Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

A MULTILEVEL APPROACH TO ADDRESSING EMERGING TECHNOLOGIES IN NUCLEAR SECURITY

Ian Andrews
US Department of Energy,
Oak Ridge National Laboratory

Rebecca Earnhardt
Stimson Center

Nickolas Roth
Stimson Center

ABSTRACT

Emerging technologies present a unique set of challenges to operators and regulators. While emerging technologies can be used to strengthen nuclear security systems, they also can increase risks to nuclear facilities. The disruptive nature of emerging technologies could also leave operators unprepared for threats to nuclear materials or facilities. To address the potentially dangerous consequences associated with these innovations, strong adaptative mechanisms and international cooperation about threat mitigation and technological integration are vital. This paper examines the nuclear security implications of emerging technologies from an institutional (as opposed to technology-specific) perspective. Drawing on insights from a recent workshop series hosted by the Stimson Center and the National Nuclear Security Administration (NNSA)'s Office of Global Material Security (GMS) as well as recent research, the paper begins with a definition of emerging technology that bounds the scope of the problem while leaving some margin for expert interpretation. The subsequent sections highlight the challenges as well as potential benefits that these technologies pose at each level of the nuclear security establishment, from the operators of sites hosting radiological or nuclear material, to regulators and national policymakers, to international institutions. Each section also includes specific recommendations for incorporating emerging technologies into radiological and nuclear security planning.

Introduction

The Stimson Center's Nuclear Security program and the National Nuclear Security Administration co-sponsored a series of workshops in 2020 with the goal of developing principles and guidelines for how operators, regulators can adapt to the challenges of emerging technologies; determining how international institutions can support them in this endeavor; and identifying key questions, concerns, and knowledge gaps on this topic. Attended by over 30 international experts, regulators, and industry partners, the workshops yielded important

Notice: This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

insights on how to think about the application of emerging technologies, the utilization of non-governmental pathways to cooperation, the reliance on existing international platforms to promote continued discussion, and the stagnation of national response imposed by regulatory hurdles. This paper draws upon findings and recommendations from those workshops.

Definitions and examples of emerging technologies are abundant, which makes any effort to characterize them a challenge. Our definition builds on important attributes that tend to be consistent across these definitions. For the purposes of this paper, we define *emerging technologies* as technological innovations that are likely to have a significant impact on nuclear security operations in the near future as they continue to mature and proliferate, but whose precise implications and uses are still uncertain.[1]

Despite some common characteristics, not all emerging technologies follow the same development path or timeline. Some feature evolutionary improvement over previous iterations, such as the structural and design enhancements of the 5G standard over previous networking technologies. Others combine multiple streams of technological development into a new novel application. For example, as commercially available unmanned aerial systems (UAS) and artificial intelligence (AI) capabilities both improve independently, AI-based autonomous UAS platforms are quickly becoming a commercial and military commodity.[2]

Risks and opportunities

Emerging technologies present a range of unique risks and opportunities for the security of radiological and nuclear materials, both from operational and institutional points of view. In some cases, technologies that mature and become more easily accessible to adversaries can close capability gaps that would otherwise prevent material theft or sabotage. Others have the potential to strengthen physical protection capabilities, but only after development, implementation and integration into existing plans and procedures. Because the potential impacts of these technological developments are not yet fully understood, they must compete for resources and attention with more immediate and well-defined priorities.

The most immediately apparent risk is that of technological surprise: a novel application of an emerging technology that presents a threat to radiological and nuclear R/N material security that planners and regulators fail to anticipate, suddenly leaving material vulnerable to theft or sabotage and operators without a way to address it. For example, recent attacks using Unmanned Aerial Systems (UAS) such recent attacks against oil processing facilities in Saudi Arabia demonstrate the vulnerability of even well-defended targets against a new adversary capability for which they lack effective countermeasures.[3,4] Technological surprise is an ever-present risk in emerging technologies because they often result from the convergence of multiple lines of technical development into an application whose effectiveness may not become apparent until used by an adversary.

