Wilton Park

Image: Fornaxus

Report

Nuclear security architecture: identifying emerging challenges and opportunities

Monday 26 – Wednesday 28 June 2017 | WP1554

In association with:

Department for
Business, Energy
& Industrial Strategy

Wilton Park

Report

Nuclear security architecture: identifying emerging challenges and opportunities

Monday 26 – Wednesday 28 June 2017 | WP1554

Executive summary

In association with the UK Department for Business, Energy and Industrial Strategy, and with support from the UK Foreign and Commonwealth Office, Wilton Park convened a three-day conference exploring the potential risks and opportunities facing today's international nuclear security architecture. The conference opened with no proposed conclusions, but rather an overarching question: Is the nuclear security architecture able to respond to emerging threats to and opportunities for nuclear security and if not, how can it be reconfigured to do this?

Seeking opinions and recommendations from a wide range of participants - inside and outside of both government and the nuclear security community - the conference primarily centred around the nature of change and how well the nuclear security architecture is prepared to adapt to it. As such, each discussion explored horizon-scanning trends and techniques from multiple sectors, with the ultimate aim of creatively addressing the central research question.

Among other things, the conference explored:

- The nature of change, specifically examining the adaptability of the nuclear security architecture when responding to emerging threats.
- The strengths and weaknesses of specific entities within the global nuclear security regime.
- The role of the International Atomic Energy Agency (IAEA) within the global nuclear security regime, and the roles of the member states within the IAEA and other organisations.
- Strategies for reducing political inertia and strengthening political will.
- How lessons from other sectors and industries can be applied to strengthening the global nuclear security architecture.

The nature of change

1. Change itself is constant, but the pace of change is intensifying. This change can be tracked through political, social, and technological lenses.
2. Political change: Non-state actors are constantly adapting and are increasingly numerous. Not all are malicious, with many large corporations expected to wield significant political influence in the coming decades. On the other hand, those which are malicious are seemingly less constrained by moral qualms. It is plausible that terrorists will seek to disrupt society through weapons of mass effect if conventional attacks fail to serve their ultimate goals. Additionally, the roles and responsibilities of state actors are expected to diminish as the world becomes increasingly globalised and unpredictable, as episodic and dramatic political changes will affect the ability of states

to meet their obligations to their citizens.

3. Social change: Social media is changing the methods of communicating and collecting information, which can have a significant effect on the efficacy of nuclear security strategies. As demonstrated by a 2016 pilot project, conducted by the James Martin Centre for Nonproliferation Studies (CNS) in Moldova, social media can be used to facilitate the tracking of orphaned and legacy radioactive sources. However, social media follows the natural trend of technological innovation, in that it can be used for both benign or malicious intent. As such, adversaries could feasibly utilise similar tracking techniques with the intent of undermining the global nuclear security regime.

4. Technological change: Advances in 3-D printing, unmanned aerial vehicles (UAVs), and computer security all pose significant proliferation concerns. Additionally, electronic trading platforms like Alibaba and eBay offer new methods of acquisition for malicious actors. However, many necessary conversations about technological threats remain unaddressed out of technological fear, 'sci-fi' thinking, and political inertia.

How adaptable is the nuclear security architecture?

5. Despite the staggering pace of change, bureaucratic challenges and a lack of consensus have kept the nuclear security regime mired in a state of inertia. The sense is that the regime, as the common refrain goes, is 'preparing to fight the last war.' A number of challenges currently face the global nuclear security architecture, discussed below:

6. The IAEA is the core of the global nuclear security architecture. However, the IAEA is akin to a slowmoving cruise ship with 168 captains; it does not turn easily. Cooperation and consensus among member states is required in order to prevent stasis and to keep the ship on course. This consensus is often difficult to find amid politically-charged debates over disarmament, security culture and verification, among other issues. However, the technically-focused mandate of the IAEA offers an opportunity for such consensus; de-politicising the work of the Agency whenever possible offers a chance for common ground.

7. The nuclear security pillar of the IAEA is neither emphasised nor implemented equally across all member states. Despite its global ramifications, many states do not see nuclear security as their concern, especially those holding little or no weapons-usable nuclear materials. The states which consistently seek to address the issue of nuclear security are, for the most part, the same ones which attend international nuclear security conferences and workshops.

8. The sheer number of stakeholders is staggering. Political representatives, academics, think tanks, industry, scientists, and many others all have valuable input to contribute. However, the challenge lies with fostering cooperation and consensus among these very different groups. It is the responsibility of government representatives to provide the necessary regulatory framework to promote such coordination.

