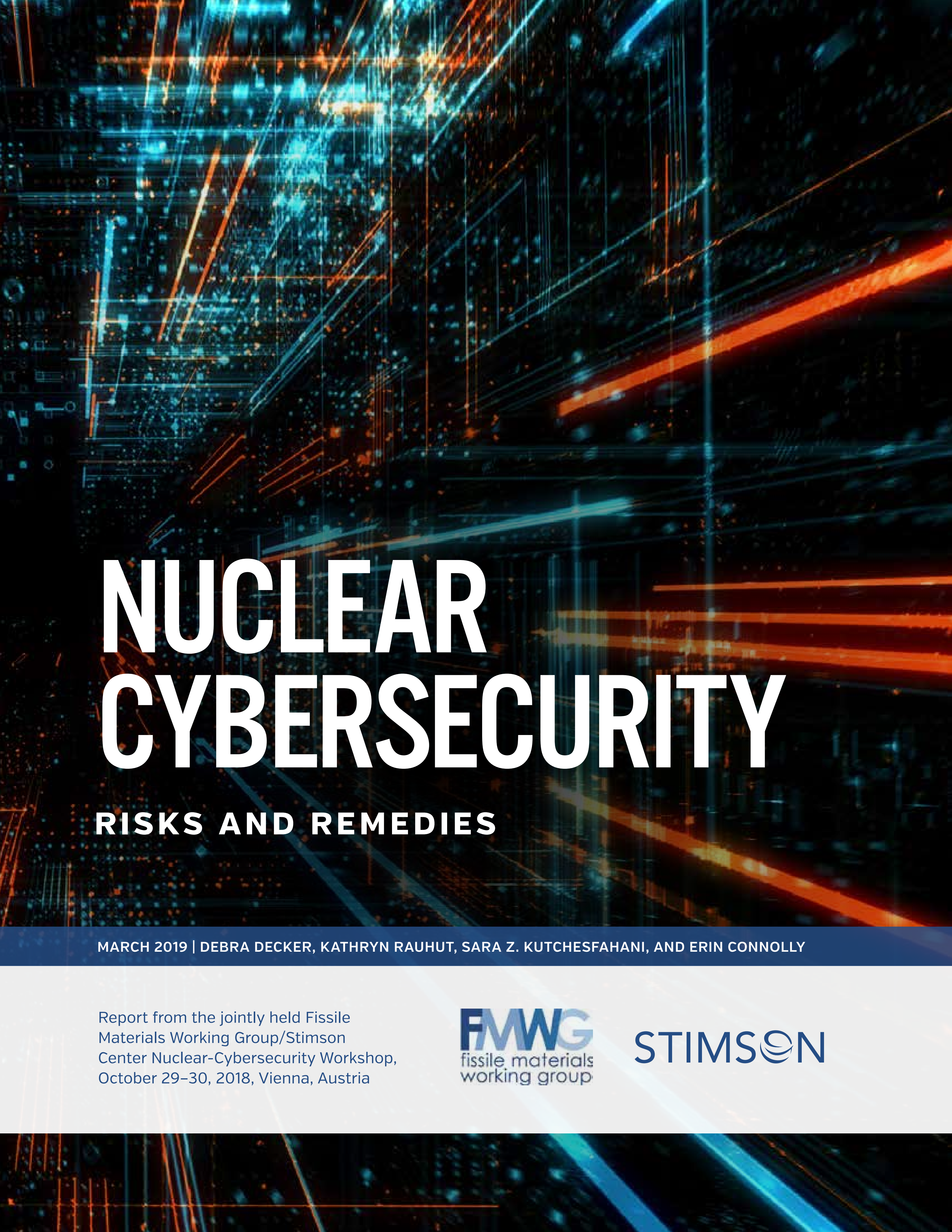


NUCLEAR CYBERSECURITY

RISKS AND REMEDIES

MARCH 2019 | DEBRA DECKER, KATHRYN RAUHUT, SARA Z. KUTCHESFAHANI, AND ERIN CONNOLLY

Report from the jointly held Fissile Materials Working Group/Stimson Center Nuclear-Cybersecurity Workshop, October 29–30, 2018, Vienna, Austria

FMWG
fissile materials working group

STIMSON

ACKNOWLEDGEMENTS

The authors would like to thank all the workshop participants for donating their time and expertise and for sharing their opinions over the course of 1.5 days in Vienna, Austria. In particular, the authors would like to thank those who took the time to make important – and, in many cases, extensive – comments on the workshop report.

The Fissile Materials Working Group is also grateful for the partnership with the Stimson Center in providing significant assistance in organizing the roundtable and producing this workshop report.

The authors would also like to thank Laura Rockwood, Executive Director of the Vienna Center for Disarmament and Non-Proliferation, for hosting the meeting, and Miles A. Pomper, who developed the concept for this workshop and supported the effort.

The Fissile Materials Working Group (FMWG) wishes to thank the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation for their continuing support of the FMWG and for allowing us to undertake this important effort.

Graphic Design by Christy Batta

ABOUT THE AUTHORS

DEBRA DECKER is a Senior Advisor at the Stimson Center. She has more than 20 years of experience in strategic planning in the private and public sectors and is a subject matter expert in the field of risk management. She has advised the Federal Bureau of Investigation, the US Department of Defense and the US Department of Homeland Security on strategy and risk and has specialized in the threats stemming from weapons of mass destruction and in the vulnerabilities of critical infrastructure. As a researcher, her work includes studies on nuclear security, nuclear forensics and attribution, national interests and public preparedness, and management of cybersecurity. Decker was previously an associate of Harvard University's Belfer Center for Science and International Affairs. Her research has been featured at the World Economic Forum and to Congress. She holds an MBA from the Wharton School of the University of Pennsylvania, an MPA from the Kennedy School of Government at Harvard University, and a BA from American University.

KATHRYN RAUHUT is a Nonresident Fellow at the Stimson Center and an attorney specializing in international security based in Vienna, Austria. She works primarily on nuclear security governance, accountability, and liability issues with a focus on cybersecurity. Prior to her work with the Stimson Center, she was a Strategic Advisor to the Internet Security Alliance and to the World Institute for Nuclear Security (WINS). In her role at WINS, Rauhut led international roundtables and authored policy papers on improving global governance of nuclear and cybersecurity through building the business value of security. Previously, she was the Deputy General Counsel of Lawrence Livermore National Laboratory in California.