Another related risk that emerging technologies present is the introduction of new vulnerabilities as emerging technologies are adopted at various points in R/N material production, storage and use. Technologies that enable increased digitalization, connectivity and automation can improve the efficiency of nuclear power plants, but they also underscore the challenge that new attack surfaces represent. Although there have been no known successful cyberattacks that successfully compromised the operational controls of nuclear power plants, malware and software malfunctions have previously rendered key monitoring systems inaccessible[5] and infected internal networks at nuclear plants. [6] Other cyberattacks against non-nuclear infrastructure, such as the May 2021 ransomware attack against Colonial Pipeline's billing system, demonstrate that attackers need not access operational technology systems to severely impact operations.[7]

The risk of missed opportunities to harness positive effects of emerging technologies remains an important one for the R/N security mission space, particularly because of safety and security concerns and implementation procedures that may inhibit technology adoption and integration into physical protection systems (PPS) or other security infrastructure. Longstanding challenges to R/N security, such as the effect of cognitive stress and fatigue on security personnel,[8] insider threats,[9] and the challenge of providing realistic training for low-frequency security events, may lessen as emerging technologies provide more potential solutions, but only if those solutions are identified and implemented effectively. Similarly, opportunities to use UAS in security applications are growing along with the technology's capabilities,[10] but the pace and scope of adoption will ultimately determine the impact of this development on global R/N security. Failure to apply these innovations to nuclear security will leave material at unnecessary risk.

In subsequent sections, we will argue that addressing these risks and opportunities in a way that maximizes the security of R/N material worldwide against theft or sabotage requires coordination across institutional and international boundaries to avoid information silos and ensure maximum awareness of both threats and opportunities. In particular, state regulatory bodies must incorporate technical assessments into their threat planning, and develop and share best practices for integrating novel technologies and techniques into operations at sites where r/n material is located or during transportation. Similarly, international engagement to develop common standards and performance-based metrics with which to assess technology-based risks could have a major impact in supporting nuclear security worldwide.

International institutions' role in strengthening approaches to emerging technologies

Every country is responsible for ensuring the security of its nuclear materials and facilities, but countries are more effective at reducing risks if they work together. Multilateral and bilateral nuclear security cooperation leads to stronger nuclear security implementation. As the rate of technological evolution increases, this cooperation will become increasingly important. In an interconnected world, nuclear security threats, especially those involving emerging technologies, often cross international boundaries. What may originate in one country could easily result in disruptions in another. Because of the interdependent nature of nuclear security and the use and response to emerging technologies, international institutions should play a central role as hubs for nuclear security capacity building, leadership and innovation. This cooperation can take place through several different modes.[11]

International Atomic Energy Agency

As the focal point for all multilateral nuclear security cooperation, the International Atomic Energy Agency (IAEA) should play a leading role in supporting states efforts to adapt to emerging technological challenges. The IAEA can offer support through implementation guidance, coordinated research projects, peer review, industry engagement, information and best practices exchanges, and in its support for legally binding agreements.

The IAEA has already demonstrated how it can provide support for emerging technologies with its approach to cybersecurity over the last 20+ years. In 1998, the IAEA published a technical report on incorporating digital technology into nuclear power plants. The report identified that the incorporation of "modern" technology could improve productivity and safety while reducing costs. It also acknowledged that emerging digital technologies present new dangers to the nuclear sector.[12] Since then, the IAEA has continued to support states as they have embraced digital technologies. INFCIRC 225 Rev. 5 emphasizes the importance of cybersecurity, stating "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise…"[13] That same year, the IAEA printed a technical guide on Computer Security at Nuclear Facilities.[14] The IAEA has also held nuclear security trainings for member states.

The IAEA has also demonstrated that it has the ability to serve as an information hub during an emergent security crisis.[15] During the COVID-19 pandemic, the IAEA encouraged its members to use the information-sharing tools it created to help operators learn from experience, including the International Reporting System for Operating Experience for nuclear power plants and the Incident Reporting System for Research Reactors.[16] In April 2020, the IAEA created the COVID-19 Nuclear Power Plant Operating Experience (OPEX) Network to help operators share information and operating experience. The IAEA also organized a survey of how the pandemic was impacting nuclear regulators.[17] These newly developed frameworks for information sharing could adapted to experiences with emerging technologies, and such a tool could be used for sharing best practices.

Another potential multilateral information sharing and innovation tool are IAEA Coordinated Research Projects (CRPs). Even though the IAEA is recognized as the international authority and facilitator on nuclear related issues, the consensus process for decision-making and action is time consuming and can stymie important discussions among member states. Because of this, CRPs can play a role in developing and sharing scientific and operational understandings of the threats and benefits posed by emerging technologies in the nuclear security space. Similar CRP efforts centered on specific emerging technologies such as artificial intelligence or autonomous systems, or more broadly on guidelines for assessing a technological development's impact on nuclear security or incorporating new capabilities into a nuclear facility's security posture, stand to provide valuable information for regulators and operators responsible for securing nuclear material.

CRPs support coordination across multiple states through the investigation of a well-defined problem, framing the member states as part of the solution and fostering higher levels of buy-in from the participating states. CRPs enhance understanding and awareness of emerging technology-related questions, building expert capacity within the member states, while promoting sustained cooperation among project stakeholders who worked together on a solution.

