentially vulnerable to cyber-attacks and espionage from terrorist groups, nation-states, ransomware hackers, and "hacktivists." This threat is compounded by an international shortage of cyber talent, particularly professionals working in the nuclear industry. The Cyber-Nuclear Forum will not fill all the gaps in global cyber-nuclear professional capacity, and states should take additional steps on their own to enhance training and career advancement (see [2]). However, the Forum is providing a venue for experts who may otherwise have limited opportunity to compare experiences with other professionals in their narrow field.

Thus far, the Cyber-Nuclear Forum has convened two meetings: July 2019 in Paris, France and February 2020 in Krems, Austria. These meetings saw the initiation of the exchanging of best practices and trust building amongst participants. Initial Forum meetings have also slowly expanded the group to a manageable forty

participants to facilitate greater engagement at the same time as preserving small-group dynamics. In addition to the bi-annual meetings, working group discussions take place between meetings. We anticipate that the next major meeting will take place in summer 2020.

ACKNOWLEDGEMENTS

We are appreciative of support from NTI, the U.K. Foreign and Commonwealth Office, Bruce Power, Exelon and URENCO.

REFERENCES

[1] VAN DINE, A., ASSANTE, M., STOUTLAND, P., Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, Washington, D.C. (2016), https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf.

[2] STOUTLAND, P., DUMBACHER, E.D., NTI Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action, Nuclear Threat Initiative, Fourth Ed., Washington, D.C. (2018), https://ntiindex.org/wp-content/uploads/2018/08/NTI_2018-Index_FINAL.pdf.

[3] PERLROTH, N., Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say, The New York Times (2017), https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?module=inline.

[4] PERLROTH, N., SCOTT, M., FRENKEL, S., Cyberattack Hits Ukraine Then Spreads Internationally, The New York Times (2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?_r=0.

[5] Russian nuclear scientists arrested for 'Bitcoin mining plot,' BBC News (2018), https://www.bbc.com/news/world-europe-43003740.

[6] SANGER, D.E., PERLROTH, N., U.S. Escalates Online Attacks on Russia's Power Grid, The New York Times (2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[7] DUNKER, C., Cooper Nuclear Station not breached by cyberattack, NPPD says, Lincoln Journal Star (2019), https://journalstar.com/news/state-and-regional/federal-politics/cooper-nuclear-station-not-breached-by-cyberattack-nppd-says/article_fbf53273-2641-57fc-9b21-e1f66ba31afa.html.

[8] SBU busts cryptocurrency miners at Ukrainian power plant, UNIAN (2019), https://www.unian.info/economics/10658847-sbu-busts-cryptocurrency-miners-at-ukrainian-power-plant.html.

[9] Nuclear Power Corp of India says detected malware in its systems, Reuters (2019), https://www.reuters.com/article/india-npcil-malware/nuclear-power-corp-of-india-says-detected-malware-in-its-systems-idUSL3N27F356

[10] SUBY, M., Women in Security: Wisely Positioned for the Future of InfoSec, Frost & Sullivan, San Antonio, TX (2015), https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-Women-In-Security-Study-2015.ashx?la=en&hash=B98F4ADE5EC87BA7B144AF1334388573D49505A8.

[11] SUBY, M., DICKSON, F., The 2015 $(ISC)^2$ Global Information Security Workforce Study, Frost & Sullivan, San Antonio, TX (2015), https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2015.ashx?la=en&hash=01D5BD45477FB7B45EF773366CF7D1D9BB6A6753.

[12] Cisco 2018 Annual Cybersecurity Report, Cisco Systems Inc., (2018), https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

[13] SCHWAB, W., POUJOL, M., The State of Industrial Cybersecurity 2018, Kaspersky Lab, Moscow, and CXP Group Co., Munich (2018), https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf.

[14] CLEMMER, S., RICHARDSON, J., SATTLER, S., LOCHBAUM, D., The Nuclear Power Dilemma: Declining Profits, Plant Closures, and the Threat of Rising Carbon Emissions, Union of Concerned Scientists, Cambridge, MA (2018), https://www.ucsusa.org/sites/default/files/attach/2018/11/Nuclear-Power-Dilemma-full-report.pdf.

[15] BAKER, B.A., Audit of NRC's Cyber Security Inspections at Nuclear Power Plants, Rep. OIG-19-A-13, Office of the Inspector General, U.S. Nuclear Regulatory Commission Defense Nuclear Facilities Safety Board, Washington, D.C. (2019), https://www.nrc.gov/docs/ML1915/ML19155A317.pdf.