SARA Z. KUTCHESFAHANI is a Senior Policy Analyst at the Center for Arms Control and Non-Proliferation and the Senior Program Coordinator for the Fissile Materials Working Group (FMWG), where she focuses on efforts to reduce the risk of nuclear proliferation and terrorism. She also teaches graduate classes at the University of Maryland, where she is a Research Associate at the Center for International & Security Studies at Maryland. She was previously the Executive Director at the Center for International Trade and Security and the Director for the Master of International Policy (MIP) Program at the University of Georgia, where she worked on nuclear security-related projects and nuclear non-proliferation policy issues, and taught graduate courses on nuclear non-proliferation history and the global nuclear order. She has held research positions at Los Alamos National Laboratory, the RAND Corporation, the European Union Institute for Security Studies in Paris, and the International Institute for Strategic Studies in London. She holds a PhD in Political Science from University College, London, and is the author of *Politics and the Bomb: The Role of Experts in the Creation of Cooperative Nuclear Non-Proliferation Agreements* (Routledge: 2014), and the recently published, *Global Nuclear Order* (Routledge: 2019).

ERIN CONNOLLY is the Program Assistant at the Center for Arms Control and Non-Proliferation and the FMWG where she provides support for nuclear security and U.S. non-proliferation policy projects, with a special emphasis on youth engagement. Erin and Kate Hewitt received the 2018 Leonard M. Rieser award from the Bulletin of the Atomic Scientists for their article and work surrounding youth education. Erin has taken part in the CSIS Project on Nuclear Issues conference series, focusing on radiological materials security in addition to the CSIS Nuclear Scholars Initiative focusing on artificial intelligence. Her recent publications include pieces on artificial intelligence, youth education, and radiological security. She received a Bachelor's degree from College of the Holy Cross in International Studies with a minor in French and a concentration in Peace and Conflict studies.

LIST OF ACRONYMS & ABBREVIATIONS

CPPNM: Convention on the Physical Protection of Nuclear Materials

DBT: Design Basis Threat

GICNT: Global Initiative to Combat Nuclear Terrorism

HEU: Highly Enriched Uranium

IAEA: International Atomic Energy Agency

IPPAS: International Physical Protection Advisory Service

MOX: Mixed Oxide Fuel

NEA MDEP: Nuclear Energy Agency's Multinational Design Evaluation Programme

NEI: Nuclear Energy Institute

NGO: Nongovernmental Organization

NIST: National Institute of Standards and Technology

NSSC: Nuclear Security Support Center

NUSEC: Nuclear Security Information Portal

OSCE: Organization for Security and Co-operation in Europe

OT: Operational Technology

PU: Plutonium

VPN: Virtual Private Network

WANO: World Association of Nuclear Operators

WINS: World Institute for Nuclear Security

WNA: World Nuclear Association

TABLE OF CONTENTS

4 FOREWORD

6 DAY ONE OVERVIEW

6 Framing the Discussion: Where are the Risks in Civilian Owned/Controlled Fissile Materials and What Can be Done About Them?

7 Current Baseline: Status of Cybersecurity Threats and Vulnerabilities

9 Trends: Examining the Dimensions of Current and Emerging Cyber Risks

10 DAY TWO OVERVIEW

10 How Are/Can Nuclear Cyber Risks Be Addressed?

13 The Patches: Identifying Current Work and Common Threads

14 Brainstorming the Future: Incentives and Other Ideas?

15 Design Basis Threat (DBT)

17 NEXT STEPS

22 APPENDIX I: A FRAMEWORK FOR CONSIDERING NUCLEAR CYBER RISKS

23 APPENDIX II: THE “AIR GAP” MYTH

FOREWORD

The Fissile Materials Working Group (FMWG), in partnership with the Stimson Center, hosted a 1.5-day off-the record (Chatham House Rule) Nuclear-Cybersecurity Workshop, which took place at the Vienna Center for Disarmament and Non-Proliferation. The invitation-only workshop comprised a group of two dozen cybersecurity experts and stakeholders in the nuclear industry, including operators, transporters, regulators, states, and nuclear security analysts. The group discussed cybersecurity risks affecting the nuclear sector and explored what needed to be done, across the board, to manage those risks.

The main goal of the highly interactive workshop was to identify the critical gaps in nuclear cybersecurity internationally and to develop preliminary recommendations on how non-governmental organizations (NGOs) can most effectively help reduce those gaps. Specifically, the workshop addressed the following questions:

1. What are the current cybersecurity threats facing the civilian nuclear sector?
2. Which elements of the nuclear sector are the most vulnerable to cybersecurity threats?
3. What progress has the international community made in addressing these vulnerabilities?
4. What are the existing gaps requiring additional support to enhance cybersecurity?

In brief, the 1.5-day workshop demonstrated clear gaps in the nexus of cyber and nuclear security, highlighting the important need for further collaboration and information sharing across all relevant stakeholders. Consequently, the experts suggested that NGOs – given that they are well-positioned to facilitate conversations among the various stakeholders – prioritize the following four action items:

1. Support information sharing on cyber and nuclear security across the various stakeholders
2. Develop and promote scenario-based discussions
3. Host table-top exercises among operators, transporters, cybersecurity experts, and other stakeholders to improve communication and build trusted relationships
4. Perform other relevant targeted research (listed at the end of the report).

This report outlines what was covered throughout the workshop. At the end of the report, there is a list of next steps the NGO community – as well as other stakeholders – should consider taking to reduce the cybersecurity risks affecting the nuclear sector.

The FMWG and Stimson's immediate next step is to share these findings with the nuclear and cybersecurity community, and to explore future collaboration amongst key stakeholders. Follow-on discussions are planned for Spring 2019.

KEY TAKEAWAY

Many cyber and nuclear security stakeholders are addressing the same challenges, but have not effectively come together to share information, experiences, knowledge and best practices. This applies to all areas of the nuclear sector. Broad international agreement to establish norms regarding cyberattacks needs discussion even beyond the nuclear community. Nuclear cybersecurity is only unique in its potential for heightened consequences. Additional research and advocacy efforts are needed to promote transparency and a coherent set of norms and principles across global critical infrastructures.

