THE RISKS AND REWARDS OF EMERGING TECHNOLOGY IN NUCLEAR SECURITY

Nickolas Roth[*]

Project on Managing the Atom, Belfer Center for Science and International Affairs
Harvard Kennedy School

February 2020

I. Introduction

Nuclear security is never finished. Nuclear security measures for protecting all nuclear weapons, weapons-usable nuclear materials, and facilities whose sabotage could cause disastrous consequences should protect against the full range of plausible threats.[1] It is an ongoing endeavor that requires constant assessment of physical protection operations and reevaluation of potential threats. One of the most challenging areas of nuclear security is how to account for the impact–positive and negative—of non-nuclear emerging technologies. The amended Convention on the Physical Protection of Nuclear Material (amended CPPNM) states it should be reviewed in light of the prevailing situation, and a key part of the prevailing situation is technological evolution. Therefore, the upcoming review conference in 2021, as well as any future review conferences, should examine the security threats and benefits posed by emerging technologies.

As security environments change, organizations responsible for the physical protection of nuclear weapons, weapons-usable nuclear materials, and nuclear facilities must adapt to new and evolving threats. Doing so involves regular assessments to determine at what point adoption of novel technology by adversaries requires reexamination of physical protection arrangements. Also, as new technologies become available to nuclear facilities, those in charge of physical protection systems must determine how, and whether, to incorporate them into their operations. The benefits of incorporating these technologies must be weighed against any increased risk resulting from their creation of new vulnerabilities. There are important lessons to be learned from how nuclear security practitioners have incorporated novel technologies into their nuclear facility operations and how they have assessed novel technologies in the hands of adversaries.

All of these activities are more effective if done with cooperation between operators, regulators, and governments. Given the pace of technological change, these discussions must be part of a regular cycle of assessment of security implementation and cooperative dialogue.

---

[*] Nickolas Roth is a Senior Research Associate at the Belfer Center's Project on Managing the Atom. Before coming to Harvard, he spent a decade working in Washington, D.C., where his work focused on arms control and nonproliferation policy. Mr. Roth has written dozens of articles on nuclear security, nonproliferation, and arms control. His work has appeared in or been cited by newspapers around the world. Roth is also a Research Fellow at the Center for International and Security Studies at the University of Maryland.

[1] See Matthew Bunn, Nickolas Roth, Will Tobey, "Protecting nuclear materials and facilities against the full spectrum of plausible threats," paper presented at Conference on Physical Protection of Nuclear Material and Nuclear Facilities, 2017, https://scholar.harvard.edu/files/matthew_bunn/files/bunn_protecting_nuclear_materials_and_facilities_against_the_full_spectrum_of_plausible_threats.pdf.

As new technologies emerge, nuclear security practitioners can learn three critical lessons from past experiences. First, emerging technologies demonstrate the need for states and operators to maintain a regularly updated and forward-thinking design basis threat (DBT) based on a thorough assessment of threats that an operator could face. Second, emerging technologies, if used judiciously, can be an important tool for strengthening nuclear security. Third, emerging technologies illustrate the need for international cooperation to strengthen nuclear security. This paper will use case studies to illustrate each of these lessons.

II. What Is an Emerging Technology?

There are many definitions for what should be considered an emerging technology. Definitions of emerging technologies focus far more on the concept of emergence than technology. One simple definition, which is a distilled interpretation of a fairly comprehensive explanation, would be, "a technology that could have a significant impact on nuclear security operations within a relatively short time span."[2] This paper will focus on three case studies over the past decade: drones, modelling and simulation tools, and digital technology from the point of view of offense and defense.

III. Protecting Against Emerging Threats: Drones

Most states with nuclear weapons, weapons-usable nuclear material, and major nuclear facilities have a formal process for determining the threats against which operators must design their security systems to protect, called a DBT, or, for lower-consequence facilities and materials, a threat assessment. Unfortunately, because there is no international agreed-upon standard, there are significant variations in the threats states deem credible.

Assessing how emerging technologies impact threats is one of the most challenging areas for threat assessment. Countries are frequently slow to respond to the adoption of emerging technologies by adversaries, even when new capabilities have been demonstrated or are on the horizon. As a result, DBTs frequently lag behind actual threats. A good example for this problem is how the United States has addressed the growing threat of unmanned aerial vehicle (UAV) technology (also known as drones, or unmanned aerial systems or UAS).