Legally Binding Agreements

The upcoming review of the amended Convention on the Physical Protection of Nuclear Material (amended CPPNM) is another potential opportunity for information sharing. The text of the amendment states that the conference should include a review of the convention's implementation "in the light of the then prevailing situation." Any such review should include discussions of some of the issues and technologies discussed in this paper, including detailed sharing of information on how states are approaching nuclear security. These reviews should also occur on a regular basis, a decision which some states have already endorsed. Additionally, UN Security Council 1540 could serve as a platform for information sharing in this area. It has already held discussions on some emerging technology topics. [18]

Government Commitments

Beyond addressing the technical risks presented by emerging technologies, nuclear security stakeholders face several structural challenges. The rapid pace of change in technological development compared to the implementation of effective guidance and regulations, the tendency against information sharing in the nuclear security field, and the ever-present need to address immediate threats all complicate the task of maintaining a forward-looking security posture that accounts for technological change.

Effective policy development at the state level is a challenge even for the most advanced countries, which can be slow to incorporate new threats into their security plans and regulations. In the United States, for example, the threat the UAS pose to nuclear security has become more prominent as more unauthorized UAS sightings near nuclear power plants are reported[19], but the US Nuclear Regulatory Commission (NRC) has not issued any requirement to date for licensees to defend against them, claiming that they do not improve adversary capabilities beyond current assessments. In fact, according to the NRC, security personnel "do not have authority to attempt to interdict or shoot down aircraft flying over their facilities," including UAS.[20] The developmental trajectory of UAS technology in particular, which now combines autonomous guidance and targeting with lethal armament[21], demonstrates the need to update security guidance and capabilities in response to rapidly changing technological threats.

However, countries such as the United States that possess robust industry and research and development infrastructure can play a key role in helping the broader nuclear security community overcome these challenges. These states can identify and commit to best practices in assessing technological risks and opportunity, and in adopting new technologies into nuclear security planning. They can also proactively share key information with partner countries and the international community via technical meetings, workshops and collaborative research efforts.

Developing an Analytical Framework

States can begin by developing a technology assessment framework (or adapting an existing one) to capture technological maturity, time horizon for developmental milestones, and impact to nuclear security for those concepts and applications that qualify as emerging technologies. While such a framework tailored specifically to nuclear security does not appear to be available to the public, there are existing models that can be adapted. One such example is the US Department of Energy (DOE)'s Technology Readiness Level (TRL) a metric "used by many U.S. government agencies to assess maturity of evolving technologies (materials, components, devices, etc.) prior to incorporating that technology into a system or subsystem."[22] Although it is primarily used within the US government, the overall methodology for conducting TRL assessments is freely available to others and easily adapted to specific attributes of concern to nuclear security stakeholders. A TRL-like metric, accompanied by guidance on the key characteristics that compose each level, could be used to inform which technological applications pose a threat and which ones warrant a high priority for adoption by security forces. A similar scoring rubric, developed and populated through an interdisciplinary engagement process involving technical experts from industry and academia, could also help identify developmental milestones that are relevant to nuclear security practitioners. Such milestones include a technological application reaching consumer markets, key capability improvements, and the point at which it no longer possesses "emerging" characteristics.

While horizon scanning and assessments of new technologies are not new practices and are ongoing across the nuclear security enterprise, a coherent emerging technology strategy requires that these activities be standardized and incorporated into binding regulations to significantly benefit nuclear security. In many countries with a nuclear fuel cycle, the primary regulator is responsible for maintaining a Design Basis Threat (DBT), a characterization of the adversary force that nuclear power plant licensees must be able to defend against.[23] Updates to the DBT are often based on current threat intelligence, but linking it to a technical assessment such as the framework described above will help guard against the potential threats that these technologies present by mandating planning and action to mitigate them. While the specifics of any technical input into the DBT would likely be classified, committing to including evolving technology-based threats and sharing general guidelines for doing so would reinforce it as a best practice for nuclear security. The roots of this concept already appear in international guidance.