DAY ONE OVERVIEW

Framing the Discussion: Where are the Risks in Civilian Owned/Controlled Fissile Materials and What Can be Done About Them?

The first day of the workshop began with an interactive exercise which focused on how to conceptualize *nuclear* cybersecurity. The nuclear sector poses a unique threat given the potential for a radiation release (on site, offsite if material is stolen, or during transportation of material, or via nuclear device if HEU/PU) and public panic due to poor/false communication and its consequences including social mayhem. Accurate, factual messaging from trusted sources is particularly important given the potential for disinformation.

Ultimately, the group agreed the intersection of cyber and nuclear risks can be found across the sector, in nuclear facilities and related operations, including: nuclear power plants (including decommissioned ones), new reactors (including small modular reactors, floating and underwater reactors), all types of research and test reactors, fuel fabrication facilities, storage sites, as well as domestic and international transportation. Moreover, the group agreed that the biggest consequences associated with the risks could come from the following scenarios:

1. Theft/diversion of separated plutonium (PU), highly enriched uranium (HEU), mixed oxide (MOX) fuel
2. An accident or sabotage resulting in radiation release
3. Public response/reputational damage from a real, potential, or false event
4. Business interruption.

Other incidents discussed included compromise of: personal/official information; sensitive technical design information and intellectual property; transportation plans; and other information/events. All these events influence the confidentiality, integrity and availability of information systems that support the safety and security of the nuclear regime and its public trust. Appendix I outlines the overall framework that developed, recognizing that each part of the nuclear sector may have different risks and cybersecurity priorities.

Current Baseline: Status of Cybersecurity Threats and Vulnerabilities

Adversaries posing threats may be terrorists, extremists, criminals (including organized groups), outsiders (such as suppliers) or insiders (acting intentionally or negligently), with nation-states posing the most credible threat. However, a state-triggered consequential event could be considered an act of war, with attribution remaining an issue. The likelihood of cyberattacks is 100%, although an attack is not always successful. The characteristics of the attacks and the best ways to address them are not always well-shared in the nuclear industry – or, some contend, not shared at all – at least not intentionally. In addition, the information that is shared has not been presented in ways that are compatible with the diversity and uniqueness of stakeholders across the nuclear community.

THE LIKELIHOOD OF CYBERATTACKS IS 100%, ALTHOUGH AN ATTACK IS NOT ALWAYS SUCCESSFUL.

In terms of vulnerabilities and impact, Stuxnet dispelled the perception that a cyberattack could only affect information

Maritime shipment of high level radioactive waste. Cherbourg, France. Photo Credit: Dean Calma / IAEA

THE EXPERTS STRESSED THE NEED TO INCENTIVIZE BETTER PERFORMANCE BEYOND REGULATIONS TO MITIGATE SECURITY RISKS.

technology systems. In fact, Stuxnet demonstrated how a cyberattack could compromise “air-gapped” security measures, kinetically impact industrial control production and safety systems, and result in the physical destruction of critical equipment.[1] The emerging landscape of cyberattacks targeting industrial control systems underscores the goals of modern adversaries and highlights their desire to cause physical damage through cyber means. Consequently, there is increasing concern for potential blended cyber-physical security/attacks to damage physical assets.

Cybersecurity specialists and facility operators debated the effectiveness of nuclear facilities being “air gapped.” An air gapped system is a computer or network that has no outward connectivity, i.e., no network interfaces, either wired or wireless, connected to outside networks. Experts from the group explained that computer-based systems are not completely insulated by “air gaps.” Though air gaps offer a high level of security, they are not failsafe. Although many asset owners

[1] Although attacks on industrial control systems were not new, Stuxnet heightened awareness of the threat; see IBM Security, “Security Attacks on Industrial Control Systems”: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03046usen/sel03046-usen-00_SEL03046USEN.pdf.

feel their systems are protected because there is no physical or logical connectivity into critical network enclaves, the networks are very rarely and ever truly isolated. Undesirable consequences can be caused by accessibility to vital networks through both authorized and unauthorized methods. This includes contractor access, removable media, or the compromise of vital networks due to misconfiguration of security countermeasures. For example, approved access points often exist for maintenance activities, including for third-party updates and monitoring, that could potentially be compromised. Appendix II provides a further discussion of air gaps.

The increased frequency of cyberattacks and their evolution demonstrate continued threat actors' interest in targeting critical infrastructure, including nuclear facilities, along with changing adversarial capabilities and attributes. A strong regulatory framework is needed to address cybersecurity, but even so, organizations that comply with cyber regulations may still be vulnerable to attack as regulations only serve as a baseline based on historic attack patterns. It has been shown that compliance does not necessarily equate to security. Numerous victims of successful cyber-attack have been fully compliant with regulatory requirements when they were compromised. The experts stressed the need to incentivize better performance beyond regulations to mitigate security risks. In this vein, it would also be useful to create an anonymized database of nuclear cybersecurity incidents to facilitate lessons learned among those working with cyber and nuclear security. Operator experience databases already exist for safety events, so why should under sharing of security events weaken this proven effective tool?

Trends: Examining the Dimensions of Current and Emerging Cyber Risks

The first day of the workshop concluded with a discussion highlighting how attackers will use the means available to them, of which there is no shortage in the cyber realm. Interoperability and interdependency requirements that an asset owner shares with its service provider and supply chain create new attack vectors for the adversary. Regulators, suppliers/vendors, auditors, advisors, and other contractors are all vulnerable to cyberattacks and are potential vectors for compromising operators/transporters. Relationships with them need to be well managed, as attackers will often target these entities as a pathway to the organization due to their often-vulnerable security posture. As a result, all organizations should be expected to include cybersecurity as part of their general risk assessment and promote cyber-awareness among their leadership, staff, and any other employed entities. The experts suggested creating stronger cybersecurity requirements for operational partners that operators and stakeholders rely on with enhanced requirements specifically for third parties, contractors, and suppliers involved with the nuclear sector.

DAY TWO OVERVIEW

How Are/Can Nuclear Cyber Risks Be Addressed?

The second day of the workshop began with a consideration of the role of regulation in cybersecurity, the establishment of nuclear security baselines and the potential for new approaches to minimize the cybersecurity risks affecting the nuclear sector.

