EVOLVING SECURITY THREATS AND ADVANCED SECURITY TECHNOLOGIES

WORKSHOP REPORT

19th – 21st MARCH 2018

BACKGROUND

The threat landscape has evolved—and is continuing to evolve—at an almost unimaginable pace. Cyber terrorism (perpetrated by both States and individuals) has become an enormous threat to businesses, industries and governments around the world. Political upheavals in several regions of the world (greatly assisted by the development of smart phones, internet and social media technology) have led to the rapid rise of terrorist groups using more and more sophisticated tools and weapons. Although difficult to predict on a long-term basis, the frequency and magnitude of attacks perpetrated by malicious individuals, including lone wolves and insiders from across the political spectrum, is unlikely to decline in the near- and medium-term future.

Nuclear operators and other nuclear security stakeholders are already investing significant resources to address these continuously evolving threats. Some high-risk facilities are deploying sophisticated modelling and simulation programmes, advanced biometrics, stress analysis technology, robotic guards, remotely operated weapons systems and/or automated mobile detection systems. One of the most important tools is data analytics, which enables the analysis of huge amounts of data in near real-time.

Considering the considerable time and expense involved, it is important to ask: “Do we fully understand our security expenditure and is it focused on the right things?”

Rapid changes are going to continue taking place–not only in the threat landscape, but also in the nuclear industry. In the years to come, nuclear reactors will change, including the deployment of small modular reactors, and the threats—many of which have not even been anticipated yet—will evolve. It is crucial that those with responsibility for nuclear materials understand the nature of such change and put strategies and structures in place to mitigate it.

With this in mind, WINS organised an International Workshop on “Evolving Security Threats and Advanced Security Technologies” between the 19th and 21st March 2018 in Vienna that was attended by over 50 international specialists. WINS also used this opportunity to commission a Special Report that synthesised the key points from the workshop and put the terrorist threat into perspective. We believe the report provides important insights into the subject area. As with all of our publications, this report will be available for WINS Members on the WINS website.

WORKSHOP STRUCTURE

The workshop was structured into seven main sessions to explore the various aspects of the topic. The workshop heard presentations from a wide variety of practitioners who addressed the technologies that could be used and misused in the context of the evolving security threat to the nuclear sector.

OPENING SESSION

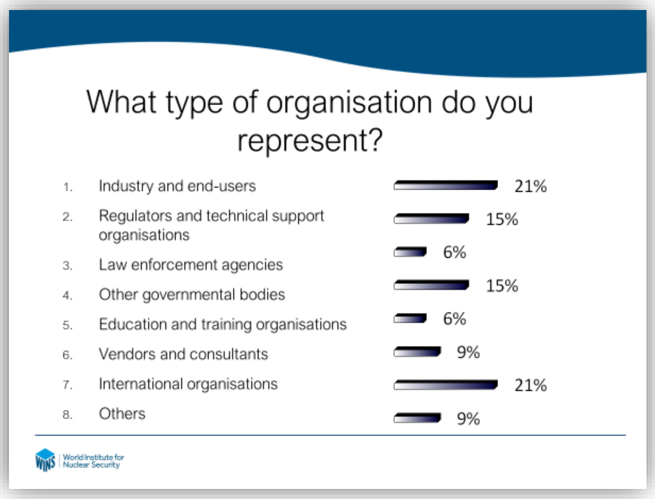
The opening session was designed to provide everyone with an overview of the current threat environment the nuclear industry is facing as well as to discuss technological changes that might take place in the coming years, and how nuclear organisations and other nuclear security stakeholders can strategically anticipate and prepare to meet them.

Presentations to introduce these themes were made by:

- **Dr Roger Howsley**, Executive Director, WINS
- **James Halverson**, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, United States – “Assessing the Threat: Past and Future”

PARTICIPANTS’ INTRODUCTION AND EXPECTATIONS

The workshop facilitator, **Julian Powe**, continued the opening session by asking participants to use the e-voting system to indicate which sector they represented (e-voting results below). After that short exercise was completed, participants were asked to introduce themselves at their tables and to discuss their expectations coming into this workshop.



What type of organisation do you represent?

1.	Industry and end-users	21%
2.	Regulators and technical support organisations	15%
3.	Law enforcement agencies	6%
4.	Other governmental bodies	15%
5.	Education and training organisations	6%
6.	Vendors and consultants	9%
7.	International organisations	21%
8.	Others	9%

The feedback that was collected in terms of expectations focused on:

1. Learning about new technology;
2. Threat assessment methodology;
3. Cross pollination – sharing information across sectors;
4. What is the “state of the art” across the industry?
5. Identifying gaps in current systems – where can technology help?
6. Benchmarking and networking;
7. Exploring performance-based solutions
8. How we can leverage technology?
9. What the regulator’s perspective is?
10. What the future threat factors are?
11. What the interface is going to look like between safety and security?
12. Exploring cyber and A.I.;
13. How technology can help as a retrofit or for a new build?
14. What the gaps in the technologies are?