UAVs are not a new technology. The current trends in UAV technology are advances in hardware, image processing and recognition, and artificial intelligence, along with declining costs. Every year, commercially available UAVs are able to carry more, fly faster and farther, and carry out sophisticated tasks with less and less human input.

UAVs are becoming increasingly common industrial tools, including in the nuclear sector. The U.S. Federal Aviation Administration estimates there are more than 1.5 million aerial drones in the United States alone. That number is expected to grow to more than 2.2 million over the next five years.[3] Drones

[2] Daniel Rotolo, Diana Hicks, Benjamin Martin, "What is an Emerging Technology?," February 11, 2015, https://ssrn.com/abstract=2743186. Alan L Porter, J David Roessner, Xiao-Yin Jin, and Nils C Newman, "Emerging technology: Measuring national 'emerging technology' capabilities," *Science and Public Policy*, volume 29, number 3, June 2002, pages 189–200, https://academic.oup.com/spp/article-abstract/29/3/189/1707115?redirectedFrom=fulltext.

[3] Andrew Meola, "Drone market shows positive outlook with strong industry growth and trends," *Business Insider,* 2017.

can be extremely useful tools to supplement and augment nuclear security systems. They can be used for surveillance of facilities and transportation operations and, with remotely operated weapon systems, for direct engagement with attacking forces.

Unfortunately, drones can, and increasingly are, also used by adversary forces. The number of security incidents at nuclear facilities involving drones is increasing every year. In 2014, multiple sophisticated drones flew into the restricted airspace of 13 French nuclear power plants.[4] In 2016, there were a dozen reported drone cases related to the Savannah River Site in South Carolina, where more than ten tons of weapons-usable plutonium are located.[5]

These flyovers are likely an ominous signal of things to come. Adversaries are increasingly using drones in combat situations, in some cases targeting heavily-protected facilities. The Islamic State has used drones for a number of purposes, including dropping grenades, suicide bombing, flying decoys, and intelligence gathering. In Ukraine, drones equipped with grenades—likely supported by the Russian government—have been used to destroy ammunition dumps, dramatically increasing the drone's destructive capability. A 2019 United Nations report noted that Houthi forces in Yemen have begun deploying extended range UAVs "with a top speed of between 200 km/h and 250 km/h" and which may have a maximum range of between 1,200 km and 1,500 km, depending on wind conditions" with a payload of about 18 kg.[6]

The 2019 attack on a Saudi Arabian oil processing facility is the latest and most alarming in a series of escalating drone-related incidents. A burgeoning capability is to use swarms of UAVs to overwhelm and attack critical infrastructure. According to officials, the attack involved "at least 20 drones and several cruise missiles" to conduct precision strikes on 17 targets disabling half of Saudi Arabia's oil production.[7] It is unclear what level of automation was involved in this attack or whether it was carried out by Houthi rebels or a government demonstrating the additional problem of attribution presented by drones. As software improves it may soon become possible for a limited number of adversaries to control a larger group or swarm of drones attacking together. While the 10,000 drones flying in formation to form the Olympic rings at the 2018 Olympics were pre-programmed, not reacting to their environment, they illustrate the potential for swarms of autonomous drones.

The debate on UAVs is by no means settled. Some continue to argue that the threat drones with small explosives pose to nuclear plants is insignificant because buildings are constructed with hardened concrete. On the other hand, others argue that drones can be used to target individual guards, create distractions, or disrupt critical systems.

---

[4] Maïa de la Baume, "Unidentified drones Are seen above French nuclear plants," *New York Times*, November 3, 2014, https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html.

[5] Thomas Gardiner, "Possible drone spotted over SRS," *Aiken Standard,* September 21, 2017, https://www.aikenstandard.com/news/possible-drone-spotted-over-srs/article_e71fcfe4-9f16-11e7-a9c4-831187e0bdbb.html.

[6] United Nations, "Final report of the panel of experts on Yemen," S/2019/83, New York (2019), https://undocs.org/en/S/2019/83.