Although nuclear security regulators do engage with each other,[2] a need was identified for a comparative analysis across states of cybersecurity specific to nuclear security in order to ascertain the effectiveness of different regulation models and elements that may be improved. The majority of cybersecurity regulations for nuclear facilities are high-level performance guidance. The challenge is how the regulations are implemented and evaluated. Best practices may not be incorporated into regulations, but they can be a part of regulatory guidance development, which is well needed.[3] As regulators are increasingly moving towards outcome-based regulation, it is up to the operators to prove they have effective systems in place. A relatively mature security department, with supportive and informed management, does not need a regulator to stimulate appropriate cybersecurity risk management.

In the realm of cyberspace, the operators and their security teams (including specialist consultants) are on the front lines and can better understand the vulnerabilities of their own facilities and systems than regulators. Thus, a dynamic open-source toolkit that leverages past experience and successes from the global community would be useful to assist the nuclear sector in the implementation of regulatory guidance. This toolkit would most certainly incorporate materials already proven effective and could be adapted from existing International Atomic Energy Agency (IAEA) guidance, international standards, and industry good practices and insight/lessons provided by nuclear regulatory agencies, cybersecurity experts, or experienced sector personnel. This model has, in fact, been tried and tested. As one participating regulator remarked, his country developed regulations and guidance through expert sources, including the IAEA, the U.S. Nuclear Regulatory Commission, and consultations with the country's own nuclear operators. Such an approach and the resulting guidance may be helpful for new nuclear countries.

[2] This includes safety regulators in some states that do not have combined safety and security regulators.

[3] See for example, U.S. Nuclear Regulatory Commission's "Nuclear Regulatory Guide 5.71" (January 2010): https://scp.nrc.gov/slo/regguide571.pdf.

Moreover, it was noted that regulations only work if they are: 1] effectively implemented, and 2] sufficiently evaluated for conformance. Both conditions depend upon the capability and capacity of the regulator and the operator. On a voluntary basis, states can request special IAEA advisory missions to review aspects of safety or security performance.[4] IAEA reviews, such as an International Physical Protection Advisory Service [IPPAS] mission, are well regarded but IAEA does not have enough staff to serve all its member states requests. For nuclear power plants, the World Association of Nuclear Operators [WANO] could be encouraged to include a cyber assessment as part of an extended safety review of power plants since many of the instrument and control systems of concern are installed for safety reasons. Moreover, insurers are currently developing a

IN THE REALM OF CYBERSPACE, THE OPERATORS AND THEIR SECURITY TEAMS...ARE ON THE FRONT LINES AND CAN BETTER UNDERSTAND THE VULNERABILITIES OF THEIR OWN FACILITIES AND SYSTEMS THAN REGULATORS.

[4] For a chart of IAEA safety and security reviews, see: https://gnssn.iaea.org/Pages/PeerReviewsandAdvisoryServicesByAudienceAndTheme.aspx. Physical security reviews are part of IAEA International Physical Protection Advisory Service (IPPAS) missions. See IPPAS Computer Security Review Guidelines starting on p. 214 of https://www-pub.iaea.org/MTCD/Publications/PDF/SVS-29_web.pdf. For a broader understanding of nuclear industry performance assessments, see: https://www.stimson.org/content/nuclear-energy-securing-future-case-voluntary-consensus-standards.

cyber assessment scheme, which could feed into cybersecurity assessments. Although WANO is not currently planning on conducting cybersecurity peer reviews, the World Institute of Nuclear Security (WINS) is in discussion with WANO, who has welcomed WINS' proposal to examine how peer reviews of cybersecurity governance could be conducted.

Although nuclear security is a state responsibility, licensees are "duty holders" – and the amended Convention on the Physical Protection of Nuclear Material (CPPNM) notes their important role in security.[5] However, it is not clear how or whether actual implementation of the amended CPPNM's fundamental principles will be assessed internationally, except within each state itself or as part of a voluntary IAEA review mission.

Moreover, the experts discussed a potential cyber non-attack-on-nuclear-facilities agreement between countries mirroring the India-Pakistan non-attack agreement.[6] Additional coordination is needed not only to agree on what actions should be prohibited but also on joint processes for investigation, prosecution, and penalties.[7] Additional research in this area would be needed to further assess this potential.

[5] The 1987 CPPNM was an instrument to secure civil nuclear material during international transport, but the 2016 amended convention transformed that into one ensuring the physical protection of all civil nuclear materials and facilities, preventing and combating related offenses, and facilitating cooperation among the States Parties. For discussion of licensee responsibilities, see: https://www.stimson.org/content/industry%E2%80%99s-potential-role-implementing-cppnm-amendment-and-improving-nuclear-security.

[6] The Non-Nuclear aggression agreement is a treaty between India and Pakistan on the reduction/limitation of nuclear arms and pledges not to attack or assist foreign powers to attack on each other's nuclear installations and facilities. For more information, see: https://www.nti.org/learn/treaties-and-regimes/india-pakistan-non-attack-agreement/.

[7] See "Interpol-Europol Conference Calls for Global Response to CyberCrime," Europol Press Release, 18 September 2018: https://www.europol.europa.eu/newsroom/news/interpol-europol-conference-calls-for-global-response-to-cybercrime.

The Patches: Identifying Current Work and Common Threads

The session considered current efforts in the cyber/nuclear security realm, including NTI's work on cybersecurity regulatory assessments,[8] and the IAEA development of soon-to-be-released guidance on cybersecurity. Participants noted that the nuclear sector may be regulated for cybersecurity as part of the state's broader critical infrastructure, as opposed to a separate nuclear security entity. As such, nuclear-specific directives may not be addressed separately in laws and regulations. As an energy provider, the nuclear industry is just one element of critical infrastructure, albeit a special one given potential consequences. The work to make critical infrastructure as a whole "cyber-secure" should therefore be considered. The potential of the European Union's certification schemes was also discussed and noted as something to follow and assess for their importance in cyber risk reduction.[9] Chatham House's nuclear cyber research was also noted, as was Stimson's work on good security governance in conjunction with the WINS Academy.[10]

The session also included discussions on the professionalization of the security element in the nuclear industry. By way of example, WINS provides a comprehensive professional development course on cybersecurity in the nuclear sector.[11] Management need to be made aware of what questions they should be asking to ensure facility security in a dynamic risk environment. In addition, it would be useful for a senior member of the management team to be responsible for contextualizing cyber risks in reports to the management team/board to promote better understanding of the risks.

