World Institute for Nuclear Security

Evolving Threats and Advanced Security Technologies

Live Session

Thursday, 29 October 2020, 16:00-19:00 CET

Background

In 2018, WINS published a Special Report on Evolving Threats and Advanced Security Technologies. Both threats and technologies are constantly changing, and it is essential for the industry to have access to the most recent information. This online conference was designed to promote productive and interactive participation, allowing all attendees to learn from each other and improve their nuclear security practices. The findings will be used to update WINS' 2018 report.

Objectives of the Live Session of the Conference

The live session was intended to be an opportunity to review and discuss the topics covered by the on-demand sessions with selected speakers. It was also a chance for the conference participants to share their perspectives on upcoming threats and future security technologies of interest. In particular, nuclear operators' perspective on the topic was in focus in order to understand what they need to know and understand how the report can support their daily work. Finally, the live session allowed the subject matter experts and participants to consolidate inputs for the revision of the WINS Special Report.

Live Session Process

The live session was professionally facilitated by Mr Carl Reynolds with Mr Chris Behan, WINS Programme Manager.

Mr Tomas Bieda of Tetratech spoke about emerging threats and adversary capabilities before being joined by Mr John Buchanan, Interpol, and Bill McGlennon, Sellafield, for a dialogue and Q&A session.

Ms Stacey Peel of Ove Arup & Partners Ltd spoke about advanced security technologies. She was joined by Mr Matthew Talbot, RhinoCorps; Mr Chris Bishop, Ipsotek Ltd; Mr Sebastian Martinez, Nuclearis; and Mr Zhe Yuan, SNERDI, for a panel discussion and Q&A session.

Mr Rob White of Xcel Energy summarised the on-demand materials on users' experiences. He was then joined by Mr Matthew Knights of Boston Dynamics and Chris Allen of Bruce Power for a panel discussion and Q&A session.

Ms Cristina Dominguez of the Argentinian Nuclear Regulatory Authority discussed regulatory and ethical matters, followed by a panel discussion and Q&A session with Meghan Hammond, Pillsbury Winthrop Shaw Pittman LLP; Mr Duane White, US Nuclear Regulatory Commission; and Mr Geoff Moore, Ove Arup & Partners Ltd.

A total of 215 participants from North and South America, Asia, Africa, the Middle East and Europe attended the live session. The live session used various tools and formats – including expert presentations, panel discussions and participant polling – to encourage audience engagement.

Introduction

Mr Behan opened with welcome remarks, including a summary of survey results and the process for revising the 2018 WINS Special Report. He emphasised the importance of input from participants, in particular operators, on upcoming threats and future security technologies of interest. Mr Behan also noted three important findings from the pre-event survey:

- In order to reduce risk associated with today's threats and advanced technologies, regulatory and government relationships with industry and the design basis threat are key;
- The democratisation of technology is a massive problem and must be recognised and not underestimated;
- Domestic terrorism should receive as much attention as international terrorism.

Mr Reynolds then reviewed the agenda for the event and technical features of the event platform.

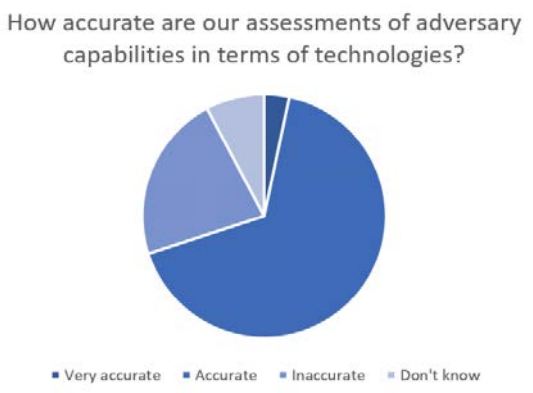
Session 1 on Emerging Threats and Adversary Capabilities