[7] Natasha Turak, "Detailed satellite photos show extent of 'surgical' attack damage to Saudi Aramco oil facilities," *CNBC*, September 17, https://www.cnbc.com/2019/09/17/satellite-photos-show-extent-of-damage-to-saudi-aramco-plants.html.

The U.S. Department of Energy's (DOE) Inspector General identified in April 2019 that the "Department has not made a threat determination on UAS utilizing the most current information pertaining to UAS capabilities; therefore, the Department may not have effective controls in place to address such encounters" and recommended the DOE "make a determination on the criticality of UAS threats and ensure that the Department uses the appropriate process to update security controls based on the most recent information available concerning UAS capabilities."[8] That same report notes that changing security orders within some facilities within the DOE can take up to seven months and implementing those orders will take several years, but there does appear to be some positive progress. According to one account, DOE's DBT currently includes 1 drone with up to 10 lbs. of explosives in its payload.[9]

Meanwhile, the U.S. Nuclear Regulatory Commission (NRC) has taken a different approach toward UAV threats. In November 2019, after reviewing the issue for two years, the NRC decided to not require owners of U.S. nuclear power plants or processing plants to defend against UAVs. The NRC argued that the facilities under its purview "do not have any risk-significant vulnerabilities that could be exploited using UAVs and result in radiological sabotage, theft of special nuclear material (SNM), or substantial diversion of SNM. Similarly, the staff has determined that information gained from UAV video surveillance of an NRC-licensed facility is bounded by the type of information that could be provided by the knowledgeable insider currently permitted in the DBTs"—a decision that was roundly criticized by independent analysts in the United States.[10] Some countries, by contrast, have already begun incorporating UAVs into their security exercises. In 2017, at the Ikata Nuclear Power Plant in Ehime Prefecture, Japan, conducted its first counterterrorism drill to simulate a UAV attack on a nuclear facility.[11]

The U.S. approach to physical protection against drones at nuclear facilities demonstrates that it is difficult to convince nuclear security practitioners that facilities need to protect against emerging technological threats, even when there is significant evidence supporting the need to do so. Moreover, even in cases where an organization is proactive in addressing threats, facilities may remain vulnerable simply because it can take a considerable amount of time to incorporate new security measures.

Adversaries will continue to develop new capabilities as they become proficient with emerging technologies.[12] Additive manufacturing could dramatically increase the ability of adversaries to produce small, inexpensive UAVs. Advancements in artificial intelligence could lead to the use of autonomous attack drones by adversaries. The internet is now being used as a tool for the rapid and clandestine

[8] Office of the Inspector General, "Low altitude airspace security over select Department of Energy sites," (Washington, DC: US Department of Energy, 2019), https://www.energy.gov/sites/prod/files/2019/04/f62/DOE-OIG-19-27_0.pdf.

[9] Based on discussions from Institute of Nuclear Materials Management and Harvard University "Workshop on Emerging Issues in Nuclear Security," Monday, August 5, 2019.

[10] "NRC decision leaves U.S. nuclear plants vulnerable to terrorist drones," (Washington, DC: Union of Concerned Scientists, November 2019), https://www.ucsusa.org/about/news/nrc-decision-leaves-nuclear-plants-vulnerable-terrorist-drones.

[11] "First counterterror drill for drone attack held at nuclear plant in Ehime," *Japan Times*, June 19, 2017, https://www.japantimes.co.jp/news/2017/06/19/national/first-counterterror-drill-drone-attack-held-nuclear-plant-ehime/.

[12] For more, see T.X. Hammes, "Technology Converges; Non-State Actors Benefit," *Governance in an Emerging New World*, Issue 319, February 25, 2019, https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

radicalization of violent insiders, presenting a threat that most personnel reliability programs have been unable to address.

It will, therefore, be increasingly important for nuclear security practitioners to improve their ability to assess and respond to threats. Some threats develop in weeks, not years, requiring a more nimble and flexible approach to DBT development. Any increased responsiveness, however, must be balanced with some level of stability to help regulators and operators make long-term plans and investments without endless cost increases and uncertainty.