The experts remarked how cybersecurity is only one of many important issues that are considered by personnel running nuclear facilities and much can be learned from other sectors' security approaches, including how the diamond industry has confronted insider threats. It is critical that the importance of cybersecurity is conveyed to those running the nuclear facility so that it is properly prioritized within an "all-risks" integrated management system.

[8] Michelle Nalabandian, Alexandra Van Dine, and Page Stoutland, "Global Action on Cybersecurity at Nuclear Facilities: Moving Beyond the Status Quo," NTI, 25 July, 2016: https://www.nti.org/analysis/articles/global-action-cybersecurity-nuclear-facilities-moving-beyond-status-quo.

[9] See Catherine Stupp, "Plan for EU cybersecurity certification receives Parliament approval," EURACTIV.com, 10 July 2018: https://www.euractiv.com/section/cybersecurity/news/plan-for-eu-cybersecurity-certification-receives-parliament-approval/.

[10] For Chatham House work, see: https://www.chathamhouse.org/research/topics/cyber-security and https://www.chathamhouse.org/about/structure/international-security-department/cyber-and-nuclear-security-project. For Stimson's work, see: https://www.stimson.org/programs/nuclear-security, especially https://www.stimson.org/content/shaping-strong-security-norms. The Center for International & Security Studies at the University of Maryland is a further entity working on this critical issue; see: http://cissm.umd.edu/project/holistic-approach-cybersecurity-risk-management.

[11] https://wins.org/product/nuclear-cyber-security/.

Brainstorming the Future: Incentives and Other Ideas?

In this session, participants discussed what cost-effective tools could be implemented to incentivize proactive cybersecurity globally. Currently, a role for incentivizing security is being explored, such as recognizing good performers and limiting liability. Insurance providers, for example, could provide a cybersecurity incentive to those with a good level of security. A cybersecurity assessment could also be completed by a trusted third party. Stimson is developing a security governance template to demonstrate management's serious attention to and involvement in security decisions. Demonstrated good governance or due care can reduce potential liabilities in the event of an incident and thereby incentivize better governance.

The group discussed the role of voluntary standards, of which there are many – albeit with little agreement on essential ones. In addition to some EU efforts, the U.S. work on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the U.S.-Canadian electric sector supply chain reliability standards were discussed as possible models that could be used alongside some countries' minimum regulatory requirements.[12] Countries might consider adopting an approach to limit liability in exchange for attaining a certain performance standard such as the U.S. Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act).[13] Such an approach would be an important step in establishing an international norm. Standards adoption and compliance are risk reduction measures that can become market differentiators for companies and vendors.

However, as the experts discussed, even if the nuclear operator performs well, the underlying issue of potential software flaws will continue to exist unless liability terms change. Most commercial off-the-shelf software providers include a disclaimer in their standard terms of sale to the effect that their product is not covered for use at a nuclear power plant (so an operator uses commercial off-the-shelf software at its own risk). An advanced persistent threat cannot be prevented; for nuclear, defense-in-depth and resilience are critical.

MOST COMMERCIAL OFF-THE-SHELF SOFTWARE PROVIDERS INCLUDE A DISCLAIMER IN THEIR STANDARD TERMS OF SALE TO THE EFFECT THAT THEIR PRODUCT IS NOT COVERED FOR USE AT A NUCLEAR POWER PLANT.

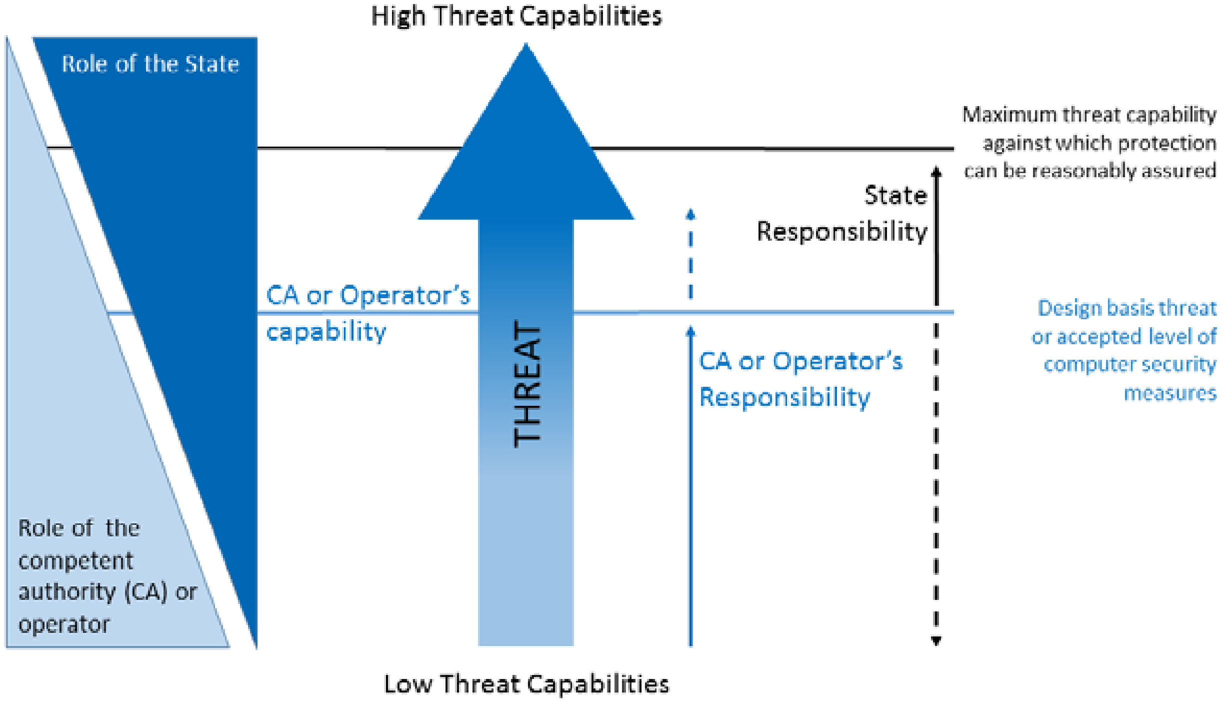
[12] See: https://www.nist.gov/cyberframework; https://www.ferc.gov/media/news-releases/2018/2018-4/10-18-18-E-1.asp#.XBRG4mZ7m70.