SESSION 1: EVOLVING THREATS

This session was designed to understand what the current threat environment looks like and how this might change in the future. Specifically, the discussions focused on what the main evolving security threats might be in the next 10 years and what challenges the industry might face in the future.

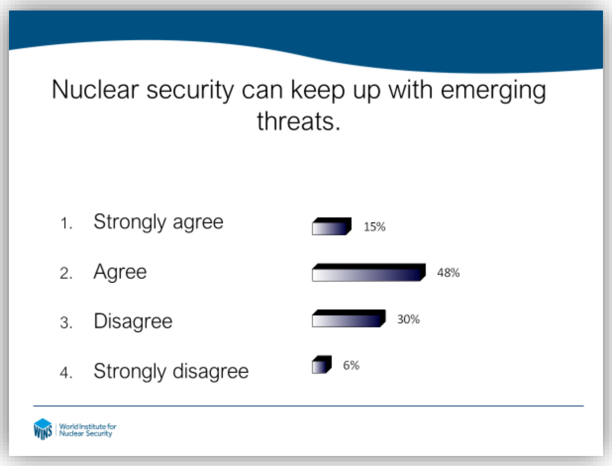
A presentation was given by **Guido Gluschke**, Viccon GmbH, Germany on “Evolving and Emerging Cyber Threats”. The discussions that followed looked at how cyber threat information is assessed and communicated and whether current security arrangements are evolving at the same pace as the cyber threat landscape. The discussion that emerged out from this presentation focused predominantly around the need to strengthen the cyber security regime around the industry. Finally, the idea of whether we should move back to analogue systems was briefly discussed – clearly highlighting the lack of consensus amongst the community.

SESSION 2: ADDRESSING FUTURE THREATS – AN INDUSTRY PERSPECTIVE

This session explored what nuclear security might look like in 2025 and the role of advanced security technologies in achieving this form of security.

E-VOTE

To introduce Session 2, an e-vote was taken to elicit participants’ views on whether nuclear security can keep up with emerging threats (e-voting results below).



Nuclear security can keep up with emerging threats.

1.	Strongly agree	15%
2.	Agree	48%
3.	Disagree	30%
4.	Strongly disagree	6%

The discussion that followed the e-vote provided the remaining speakers with a snapshot of the beliefs the audience held. Those individuals that agreed that nuclear security is able to keep up with emerging threats argued that there is sufficient knowledge available that one could draw from and that the exchange of information has increased historically. It was also mentioned that there is a real drive to do “the job” right and therefore nuclear security professionals would take their responsibilities seriously.

Those individuals who disagreed with the e-voting questions argued the following:

1. Today’s tactics are changing;
2. Prediction is a challenge;
3. Institutional inertia – reactive rather than proactive;
4. We aren't being “tested” properly; can lead to complacency
5. Demographics – younger generation – the loss of the collective memory;
6. Availability of information helps the attackers;
7. Challenging to get ahead of cyber – can enhance physical threats.

Building off of this introductory discussion, two presentations were held by:

- **Eddie Marrett**, Rolls-Royce, United Kingdom – “Securing Small Modular Reactors – A Case Study”
- **Kevin Louth**, Horizon Nuclear Power, United Kingdom – “Proactive Attitude Towards New Technologies and The Future”

The breakout discussions that followed both presentations highlighted several ideas that need to be addressed in the future such as:

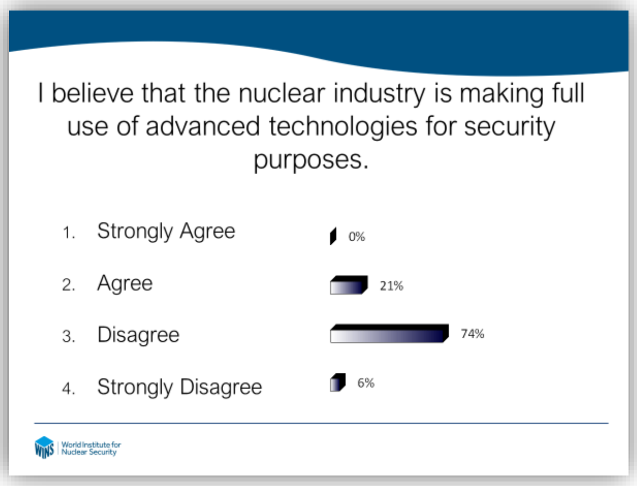
1. The regulation of dual use technology;
2. Where the liability lies with decisions that are made by artificial intelligence;
3. How to leverage machine learning and artificial intelligence;
4. Whether the **“**as low as reasonably practicable” (ALARP) concept could be widened to encompass security;
5. How technology can support the integration of safety and security further.