IV. Judicious Use of Emerging Technology Enhances Nuclear Security: Modelling and Simulation

Over the past several decades, there have been significant advances in security technology. For example, the incorporation of e-field, microwave, and infrared intrusion detection systems has enhanced surveillance and monitoring capabilities. Emerging technologies can, if used judiciously, be an important tool for strengthening security at nuclear facilities, but understanding their strengths and limitations, as well as if they introduce new vulnerabilities, is critical. The adoption of tools for modelling and simulation (mod/sim) of nuclear security systems over the past few decades are a perfect example.

Like many emerging technologies, modelling and simulation are not new, but the technique is being used in new and innovative ways. Beginning in the 1970s, mod/sim has been used to determine the likelihood and response times for detecting and delaying an adversary to assess the impact of security arrangements on operations and to evaluate and train personnel at U.S. nuclear facilities.[13] Today, advancements in computing power create new opportunities to use modelling and simulation to better understand how potential adversaries might try to get through nuclear facility defenses. Mod/sim tools can assess more scenarios, in more depth, and faster than ever before.

When used in conjunction with other performance testing and vulnerability assessment strategies—like realistic force-on-force exercises—modern, advanced, computer-based modelling and simulation technology can identify weaknesses and strengthen physical protection systems. They can also help security forces think about new adversary and response tactics, predict adaptive adversary and defender tactics, and fight complacency. Overreliance on this technology, however, can sometimes lead to a misleading level of confidence in the security at a nuclear facility.[14]

For mod/sim to be used effectively, nuclear security practitioners need to be aware of its strengths and weaknesses. First, there are significant uncertainties. Models and simulations are based on the collection of data, but it is impossible to accurately predict the number of adversaries that will attack a facility and the capabilities and tactics they will use, or the weaknesses they will exploit, or how security teams will actually respond in real life. Nor, in most cases, do we fully understand what the consequences could be. Hence, models should not be relied on to make absolute judgments about levels of remaining risk. Second, with mod/sim it is extremely difficult to accurately model how an organization and the people within it behave on a day-to-day basis, or in the event of an emergency. Third, models only consider scenarios that security practitioners anticipate. Adversaries attempting to

[13] "Modelling and Simulation for Nuclear Security" (Vienna: World Institute for Nuclear Security, 2013).
[14] Matthew Bunn, "Modeling of nuclear security: Use the tool, but remember its limits," (presented at Institute of Nuclear Materials Management/Managing the Atom workshop on Emerging Issues in Nuclear Security, Cambridge, 2019), https://scholar.harvard.edu/matthew_bunn/other-nuclear-security-issues.

steal from heavily guarded non-nuclear facilities often manage to defeat defenses with approaches security practitioners did not anticipate. Fourth, current modelling technology is not as good at modelling insider threats as it is in modelling outsider engagements. Insiders benefit from having long periods of time to observe and plan to defeat security systems, sometimes being able to have a more accurate understanding of vulnerabilities than models have. Moreover, modelling and simulation technology is only beginning to address blended attacks involving a combination of tactics like cyber and physical attacks or UAV and ground attacks.

Understanding the scenarios where mod/sim would not be a helpful tool for determining the results of an adversary scenario is critical. One famous example is the 2012 break-in at the Y-12 nuclear weapons facility. Early in the morning on July 28, when it was still dark, an 82-year old nun and two other protesters broke into the Y-12 nuclear weapons production facility. Equipped with hammers, paint, blood, and a pair of bolt cutters, they cut through four fences— three which were equipped with intrusion detectors—setting off alarms, and traversed a 600-meter semi-wooded area until they arrived at the wall of a building housing hundreds of tons of HEU. They painted blood on the walls and pounded on the building with their hammers, before finally being accosted by a single guard.

The subsequent investigation of the incident by the DOE Inspector General revealed a spectacular collapse in Y-12's security culture. For example, a newly installed intrusion detection system was setting off ten times the normal number of false alarms. Ordinarily, the guard at the central alarm station would use cameras to check to see if there was a real intruder, but the cameras had been broken for months. Fixing the cameras was not a priority because there was an assumption that the guards would check out the situation if the alarm went off. Managers did not anticipate that the guards would grow complacent because of too many false alarms. The heavily armed guards inside the facility heard the hammering and thought it might be construction they had not been told about, even though it was before dawn, and did not bother to check.[15]

The Y-12 incident demonstrates the limitations of mod/sim. Although a model and simulation of such a scenario could have been created, some scenarios—like a staggering systemic collapse of security—would almost certainly be dismissed as too implausible to take seriously—though such scenarios could be used to educate security forces. Moreover, while it would have been possible to develop a simulation where guards don't respond and cameras don't work, it would have been extremely difficult to model the organizational factors that led to that situation existing. The Y-12 case shows that many modern-day technologies like cameras and intrusion detection are only as good as the people using them.