[13] https://www.insideenergyandenvironment.com/2018/08/pseg-becomes-first-public-utility-to-secure-safety-act-liability-protections-from-dhs/.

Design Basis Threat (DBT)

This session focused on the extent to which the current Design Basis Threat (DBT) process is sufficient. The DBT identifies the set of adversarial capabilities against which a nuclear operator can reasonably be expected to defend. In addition, it acknowledges that nuclear operators are unable to defend against the entire spectrum of security threats, including possible state-sponsored actions. For these threats that lie "beyond the DBT," while defense is a joint responsibility, the state will be the primary party responsible for addressing the threat.

Cyber DBT Roles: State vs. Operator


High Threat Capabilities
Role of the State
Maximum threat capability against which protection can be reasonably assured
State Responsibility
CA or Operator's capability
THREAT
Design basis threat or accepted level of computer security measures
CA or Operator's Responsibility
Role of the competent authority (CA) or operator
Low Threat Capabilities

Source: International Atomic Energy Agency, "Computer Security for Nuclear Security: Draft Implementing Guide," (2016). NST045, IAEA, Vienna (2018 Member State Approved).

The DBT discussion sparked significant interest as experts considered what is the most reasonable (credible) level of threat for which a facility needs to plan to defend. Cyberattacks have proven difficult to incorporate into the DBT framework, and experts suggested better integration of cyber threats (and the potential for blended cyber-physical attacks) into facility DBTs. Facilities should be able to defend against a tactical cyberattack that has been designed to target the facility information systems or physical protection systems that support the safety and security of operations. Modern physical protection systems are becoming more digital in nature. As such, their susceptibility to cyberattack (and the consequence that such an attack has on the level of physical protection that can be enforced) must be taken into consideration. It is possible that an advanced persistent attack could be beyond the DBT and the facility's ability and resources. However, delaying, defending and responding to any cyberattack may be considered part of the nuclear industry's defense-in-depth approach and required resilience. IAEA guidance on developing a Cyber DBT is forthcoming.

The operators have the responsibility for the protection of their computer-based systems. Defense-in-depth principles should be applied to manage unauthorized access and manipulation to computer-based systems. But the operator's information systems (as well as the underlying digital infrastructure of physical protection systems) may include commercial off-the-shelf software that it does not really own. In practice the solution provider may lease applications and programs from a software provider, who may or may not be diligent in maintaining software integrity or security. The inherent vulnerability in these commercial applications are passed on to the operator and may be unknowingly resident in the systems responsible for safety and security. Software providers often perform "best effort" analysis and safeguarding to prevent their products from creating cybersecurity risks in the environments in which they are used. Panel experts did comment on how software providers can try their best to prevent their product from being corrupted by malware through continual improvements (patching and upgrades) but caution about its uses in mission-critical environments and takes no responsibility in the event their product fails or contributes to a security incident. The operator carries the responsibility of updating software and applications while the provider of the software makes no guarantees about the security of the software itself. Additionally, outsourcing of services is becoming more common and can present a source of vulnerability. These additional vectors must be considered in security planning. Security is a process and continual improvement is critical.

Given that cyber threats do not respect physical boundaries, experts emphasized the need to nurture the relationships among the intelligence community, nuclear operators/transporters, private sector, and research communities in order to share information and better understand potential threats. Experts agreed on the need to examine: ways to better utilize operator knowledge, and methods to better educate and inform senior management on cyber risks and operator responsibilities.

NEXT STEPS

The following is a list of ideas (not all mentioned above) where additional research/advocacy/facilitated discussions could help to reduce nuclear cyber risks. Some can be led by the NGO community or by other stakeholders with NGO participation:

1. **Facilitate more communication among stakeholders (including nuclear operators/transporters, regulators and other competent authorities, cyber experts, nuclear security experts) to improve information exchange regarding best practices, emerging threats/risks, and new regulatory approaches which are especially important as there is more digitization in existing facilities and new technologies.**

    a. This can be accomplished through forums ranging from workshops to table-top exercises, as appropriate for each targeted effort. NGOs could provide an independent forum for information exchange, potentially as side events to existing events and/or conferences. Some examples include:

        i. WINS' large membership base and its workshops could be further supported to provide a system of regular exchanges among selected parties.

        ii. The Nuclear Energy Agency's Multinational Design Evaluation Programme (NEA MDEP), the World Nuclear Association's (WNA) Cooperation in Reactor Design Evaluation and Licensing group, and others have initiated joint discussions that might be leveraged.

        iii. WNA's Security and Resilience Working Group has been established to share expertise and good practice which could be engaged to work with NGOs and others in this area.

    b. Regional discussions could include topics on risk management, standards, and approaches to certification, e.g. EU certifications, and good practices.

2. **In support of the above, it is recommended that a comparative analysis of existing cybersecurity regulation and assessment activities be conducted to identify effective strategies and good practices and how to enforce or incentivize compliance. NGOs, the IAEA, and/or regulators could lead the effort, which should include multiple stakeholder groups. Specific topics of interest should include but may not be limited to:**

    a. Required information disclosures: trigger events, when to disclose, to whom, what type of communication to use, etc. This should include incidents currently classified as "safety" events that also have a security aspect.

b. Vulnerabilities that are not being sufficiently addressed, e.g., the myth of air gaps (See Appendix II), threat actors gaining access by exploiting the access of the sector's trusted partners (including regulators, suppliers, lawyers, owners, auditors, assessors, researchers, etc.).

c. New technologies' threats and opportunities, which include:

   i. How/whether to control electronics, small-scale digital devices, including those used for system health and intelligence, and researching how those devices can be compromised to support a cyberattack and for intelligence gathering.

   ii. Possible threats posed by drones overflying facilities/transport for purposes of surveillance or targeting.

   iii. Instrumentation and control visualization technologies.

   iv. Using cloud-based applications, i.e., simply moving your data and applications to other people's computers.

   v. VPN challenges including an attack on software or use of split tunneling.

d. State approaches to investigation, prosecution, and penalties for cybercrimes, e.g., cyberattacks, cyber terrorism, etc.