Assessing Threats

Recognizing the key role of the DBT tool outlined in INFCIRC/225, the IAEA designed methodology and implementation guidance on how to design, administer, and assess a state DBT.[24] Some emerging technology challenges like cyber security are mentioned, but no comprehensive approach is described. NSS No. 10, however, does state that maintaining the DBT and keeping it up to date is in the purview of the state and will vary depending on the context.[25] Moreover, the document does provide examples of why a DBT would need to be updated and review. Justification includes significant changes to the threat environment, government policy, nuclear material related activities, and third-party review of the DBT.[26] Any of these events could explicitly incorporate emerging technologies related triggers for the modification of the DBT. This guidance is further elaborated upon in other IAEA documents.[27]

Apart from addressing technology-based threats, a comprehensive nuclear security strategy for emerging technologies must also guide the adoption of technologies that can aid in protecting material against theft or sabotage. However, technology adoption carries the risk of adding new vulnerabilities, and tends to be a slow process where critical infrastructure is affected.[28] Balancing the potential security benefits of a new capability with the need for thorough assessment and testing ahead of implementation requires a broad range of resources and expertise. Executive-level bodies such as the National Science and Technology Council (NSTC) in the United States are well-positioned to coordinate research, development and implementation efforts across interagency boundaries, and solicit expertise from the academy and private sector in developing technology adoption strategies for the nuclear security establishment. Moreover, states can develop of strategies and guidance for adapting to rapid changes in threat environments by establishing pre-determined adaptable systems that adjust to elevated threats with corresponding pre-determined levels of additional nuclear security.

States should also proactively engage the international community in developing and implementing training courses, technical exchanges, and workshops that target technology-specific issues as well as strategic approaches to emerging technologies. Best practice exchanges don’t need to be limited to IAEA initiatives. States could commit to including information exchanges on the challenges of adapting to emerging technologies as part of dialogue within the Nuclear Security Contact Group (NSCG). One of the important innovations stemming from the Nuclear Security Summit Process was the NSCG. The NCSG is supposed to meet “annually on the margins of the General Conference of the International Atomic Energy Agency, and, as may be useful, in connection with other related meetings” to discuss “a broad range of nuclear security-related issues, including identifying emerging trends that may require more focused attention.”[29] States participating in the NSCG could create sub-group of the NCSG consisting of government and non-government experts focused emerging technology trends and their near- and long-term impacts on nuclear security. The sub-group would publish assessments to be shared with member states.

States, international organizations, and groups could incorporate emerging technologies into nuclear security-related exercises. The Global Initiative to Combat Nuclear Terrorism could include emerging technologies into its exercises. Nuclear Security Training and Support Centers or Nuclear Security Centers of Excellence could serve as international hubs for assessing emerging technology trends and for the research and development of emerging technologies to be incorporated into physical protection systems. Additionally, through international networks, professional associations, and expert gatherings, nuclear security practitioners could reinforce best practices on the development and maintenance of nuclear security threat assessments, design basis threats, and representative threat statements associated with emerging technologies.

Conclusion

This workshop series helped to illuminate many of the challenges nuclear operators will face as they adapt to the rapid pace of technological evolution. Emerging technologies will continue to challenge those responsible for maintaining security for nuclear facilities. The risks posed by these technologies, however, can be mitigated through focused engagement by international institutions and national commitments to proactive nuclear security implementation.

[1] Daniele Rotolo, Diana Hicks, Ben R. Martin, "What is an emerging technology?," *Research Policy*, Vol. 44, Issue 10, 2015, pp. 1827-1843, https://www.sciencedirect.com/science/article/abs/pii/S0048733315001031 (accessed August 11, 2021).

[2] Joe Hernandez, "A Military Drone With A Mind Of Its Own Was Used In Combat, U.N. Says," *NPR,* June 1, 2021, https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d#:~:text=Pop%20Culture-,Autonomous%20Drone%20Strike%20In%20Libya%20Subject%20Of%20Recent%20United%20Nations,the%20air%20in%20March%202020 (accessed August 11, 2021).

[3] Michael Safi, Julian Borger, "How did oil attack breach Saudi defences and what will happen next?," *The Guardian,* September 18, 2019, https://www.theguardian.com/world/2019/sep/19/how-did-attack-breach-saudi-defences-and-what-will-happen-next (accessed August 11, 2021).

[4] Mohammed Hatem, Dana Khraiche, "Successful drone attack on Saudi Aramco in Riyadh claimed by Yemen rebels," *World Oil*, March 19, 2021, https://www.worldoil.com/news/2021/3/19/successful-drone-attack-on-saudi-aramco-in-riyadh-claimed-by-yemen-rebels (accessed August 11, 2021).

[5] Brent Kesler, "The vulnerability of nuclear facilities to cyber attack", Strategic Insights, Spring 2011

[6] "German nuclear plant hit by computer viruses," *BBC,* April 28, 2016, https://www.bbc.com/news/technology-36158606 (accessed August 11, 2021).