9. In the nuclear security field, information exchange involves a critical tradeoff. On the one hand, transparency is crucial in order to strengthen cooperation and work effectively; however, on the other hand, too much public information could enable proliferation or present targets to adversaries.

10. Traditional defence and denial efforts are often focused on outsiders, not insiders; however, the insider threat remains the greatest nuclear security risk, and this requires a change in security and organisational culture. The challenge lies in finding a balance between improving security culture and not disrupting employee relations or trust. Fostering suspicion amongst employees or attaching stigma to broken security practices could create a collective sense of disgruntlement - one of the greatest insider motivations - thus instigating a spiral. Additionally, common background checks do not account for specific risks (e.g. individuals being blackmailed).

11. Improving nuclear security is a slow and technically-focused process, but national leadership always wants rapid and politically-focused results. Political attention span is short, especially because of quick four-year term averages. Therefore, political resilience, commitment, and will at all levels – but especially at the very top - is paramount, and not always easy to find.

12. The IAEA is the centre of gravity for the nuclear security regime; however, the real power lies with individual member states. States must continue to ask themselves how they can best stay abreast of emerging and potentially destabilising technologies; how they can account for new and changing forms of communication on nuclear security; and how they can develop good nuclear security practices to address both of these concerns. At the IAEA's 60th General Conference, Resolution 10 (OP 4) on nuclear security 'encourages the Agency to enhance its technical capabilities and keep abreast of scientific and technological innovations with a view to confronting current and evolving challenges and risks to nuclear security.' However, while the IAEA provides states with a framework for technical guidance, the Agency is not in the business of assessing threats, which can often be coupled with political consequences. For this reason, the IAEA would prefer to support member state initiatives to promote open information exchange and international coordination on these technical matters.

Lessons from other sectors

13. Biosecurity faces many of the same challenges as the nuclear security field, albeit with even less resources. When addressing the risks of emerging technologies, the biosecurity sector has found success in tracking technological developments over time, rather than assessing individual biodevelopments. This big-picture focus also enables a focus on future public health benefits, rather than just immediate threats.

14. Previous eras of cyber security took wholly technological (until the early 2000s) or data-centric (until early 2010s) approaches to risk management. After the failures of these methodologies, best practices in cyber security have focused upon an organisational approach, in which technological and data-driven responses form only part of the risk management process. This new cultural shift is outcome-driven rather than process-driven, and attempts to eliminate 'tick-box mentality' through establishing a productive security culture within the industry.

15. Radiological security initiatives have found success through eliminating resistance to change, piece by piece. Typically, such initiatives will hit political, technological, and financial walls prior to implementation; however, addressing each individual concern serves to remove a piece of the wall. Eventually, the removal of enough bricks will cause these barriers to crumble, and the initiative can be more easily implemented. For example, US-led security initiatives to reduce the global use of cobalt-60 in cancer treatments have been met with resistance because alternative technologies, such as linear accelerators (LINACs), require reliable electricity, training, and servicing. With this in mind, the IAEA, the European Organization for Nuclear Research (CERN), and other groups are working towards reducing the complexity and cost of LINAC systems, hoping that global implementation can be achieved by removing these technological barriers. This approach centres around convincing policymakers that the same outcome can be achieved with less risky technology, thereby reducing the disincentives for change.

16. It is important to note that despite the political, social, and technological upheavals described above, the big picture strategy for nuclear security has not changed: to protect and prevent the unauthorised removal or sabotage of nuclear material, while the greatest threat to nuclear security still remains the insider. The following recommendations, drawn from focused breakout sessions on improving the existing security architecture, devising new initiatives, and practical implementation, seek to address these points.

Recommendations

The following recommendations, which were made by workshop participants, addressed the main topic of the workshop: "how to identify and address emerging and evolving challenges". Recommendations do not necessarily reflect the consensus or majority view of all workshop participants.

17. Examine existing IAEA nuclear security architecture (e.g. AdSec, Nuclear Security Guidance Committee (NSGC)) to identify how identifying and addressing emerging and evolving challenges could be integrated into IAEA nuclear security planning and activities.

18. Create or task an open-source information analysis group to conduct horizon-scanning work on nuclear security risks. This would allow a multilateral and independent third party group to conduct unbiased nuclear futures work. This initiative could follow the model of the EU Non-Proliferation Consortium (which does similar work on WMD proliferation). This would allow a multilateral and independent third party group to conduct unbiased futures work on nuclear security.

19. Use the nuclear security architecture to promote senior level scenario-based policy discussions, to be held at national, regional, and international levels. Rather than just focusing these discussions on a first-responder level, this is a good way of educating and getting buy-ins from senior policymakers. Additionally, the Global Initiative to Combat Nuclear Terrorism (GICNT), INTERPOL, and the IAEA could conduct joint exercises for states relating to incident response, which would integrate law enforcement efforts on both the first-responder and national levels.