SESSION 3: ADVANCED TECHNOLOGIES AND THEIR IMPACT ON NUCLEAR SECURITY

The presentations and plenary discussions in this session looked at the various upcoming technologies and their associated risks and opportunities.

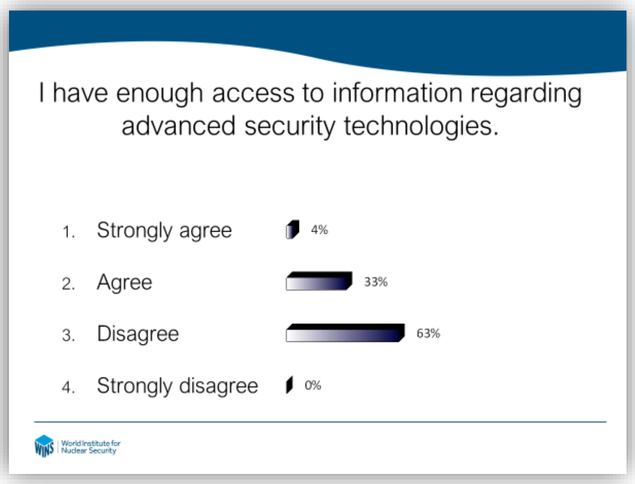
E-VOTE

To introduce Session 3, an e-vote was taken to elicit participants’ views on whether the nuclear industry was making full use of advanced technologies and whether the community had enough access to information about the availability of such technologies (e-voting results below).



I believe that the nuclear industry is making full use of advanced technologies for security purposes.

1.	Strongly Agree	0%
2.	Agree	21%
3.	Disagree	74%
4.	Strongly Disagree	6%



I have enough access to information regarding advanced security technologies.

1. Strongly agree 4%
2. Agree 33%
3. Disagree 63%
4. Strongly disagree 0%

The conversation that followed the e-vote highlighted the need for further information exchange - especially cross pollination from other critical infrastructures, as well as financial institutions, was identified as one way to access valuable experience.

With this in mind, the following technologies - unmanned aerial vehicles (UAVs), robotics, and augmented and virtual reality - were discussed by:

- **Chad Monthan**, Sandia National Laboratories, United States – “Security Challenges: Unmanned Aerial Vehicles”
- **Matthias Biegl**, Taurob GmbH, Austria – “Responding to Dangerous Situations: A Robotic Solution”
- **Morten Wenstad**, EON Reality, Norway – “How Augmented and Virtual Reality can help enhance Nuclear Security”

The plenary and panel discussion points are summarised below:

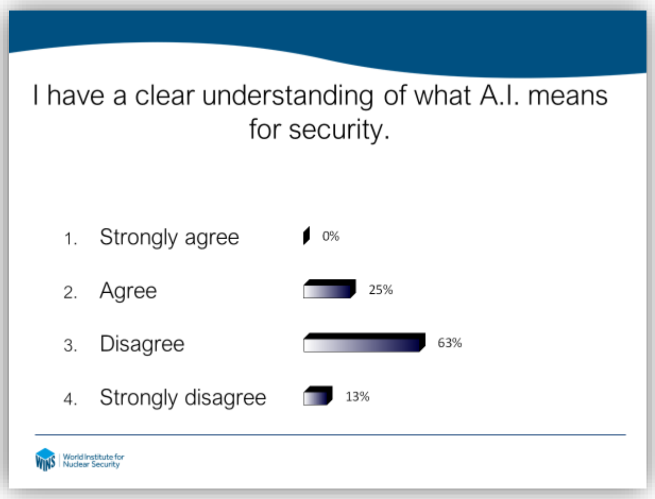
1. Regulations can’t keep up – partnerships across industry and vendors need to contribute to the thinking, and support outcome rather than prescriptive regulation which won’t work;
2. Financial benefit has to be certain as well as safety and security;
3. Benefit of partnering between other partners to de-risk and maximising their usefulness;
4. When do we jump into a technology?
5. Anxiety when a technology becomes a type of “compendium” of your assets;
6. The less people touch the “material” the lower is the insider threat;
7. Technology which helps safety and security – will be popular and easy to “sell” to management;
8. Build a model for assessing, tracing and deciding on whether to invest in different technologies;
9. More help is needed (from WINS, IAEA etc.) to support this;
10. Reputational damage – enormous risk for the operator;
11. Diffusion of information – certain information becomes available via AR training materials.