[7] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[8] https://www.researchgate.net/publication/280720442_Fatigue_Effects_and_Countermeasures_in_247_Security_Operations

[9] https://www.iaea.org/sites/default/files/publications/documents/infcircs/2017/infcirc908.pdf

[10] Nicolas Billecocq, "The role of drones in bolstering the operational efficiency of today's security measures," *Security Magazine,* January 26, 2021, https://www.securitymagazine.com/articles/94432-the-role-of-drones-in-bolstering-the-operational-efficiency-of-todays-security-measures (accessed August 11, 2021).

[11] For more, see https://media.nti.org/documents/THE_RISKS_AND_REWARDS_OF_EMERGING_TECHNOLOGY_IN_NUCLEAR_SECURITY.pdf.

[12] “Modernization of instrumentation and control in nuclear power plants,” IAEA-TECDOC-1016 (Vienna: International Atomic Energy Agency, May 1998), https://wwwpub.iaea.org/MTCD/Publications/PDF/te_1016_prn.pdf.

[13] “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225/Rev.5 (Vienna: International Atomic Energy Agency, 2011), http://wwwpub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

[14] Computer Security at Nuclear Facilities,” Technical Guidance Reference Manual (Vienna: International Atomic Energy Agency, 2011), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.

[15] Sinead Harvey, ‘Regulators Use Innovative Methods to Assess Safety of Radiation Sources During COVID-19 Pandemic, IAEA Survey Finds’, International Atomic Energy Agency (IAEA), 12 June 2020, <https://www.iaea.org/newscenter/news/regulators-use-innovative-methods-to-assess-safety-of-radiation-sources-during-Covid-19-pandemic-iaea-survey-finds>.

[16] IAEA, ‘The Operation, Safety and Security of Nuclear and Radiation Facilities and Activities During the COVID-19 Pandemic’.

[17] IAEA, ‘Impact of COVID-19 Pandemic on the Regulatory Activities for the Safety of Radiation Sources’, p. 2.

[18] “Committee Meetings,” https://www.un.org/en/sc/1540/about-1540-committee/committee-activities/committee-meetings.shtml.

[19] Adam Kehoe, “Explore Thousands Of FAA Drone And Unidentified Aircraft Incident Reports With Our Interactive Tool,” *The Drive,* July 14, 2021, https://www.thedrive.com/the-war-zone/41526/the-faa-has-collected-thousands-of-drone-incident-reports-our-new-tool-lets-you-explore-them (accessed August 11, 2021).

[20] “Drones and Nuclear Power Plant Security,” *United States Nuclear Regulatory Commission,* October 2020, https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-drone-pwr-plant-security.html (accessed August 11, 2021).

[21] Hernandez, “A Military Drone With A Mind Of Its Own Was Used In Combat, U.N. Says.”

[22] U.S. Department of Energy, Technology Readiness Assessment Guide (Washington, D.C.: DOE, September 15, 2011), https://www.directives.doe.gov/directives-documents/400-series/0413.3-EGuide-04-admchg1/@@images/file (accessed August 11, 2021).

[23] United States Nuclear Regulatory Commission (Office of Nuclear Security and Incident Response), *Protecting Our Nation: A Report of the U.S. Nuclear Regulatory Commission* (Rockville, MD: United States Nuclear Regulatory Commission, 2015), https://www.nrc.gov/docs/ML1523/ML15232A263.pdf (accessed August 11, 2021).

[24] International Atomic Energy Agency, “IAEA Nuclear Security Series No. 10: Development, Use and Maintenance of the Design Basis Threat,” 2009, (Vienna: International Atomic Energy Agency, 2009) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf (accessed March 3, 2021).

[25] International Atomic Energy Agency, “IAEA Nuclear Security Series No. 10: Development, Use and Maintenance of the Design Basis Threat,” 2009, (Vienna: International Atomic Energy Agency, 2009) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf (accessed March 3, 2021), pp. 27-28.

[26] International Atomic Energy Agency, “IAEA Nuclear Security Series No. 10: Development, Use and Maintenance of the Design Basis Threat,” 2009, (Vienna: International Atomic Energy Agency, 2009) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf (accessed March 3, 2021), p. 28.

[27] International Atomic Energy Agency, “IAEA Nuclear Security Series No. 10: Development, Use and Maintenance of the Design Basis Threat,” 2009, (Vienna: International Atomic Energy Agency, 2009) https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf (accessed March 3, 2021), pp. 27-28.

[28] Citation needed for this…

[29] Joint Statement on Sustaining Action to Strengthen Global Nuclear Security Architecture by Nuclear Security Contact Group, April 5, 2016, http://www.nscontactgroup.org/joint-statement.php (accessed August 11, 2021).