Over the next decade, the incorporation of the Internet of Things; smart cameras; facilities integrated with national and international intelligence data; facial recognition software; remotely operated weapons, among others, have the potential to significantly enhance the ability of security systems to detect and assess threats.[16] While these emerging technologies may be important tools for nuclear

[15] For a detailed account of the incident, see Office of the Inspector General US Department of Energy, Inquiry Into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex, DOE/IG-0868 (Washington, D.C.: Department of Energy, August, 2012); http://energy.gov/sites/prod/files/IG-0868_0.pdf, p. 14.

[16] For more, see Richard P. Rosano, "The Future of Nuclear Security," paper presented at the IAEA International Conference on Nuclear Security, December 8, 2016.

security, they are not a substitute for intelligent, motivated security personnel constantly on the look-out for vulnerabilities and ways of improving facility operations.

V. International Cooperation Mitigates Risks and Maximizes Rewards: Cyber Attacks

As this paper illustrates, effective national governance of emerging technologies is extremely difficult. Technological evolution and revolutions occur far faster than the development and implementation of government regulations. This is one of the reasons why nuclear security is more effective when countries work together to strengthen it.

Countries are better equipped to take advantage, or reduce the risks, of emerging technologies if they are sharing information on best practices, lessons learned from mistakes, and new advances in research and development. There are numerous examples where countries have worked together, sometimes with the support of international organizations and groups, to determine how best to address emerging technologies. One of the most prominent examples of cooperation over the past decade has been around the incorporation of digital technology around the world and the race to mitigate the growing risk of cyber attacks.

The international cooperation around the incorporation of digital technology into nuclear power plants has been a gradual process for more than two decades. In 1998, the International Atomic Energy Agency (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. The report also acknowledged that emerging digital technologies present new dangers to the nuclear sector, "unauthorized access can not only jeopardize the safety of the plant but also availability. Therefore, a plant policy must be defined consistent to the security policy of the utility."[17]

Cyber attacks can be used to sabotage a nuclear facility, as was the case with the Stuxnet virus that damaged centrifuge cascades in Iran. Conceivably, this kind of attack could also have the effect of creating a large radioactive release. A cyber attack could also be part of a blended attack where the disruption of an alarm or monitoring system could be used to assist in theft of nuclear material. A cyber attack could be used to access sensitive information at a nuclear facility that could provide valuable insight to would-be attackers on how to defeat security systems. It can also be used to gain sensitive information about nuclear facility employees. According to the 2019, Worldwide Threat Assessment, "Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims."[18]

As adversaries are becoming increasingly familiar with cyber tactics and more capable of taking advantage of vulnerabilities, the frequency of cyber security incidents at nuclear facilities is increasing.[19] In 2014, malware was introduced into a computer at the Monju Nuclear Power Plant in Japan during a

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

[18] Daniel R. Coats, "Worldwide Threat Assessment 2019," Statement for the Record, January 29, 2019.

[19] For a discussion of the growing cyber threat to nuclear facilities, see Alexandra Van Dine, Michael Assante, and Page Stoutland, *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities* (Washington, D.C.: Nuclear Threat Initiative, 2016), https://www.nti.org/media/documents/NTI_CyberThreats__FINAL.pdf.

routine software upgrade.[20] Company-sensitive emails, employee data sheets, and training logs were stolen. The same year, Korea Hydro and Nuclear Power offices in South Korea were hacked resulting in the release of technical information. In 2016, two viruses infected a German nuclear power plant's monitoring systems. None of these incidents involved control systems or resulted in radioactive release, but there are realistic cyber attack scenarios where the outcome could be much worse. One recent study demonstrated how an adversary could access closed circuit cameras and Bluetooth devices to infiltrate local networks, which would allow the adversary to disable security systems and compromise nuclear instrumentation and control equipment.[21]

Aware of this growing danger, international leaders have been engaged in a significant international effort to make cyber security a nuclear security priority. This effort included direct cooperation between states and cooperation through international organizations and groups.