SESSION 4: EXPLORING THE ROLE OF ARTIFICIAL INTELLIGENCE IN NUCLEAR SECURITY

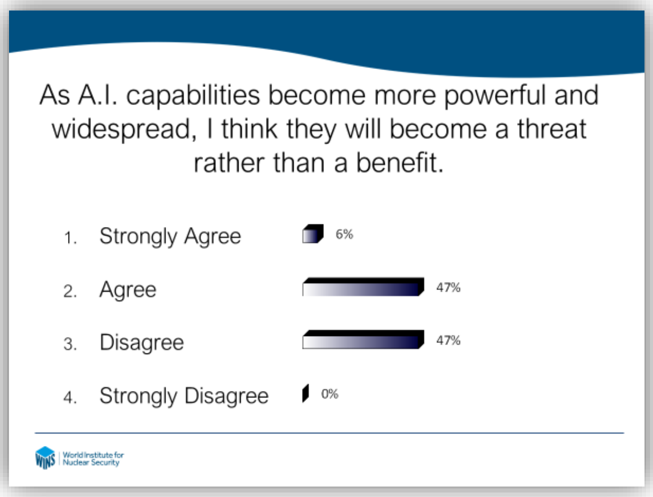
The purpose of this session was to explore the potential role artificial intelligence (A.I.) might have within nuclear security and specifically focusing on the associated risks and opportunities. This session also explored the role of data analytics and demonstrated how such systems could be used to enhance nuclear security.

E-VOTE

An e-vote was taken at the beginning of Session 4 to gauge participants’ understanding of what A.I. means for security and whether they believed that as A.I. capabilities increase these represent more of a threat rather than a benefit (e-voting results below).



I have a clear understanding of what A.I. means for security.



As A.I. capabilities become more powerful and widespread, I think they will become a threat rather than a benefit.

As clearly demonstrated by the results above, the field of A.I. remains a novel area for most nuclear practitioners and therefore might require closer collaboration with A.I. service providers to be able to bridge this gap in the community's understanding. Currently, as indicated above, over 50% remain sceptical in regard to the positive application of A.I. in the security realm.

Two presentations, addressing these issues, were made by:

- **Dr Martin Svik**, IBM iLab, Czech Republic - "Exploring the Role of Artificial Intelligence in Nuclear Security"
- **Christopher Hawkes**, Point Duty Pty Ltd, UK – "Data Analytics from a Security Perspective"

The breakout group discussion that followed addressed a variety of topics listed below:

1. If these tools can deliver important answers – what are the important questions?
2. State priorities vs. Business priorities - balancing those is often very difficult;
3. How far have we gone with data analytics in business?
4. How do smaller nations/organisations deal with data analytics and A.I.? Are they even capable of running such systems?
5. What is the maturity of the nuclear sector? Are we leaders? Fast adopters? Slow adopters? Will we be forced into it? - If we are slow - we need more partnerships with other sectors (banking, aviation, etc.);
6. Apply these tools to supply chain management and other areas;

SESSION 5: THE USE OF REMOTELY OPERATED WEAPON SYSTEMS – A CASE STUDY

This section of the agenda explored the role of remotely operated weapon systems and discussed the rational and associated business case for their deployment at nuclear power plants.

A presentation was made by:

- **Anthony Qualantone**, Precision Remotes LLC, United States – "Evolving Security Threats and Advanced Security Technologies"

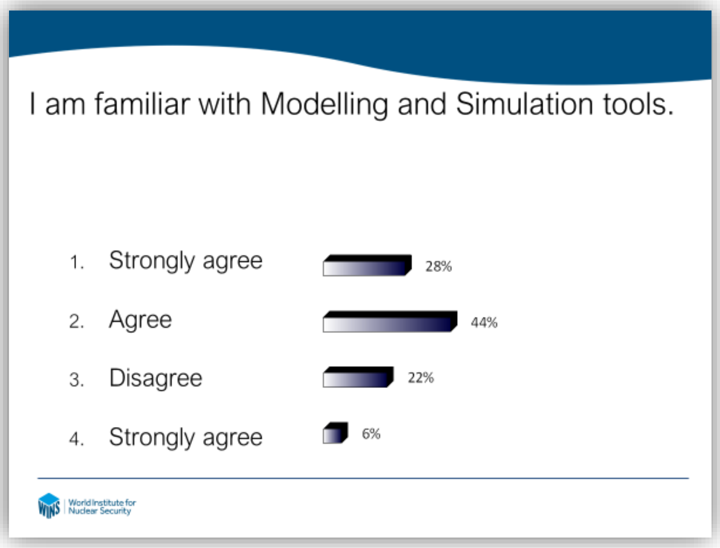
The discussions that followed the presentation focused on how the most significant potential impact of remotely operated weapons systems (ROWS) on nuclear facility security is their employment as defensive, force multiplying sentries. The workshop participants were also very interested in how these systems have become more resilient over the years.