3. In support of the above, advocate for more reviews, sharing of best practices, tabletops, and leverage existing institutions. Some examples to consider may include:

a. CPPNM: Leverage the newly amended treaty. Look at other successful models for development of successful norms (e.g., Montreal Protocol) and consider how best to apply this to the implementation of CPPNM including monitoring and supporting compliance with its fundamental principles.

b. IAEA: Explore ways to incentivize states to request and use IAEA review missions and follow-up missions. For example:

   i. Explore developing simpler/consolidated reviews, with more of an agreed norm across different IAEA divisions/departments.

   ii. Evaluate and identify areas where security can be included in other reviews or combined into joint reviews to be more efficient and productive, e.g., safety and security culture.

   iii. Publicize the reviews and the results of the reviews and follow-up missions more broadly, e.g., by noting on a webpage which state is having reviews and follow-ups. This may foster reputational gains and public support.

c. Consider what other roles the IAEA, Nuclear Suppliers Group, Global Initiative to Combat Nuclear Terrorism (GICNT), Global Partnership, Interpol, can undertake with NGOs bringing together non-state stakeholders.

d. Support third-party assessments and other independent reviews, including how an operator responds to the dynamic threat environment, assessing and adjusting to the criticality of risks, and managing incident response.

4. **Develop more scenario-driven exercises in cyber-incident response management and communications to address the issues of misinformation being fed to the public and the potential sabotage of emergency response efforts. For example, develop, including from the exercises, more good practices in this area. This can include working towards the creation of an "accurate news" repository and the joint development of prepared public emergency communications and pre-planned incident reporting for various scenarios. This should be coordinated with IAEA emergency response work and could be exercised through GICNT as well as NGO-coordinated table tops.**[14]

5. **Compile an anonymized database comprising lessons learnt regarding nuclear and cybersecurity to create an "operator's database" resource. This could be based on opensource reporting and may include safety incidents. The viability of this could be considered, including based on other's efforts, such as RISI Online Incident Database.**[15]

[14] See, for example, the IAEA Safety standards on emergency preparedness and response: https://www.iaea.org/topics/emergency-preparedness-and-response/safety-standards-technical-guidance.

[15] RISI Online Incident Database can be accessed here: https://www.risidata.com/Database.

6. **Help develop new thinking on cooperative efforts (perhaps similar to the Proliferation Security Initiative) and on multilateral agreements not to target each other's nuclear facilities and explore the potential for other related nuclear/radiological or critical infrastructure agreements. Some examples to consider may include:**

    a. An assessment of the global response to attacks on nuclear facilities, e.g., in Iraq, Syria, Iran, and how this could/should be adjusted.

    b. An evaluation of agreements that worked, such as the Obama-Xi 2014 agreement, to reduce economic espionage or India-Pakistan's agreement not to attack nuclear facilities, which would include an assessment of how well they have or could work.

    c. Considering new ways/forums to develop agreements, such as a protocol to the convention on nuclear safety, discussion in OSCE for more confidence-building measures, and discussion in the South Korea/Japan/China safety and security forum.

7. **Educate (congressional, governmental, operator) leadership regarding the importance of cybersecurity through increased communication and putting cyber in the context of other threats. This includes, *a priori,* the need to identify a common understanding of the cyber/nuclear security issues. In the United States, for example, it would be beneficial to educate Members of Congress and their staff on the intersection of cyber and nuclear threat vectors. Congressional engagement may cultivate more effective cybersecurity legislation and standards.**

8. **Support the current and next generation of cybersecurity experts – i.e., human capacity development – to increase all nuclear professionals' cyber awareness, and advocate for organizations to understand the importance of a need for regular cyber training. Moreover, there needs to be a concerted effort to get the IAEA and nuclear industry to understand the importance of and need for certified professional development programs that build cybersecurity competence and capacity. Some examples to consider may include:**

    a. NGOs can work with existing programs such as the IAEA's Nuclear Security Information Portal (NUSEC) and the Nuclear Security Training and Support Center (NSSC) Networks to promote appropriate cybersecurity professional certification.

    b. Organizations such as WINS can provide targeted professional development programs (e.g., the WINS Academy) for those working in the nuclear industry to address emerging issues, gaps, and best practices.

    c. NGOs can work with funders in order to provide financial support for sustained education or workshops that often prove difficult for organizations to finance.

9. **Consider transportation, given its special regulatory controls and differing international (and even domestic) requirements. For example:**

    a. NGOs can research instructions and communication handling for the transportation of nuclear materials (e.g., who is aware of movements and risk mitigation) and how jurisdictions do and should differ to effectively manage risks.

    b. Future transport trends should be considered, e.g., driverless cars, drones (for transportation and for monitoring), blockchain smart contracts, including the need to generally examine the security of third-party outsourcing and establishing trusted relationships.

10. **Other ideas include:**

    a. Research the possibility of sharing lists of vendors who perform poorly/do not meet standards (blacklisting or whitelisting) and potential for mitigating any associated liabilities with that sharing.

    b. Develop agreement around shared reporting of incidents using a cybersecurity incident scale to gauge how severe an event is to clarify context and significance.[16]

    c. Review/support iterations of IAEA's Cyber DBT development guidelines.

    d. Help sponsor an award for an organization that displays good security practices, such as the Canadian excellence award, the NEI awards, etc.

    e. Undertake cutting-edge research to bring about a new, more secure method of connectivity.

[16] Perhaps based on the simple one devised by the IAEA, "Computer Security Incident Response Planning at Nuclear Facilities," 2016, p.27: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf.

APPENDIX I: A FRAMEWORK FOR CONSIDERING NUCLEAR CYBER RISKS

Where are the Risks in Civilian Owned/Controlled Fissile Materials? What is the range of incident scenarios?