20. Improve coordination and collaboration by inviting IAEA member states to attend the information sharing session of the Information Exchange Meeting (IEM), and share a comprehensive report of each IEM with all participating initiatives and their respective members. This action would address the existing information-sharing weaknesses between initiatives, as at present, information does not often spread easily and typically takes the form of oversimplified one-page briefs. There is no risk of 'selfproliferation,' as no real nuclear security data would be shared; however, practical concerns remain over costs and the potential perception of imposing obligations on member states.

21. The International Network for Nuclear Security Training and Support Centres (NSSC Network) could organise regional discussions to identify new and emerging threats and trends, and report back to the network for dissemination. This would serve to address threats through a regional approach and could improve collaboration between localised groups of states.

22. Expand the mandate of the Centres of Excellence (CoEs) to further emphasise on-site, in-country training with distance learning (e.g. webinars) and social media support. Additionally, train additional in-country trainers who can continue the process and 'up-skill' themselves online.

23. Provide repeated peer reviews, as distinct from one-off initiatives, to allow facilities to regularly and confidentially test security procedures using outside experts. This could be accomplished by hiring external red-teaming contractors, or by applying the US Department of Energy's model, in which different organisations within the same department will red-team each other, thus mitigating the risks to both security and confidentiality.

24. Promote external horizon-scanning studies for emerging technologies and other areas in need of further exploration, including 3-D printing, UAVs, computer security, machine learning, automation, the dynamics of smuggling, the evolution of international commerce (especially intangible technologies, blockchain, and cryptocurrencies), the dark web and electronic trading platforms (such as eBay and Alibaba). The emerging technological threats of today are not always going to be relevant, so it is futile to agree

upon a definitive list. Instead, the nuclear security community should focus on understanding the nature and trends of specific technologies and disseminating that information to relevant forums and organisations.

25. Foster public-private partnerships. Financial incentives will always drive the private sector to outpace the public policy community in terms of technological innovation; however, it is advisable to involve the private sector in nuclear security issues - security culture in particular - as the members of these industries are the ones that are actually utilising these emerging technologies. The public sector can find success by setting a focused policy agenda, and pushing the private sector to achieve the stated goals. This would be very helpful in securing buy-in from political leadership, and moving technical knowledge up the political ladder.
26. Promote effective security culture through a number of concurrent initiatives: designing security into nuclear facilities before they are built; using outside evaluators for red-teaming and security testing; making use of incentives - not just punishments - to promote a healthy security culture.
27. The nuclear security community should develop a coherent response plan to potential nuclear or radiological security incidents. The immediate response to a high-profile nuclear security incident will set a precedent; a panicked or disorganised response may encourage similar targets and methods in the future.
28. Address the clear gender disparity in the nuclear security field. Promote female participation and leadership at all levels.

Other recommendations for existing challenges

The following recommendations were made by participants in the course which address existing, rather than emerging or evolving, challenges. Recommendations do not necessarily reflect the consensus or majority view of all workshop participants.

29. Establish an international clearing house for instances of cyber intrusion at nuclear facilities, building upon the concept of the US Information Sharing and Analysis Centers (ISACs). It could be housed at INTERPOL, and would be both international in scope and voluntary in mandate.
30. The creation of a ‘Plutonium Bank,’ centred around the consolidation of global civil plutonium stocks. Based on the model of the LEU Bank, this would address the issue of extant plutonium stockpiles, and would improve overall security by centralising it under international control. This could potentially usurp closed fuel cycles and would be placed under IAEA safeguards. It would have to be located in an area already containing significant plutonium stocks and where global confidence in nuclear security is high, such as in the United Kingdom or France.
31. Offer bounties for orphaned radiological sources. Although the cost of transport remains a concern, this initiative would create a market pull and would facilitate secure centralisation of these sources.

Conclusion

Given the staggering pace of change, improving the efficacy of horizon-scanning has become more important than ever. Best practices for transparency, decision-making and adaptability should be adapted from other sectors, and in the spirit of consensus the nuclear security community should focus on technical cooperation rather than political divisions. In this regard, the IAEA should be used as a tool to provide technological guidance and bring together relevant stakeholders, and should continue to be supported and strengthened by its member states. However, member states must acknowledge that they hold the keys to strengthening the nuclear security regime, and consensus among the most committed states is necessary in order to convince other states and their leaders to

take nuclear security seriously.

To that end, proactively exploring the above recommendations and continuing to convene similarly productive meetings would be significant steps in the right direction.

Matt Korda
Wilton Park | July 2017