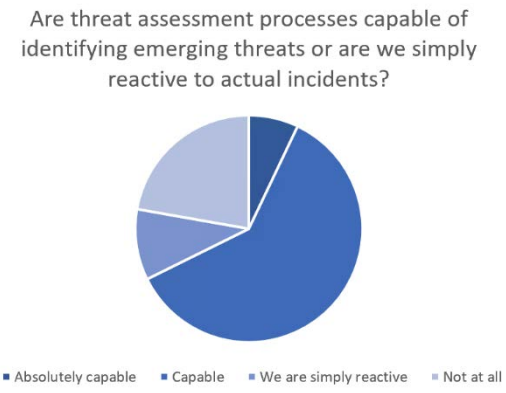
Mr Bieda is former Director of Nuclear Security Policies and Non-proliferation from the Secretary of Energy of Argentina and now works as Tetra Tech Nuclear Security Specialist Affiliated with Oak Ridge National Laboratories.

He summarised the findings of the first session on emerging threats and adversary capabilities. Mr Bieda noted that knowing the stakeholders, process for addressing threats and local situation is critical. He added that regulations and norms need to be updated to address evolving threats. Mr Bieda concluded that funding, awareness and exercises are all important components of a threat mitigation strategy.

The participants were then asked to share their views on whether threat assessment processes are capable of identifying emerging threats and how accurate assessments of adversary capabilities are.

Most participants, 60%, believed threat assessment processes are capable of identifying emerging threats, 7% said absolutely capable, 22% not at all capable, and 10% said we are simply reactive. A total of 60% of respondents characterised assessments as accurate, 3% as very accurate, 20% inaccurate and 7% didn't know.





Mr Buchanan and Mr McGlennon came on stage to discuss the results. Mr Buchanan noted that there is an overlap between preventative identification of emerging threats and a reactive response. He suggested more information sharing between operators, regulators and national police would improve accuracy.

Asked about advanced technologies in use, Mr Buchanan said criminal use of drones was increasing. Mr Bieda added that everyday technology such as 3D printers and drones could be used by a threat. Mr McGlennon referred to a hack on shipping giant Maersk that caused great disruption, noting how the knock-on effects of such incidents can be significant.

Participants noted that not all regulatory agencies have their own intelligence assessment units, which can be a challenge as the threat assessment process must be continuous. Others noted that many national agencies can contribute to threat assessments, as well as local agencies and open source information.

Another participant drew a parallel to the National Aviation Security Risk Context Statement as a valuable way to share threat-related information without compromising that data. Participants and panellists agreed that channels and mechanisms should be developed ahead of time.

The panellists also discussed strategies for addressing other risks, such as reputational risk and local criminality, and the assessment of advanced technology threats. They also discussed geographical variations on threats and threat assessments. They concluded that threat assessment work must be ongoing, cooperation is critical, and complacency must be avoided.

Session 2 on Advanced Security Technologies

Ms Peel, an aviation security specialist, presented about the content of the advanced security technology session. She noted that security technology encompasses a broad range of tools and that they are constantly evolving. She added that selecting relevant and appropriate mitigation tools is challenging and requires close consideration of a facility's circumstances and needs.

Mr Talbot noted that modelling and simulation technology provides compliance data without live testing while allowing facilities to study possible additions or modifications before making them and examine different possible threats. Mr Martinez explained that blockchain technology would enable the encryption of data on tracking devices for radioactive material, so various stakeholders can access the information while it remains protected. Mr Bishop stated that technologies should be assessed on the basis of robustness, resilience and demonstrated efficacy. Mr Zhe spoke about the potential impact of artificial intelligence and the shifting requirements of physical protection zones to account for airborne threats. He noted that operators could add new equipment without removing the old ones to facilitate regulatory approval.

Participants noted that the client may not have the commercial mechanisms that allow the introduction of innovative technologies that can improve upon an adequate solution to make it optimal. They also pointed out that the supply chain can better find the solution if the client can clearly explain the issue, and that integration with the existing security network is needed. They noted that regulator approval of solutions could pose a barrier to adopting new technologies.

Session 3 on Users' Experiences

Mr R. White reflected on the third session, which covered users' experiences. He noted that security culture remains critical and is often more important than advanced technology He added that the industry's focus on safety and security encourage operators to be conservative in adopting new technology, which he noted has advantages.