Where are the Risks in Civilian Owned/Controlled Fissile Materials?			Threats	Vulnerabilities		Consequences	
WHAT: DISCUSS RANGE OF INCIDENT SCENARIOS			IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
WHERE	WHO	SUB-CLASS OF ACTIONS?					
POWER PLANTS–EXISTING	State	• Intentional, accessing remotely (digitally) or via roles below (insider or outsider) • Consider a combined cyber/physical attack				• Public panic • Sabotage for rad release • Theft of material (Pu, HEU, MOX) • Business Interruption, power outages • Theft of personal information • IP Theft • Reputation, incl. effect on nuclear industry	
	Terrorist						
	Extremists						
	Criminal elements						
	Workers (incl. former workers, retirees)	Intentional					
		Accidental					
		Negligent					
	Contractors (and subcontractors, incl. those who built the facility)	Intentional					
		Accidental					
		Negligent					
	Suppliers (and their suppliers)						
	Lawyers/Accountants/ Other service providers						
	Owner/business offices						
	Regulator						
DECOMMISSIONED NPP			Conclusion: Better cyber hygiene (e.g. awareness training and certifications, automated protections) and info sharing can reduce vulnerabilities. However, organizations cannot prevent a determined adversary and will need defense in depth and planning for incident response–including planned internal and public communications–to manage risks.				
NEW GENERATION NPP							
SMRS							
FLOATING/UNDERWATER REACTORS							
OTHER							
RTRS							
FUEL FACILITIES							
STORAGE SITES?							
TRANSPORT							

"Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[17]

[17] Source: Operational Guidance for the EU's international cooperation on cyber capacity building, European Commission, 2018, p. 15: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.

APPENDIX II: THE "AIR GAP" MYTH

Laser/optical data diodes, which physically ensure a one-way flow of information, are widely used in nuclear facilities as a way to help ensure security between networked zones. These devices facilitate the one-way egress of operational data from vital networks to non-vital areas while preventing the ingress of data into vital networks from non-vital networks. However, a data diode does not make an air-gapped network. In practice, organizations must transfer data into and out of their operational networks for a variety of reasons and in many cases augment their architecture to meet data transfer needs, thus risks arise:

1. Some power operators are segmenting their networks using traditional network firewalls/switches for network segmentation. These devices can be reconfigured to compromise the segmentation and create a bypass around security measures.
2. Some organizations allow USB keys to enter and exit their operational technology (OT) network. A data diode, firewall or switch has no capability to stop removable media from being physically brought into a facility networking environment.
3. Organizations also allow hardware (e.g. computers, phones, etc.) to enter and exit their OT network as part of facility and operations vendor maintenance.
4. Some use a laser data-diode in one direction, but still have a need for data to go the other direction and thus there is always some access allowed by someone. The requirement for bi-directional data exchange results in some cases in the use of one data diode for inbound and one for outbound. This effectively means there is no air gap (there is a literal air gap, but operators have allowed data to enter and exit).

The real issue is "can data enter the OT network?" Without allowing data to enter the OT network, an operator may not be able to update software, hardware, etc., in the environment. The David Besse nuclear power plant is a good example of a facility that, in theory, was air-gapped. However, due to a secondary "support" connection that bypassed the cybersecurity countermeasures, some facility systems were compromised by the Slammer Worm.[18] More recent threats to critical infrastructure operating systems, including in nuclear power plants, have demonstrated the risks.[19]

In summary

1. Networks are often segmented using protective devices such as firewalls, and these devices can be vulnerable to attacks with the device being bypassed or completely compromised
2. Networks that do use "one-way" data diodes for data egress often still have business requirements to allow data ingress which then happens through physical means (e.g., removable media or vendor laptop) or digital means (e.g., undocumented remote access or maintenance channel)

Thus, operators need to adopt best practices, and to ensure defense in depth, including plans for emergency response/resilience planning.[20]

[18] Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network," *Security Focus*, August 19, 2003: https://www.securityfocus.com/news/6767.

[19] Debra Decker, Kathryn Rauhut, "Cyber Risks Go Nuclear," *Nuclear Intelligence Weekly*, August 10, 2018: https://www.stimson.org/content/cyber-risks-go-nuclear.

[20] See ICS-CERT Recommended Practices: https://ics-cert.us-cert.gov/Recommended-Practices.

THE STIMSON CENTER is a nonpartisan policy research center working to protect people, preserve the planet, and promote security & prosperity. Stimson's award-winning research serves as a roadmap to address borderless threats through concerted action. Our formula is simple: we gather the brightest people to think beyond soundbites, create solutions, and make those solutions a reality. We follow the credo of one of history's leading statesmen, Henry L. Stimson, in taking "pragmatic steps toward ideal objectives." We are practical in our approach and independent in our analysis. Our innovative ideas change the world.

THE FISSILE MATERIALS WORKING GROUP (FMWG) is a non-governmental coalition of over 80 civil society organizations from around the world working to provide actionable policy solutions to keep the world safe from nuclear terrorism. Since September 2017, it has been hosted by the Center for Arms Control and Non-Proliferation, a national nonpartisan, non-profit dedicated to enhancing peace and security through expert policy analysis and thought-provoking research.

FMWG
fissile materials
working group

STIMSON

Nuclear cybersecurity is an important issue that affects not just the nuclear sector but also the world. The nuclear industry offers many benefits, not just as some have noted in the power sector for mitigation of climate change, but also in the fields of medicine and industry. For these benefits to be fully realized, costs and risks in the nuclear sector – including the critical cybersecurity risks - must be well managed or else public acceptance of nuclear's beneficial uses may decline even further.

This report summarizes the outcome of a 1.5-day off-the-record Nuclear-Cybersecurity Workshop hosted by the Fissile Materials Working Group (FMWG), in partnership with the Stimson Center. The group discussed cybersecurity risks affecting the nuclear sector and explored what needed to be done, across the board, to manage those risks. At the end of the report, there is a list of next steps the NGO community – as well as other stakeholders – should consider taking to reduce the cybersecurity risks affecting the nuclear sector.

Many cyber and nuclear security stakeholders are addressing the same challenges, but have not effectively come together to share information, experiences, knowledge and best practices. This applies to all areas of the nuclear sector. Broad international agreement to establish norms regarding cyberattacks needs discussion even beyond the nuclear community. Nuclear cybersecurity is only unique in its potential for heightened consequences. Additional research and advocacy efforts are needed to promote transparency and a coherent set of norms and principles across critical infrastructures.

Fissile Materials Working Group
820 1st Street NE, Suite LL-180
Washington, D.C. 20002
https://armscontrolcenter.org/fmwg/

Stimson Center
1211 Connecticut Avenue NW, 8th Floor
Washington, D.C. 20036
www.stimson.org