The IAEA has been one of the key organizations helping to strengthen cyber security at nuclear facilities. Its nuclear security guidance document, Information Circular 225, first referenced cyber security in its fifth revision in 2011, stating "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g., cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat."[22] That same year, the IAEA printed a technical guide on *Computer Security at Nuclear Facilities*.[23] The IAEA has also held nuclear security trainings for member states.

In the next few years after 2011, there was a steady increase in international work in this area. In 2013, the United States and Russia agreed to "the regular exchange of practical technical information on cybersecurity risks to critical systems," including a continuous exchange of "technical information about malware or other malicious indicators, appearing to originate from each other's territory, to aid in proactive mitigation of threats."[24] Three years later, at the 2016 Nuclear Security Summit, nearly 30 countries signed a joint statement on cyber security at nuclear facilities in which they pledge to "ensure adequate cyber security at industrial control and plant systems at nuclear facilities."[25] In 2018 alone, the

[20] Pierlugi Paganini, "Malware Based Attack Hit Japanese Monju Nuclear Plant," Security Affairs, January 10, 2014, http://securityaffairs.co/wordpress/21109.
[21] Rodolfo Quevenco, "Secure Computer Systems Essential to Nuclear Security, Conference Finds," (Vienna: International Atomic Energy Agency, June 8, 2015), https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds.
[22] "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," INFCIRC/225/Rev.5 (Vienna: International Atomic Energy Agency, 2011), http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.
[23] "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.
[24] "U.S.-Russian Cooperation on Information and Communications Technology Security" (Washington, DC: The White House, June 17, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.
[25] Debak Das, "Most recently, in 2019, there was a cyberattack on the Kudankulam Nuclear Power Plant in Tamil Nadu, India in which data was stolen from the plant's administrative network," *Washington Post*, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

IAEA convened four international training courses, two regional workshops, and two technical meetings with representatives from dozens of member states all focused on cyber security.[26]

The impact of these activities is unclear. Over this same period, however, many states have incorporated protection against cyber attacks into their nuclear security requirements. Between 2011 and 2012, Japan approved changes to its nuclear security rules that included requirements for cybersecurity. In progress reports at the 2016 Nuclear Security Summit, Finland announced it was revising its national DBT to include cyber threats; Hungary announced that it had already made such a revision; and the Netherlands announced that it was implementing a new DBT, which would be updated to account for cyber threats.[27]

VI. Looking Forward

While there has already been significant cooperation in the areas of cybersecurity, there are many opportunities for greater collaboration on issues related to emerging technologies. International forums provide opportunities for states to share information about operating experience, best practices, and lessons learned from actual security incidents.

States could engage directly through bilateral engagement, as in the case of U.S.-Russian cooperation. Additionally, international organizations or groups like the IAEA, the Global Initiative to Combat Nuclear Terrorism, or the Nuclear Security Contact Group can facilitate information and best practice exchanges. Regional structures, such as the Association of Southeast Asian Nations Nuclear Forum, offer another platform, as does the International Network for Nuclear Security Training and Support Centres.

Legally binding agreements like the amended CPPNM also provide opportunities for cooperation. The upcoming review of the amended CPPNM in 2021 is another critical opportunity to discuss emerging nuclear security technologies. The text of the amendment states that the conference should include a review of the conventions 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.[28] Additionally, over the next year, the IAEA could appoint an independent advisory group to provide assessments of emerging technologies to be discussed at the review.

[26] International Atomic Energy Agency, Nuclear Security Report 2019, GOV/2019/31-GC(63)/10, Vienna (2019),
[27] "Highlights of National Progress Reports," Nuclear Security Summit 2016 website, http://www.nss2016.org/news/2016/4/5/highlights-from-national-progress-reportsnuclear-security-summit.
[28] The International Atomic Energy Agency's action plan from the 2016 Nuclear Security summit endorses "regular review conferences." See "Action Plan in Support of the International Atomic Energy Agency" (Washington, D.C.: International Atomic Energy Agency, April 1, 2016).