An audience poll asked participants whether nuclear organisations have a clear process in place for identifying emerging security technologies and for integrating them into their security arrangements in a timely manner. The results were equally split between agree and disagree.

Mr Knights noted that robotics technology cannot address every threat but that potential users can often find new applications when they review a new innovation, allowing it to be equipped appropriately. They also discussed the potential of artificial intelligence and drone technology for security applications. Mr Allen noted that in addition to the advantages technologies such as drones offer, the risks they pose must be considered.

Participants noted that drones could be deployed for remote surveillance/monitoring and/or communications with trespassers as many nuclear power plants are in remote locations. Participants and panellists agreed that no single technology would provide an overall solution.

The audience asked whether small modular reactors would be good for security. Mr R. White said they have an advantage as they are designed with security in mind. The reactor has security and safety features that are not reliant on human interaction.

The panellists concluded that testing new technology alongside current technology and information sharing within the industry help to ensure it performs as expected before full implementation. Offering a perspective from the aviation industry, Mr Moore noted that operators need to consider the local circumstances and supply chain when selecting technologies. Mr R. White emphasised the importance of safety and security culture in the implementation of new technologies.

Session 4 on Regulatory and Ethical Matters

Ms Dominguez presented a summary and analysis of the regulatory and ethical matters addressed in the fourth session. She pointed out that a great number of actors must be involved in implementing technological and normative solutions and that the technology is mostly dual use. She added that engaging stakeholders is the most important factor in the implementation of technological advances, and many groups should take part. She concluded that agreeing what is ethically acceptable for industry's participation in oversight mechanisms would be a key step.

Asked about how regulatory processes allow regulators to respond to emerging threats, Ms Dominguez said security frameworks would need to be adapted over time and all actors have to be involved from the beginning. Mr D. White noted that the US Nuclear Regulatory Commission has intelligence staff looking at evolving threats, so instructions could be issued to licensees as needed or the design basis threat could be modified.

Asked whether drone-specific or more general regulation was required, Mr Moore argued that blanket regulation would be ineffective. He said threat, vulnerability and risk assessments were needed to protect sites with differing circumstances and operations.

Ms Dominguez pointed out that regulations can be slow to adapt to new technologies, so performance-based requirements can be more flexible. Mr D. White said performance-based regulations in the US allow operators to receive exemptions to implement new technologies, providing proof of their performance backed up with the option of inspections.

The audience noted that after 9/11, the US Nuclear Regulatory Commission was able to address immediate threats with orders and compensatory measures that operators were required to implement while regulations were developed. Participants also noted that the commission has regularly interacted with industry to better understand their programmes and protective strategies as we develop and impose regulatory requirements.

Ms Hammond said that when technology outpaces regulation, a set of principles can allow regulatory flexibility to make the necessary modifications to meet technological developments or implement technology without specific regulation. She added that issues around data and biometric privacy would be a growing area of concern, and that transparency with regulators, employees and external employees was essential when implementing new technologies.

Ms Dominguez encouraged a focus on best practices, safety culture and security culture, adding that guidelines and education lead to improved and more efficient practices in industry. Mr D. White added that a public process allowed the regulator to gather information from industry and avoid potential issues.

Ms Dominguez concluded that good cooperation, experience sharing and assigning responsibility are essential to ensuring effective regulations and security measures. International collaboration will be particularly important to address the cross-border issues that emerging technologies raise. Mr D. White added that in addition to collaboration and transparency, a risk-informed approach is crucial for technology implementation.

Conclusion Session

In the final poll, 97% of participants said they would recommend this kind of event. Participants appreciated having the on-demand presentations in advance of the live event so they had ample time to gather their thoughts and prepare. Participants also noted that the discussions had been thought provoking and that this type of knowledge sharing is important for adapting to technology developments in the highly specialised nuclear field.

Mr Reynolds, Mr Behan and Mr Pierre Legoux closed the event, thanking the participants and speakers for their contributions. Mr Legoux noted that the Special Report on Evolving Threats and Advanced Security Technologies would be revised through the end of the year, taking into account the key findings from this online conference.