SESSION 6: MODELLING AND SIMULATION TOOLS IN SUPPORT OF RISK MANAGEMENT

The objective of this session was to consider the current status of modelling and simulation (M&S) tools for nuclear security planning and assessment. The goal of this session was also to discuss the role of M&S in developing skills and competencies, establishing security arrangements, and preparing for emergency situations.

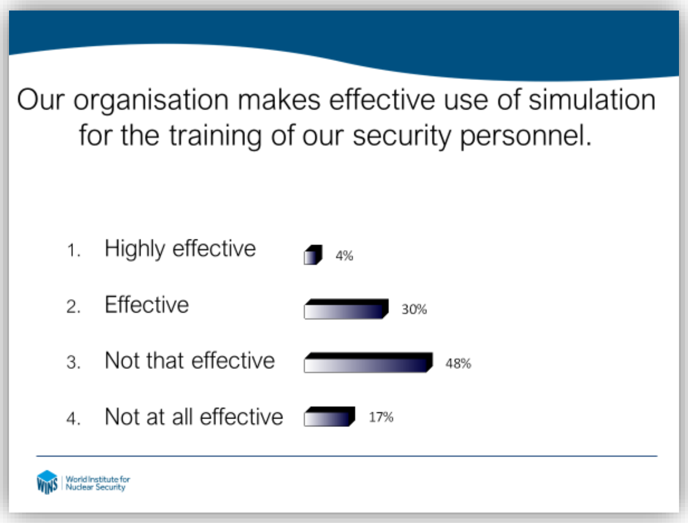
E-VOTE

An e-vote was taken at the beginning of Session 6 to gauge participants' familiarity with Modelling and Simulation tools and whether their respective organisations made effective use of such tools for training purposes (e-voting results below).



I am familiar with Modelling and Simulation tools.

1. Strongly agree 28%
2. Agree 44%
3. Disagree 22%
4. Strongly agree 6%



Our organisation makes effective use of simulation for the training of our security personnel.

1. Highly effective
2. Effective
3. Not that effective
4. Not at all effective

The results highlighted that although participants had a high familiarity with the variety of modelling and simulation tools available they also believed that their respective organisations needed to improve the way these tools are used to inform the training of their security personnel.

The presentations on modelling and simulation tools that followed were made by:

- **Robert Scott**, ARES Security Corporation, United States – “ARES Security: Protecting the World’s Most Critical Assets”
- **Matthew Talbot**, RhinoCorps, United States – “Advanced Security Tools”

The plenary discussion that followed focused on the following questions and themes:

1. What about active insider capability?
2. What about egress modelling?
3. Modelling and Simulation is very versatile;
4. ‘Don’t inhale all that cyber smoke’ – you have to ask yourself why you are testing a scenario;
5. Keep the scenarios real so that the result is useful;
6. It adds extra depth and value;
7. Easy to make decisions when we know everything – very different when knowledge is limited in the situation;
8. Modelling cyber requires live databases as these things change. Physical systems don’t change anything like as fast;
9. Cyber realm is much more opinionated vs. real data and visualisation in the physical realm;
10. Modelling isn’t absolute;
11. Not every event starts with a “bang” – sometimes there is a lack of imagination on how scenarios can be initiated and subsequently develop.

Building of these themes, the facilitator asked participants to break into small groups and to complete the following sentence: “If we are going to do a really good job on modelling and simulation in the next few years, nuclear security needs to….”. The feedback from the groups is listed below:

1. Create a justification beyond money;
2. Understand softer issues;
3. Account for varied adversary intentions;
4. Utilise a variety of tools to identify the problem and train for the problem;
5. Be globally accepted;
6. Implement regulatory guidance consistently;
7. Have good data - i.e. good data in – good data out;

8. Be honest and transparent with the results;
9. Recognise its strengths and limitations;
10. Address airborne threats (Drones);
11. Make it useful for the operators (ex. demonstrates usefulness during an outage) - easier to sell;
12. Make sure the threat is real and credible - not something random;
13. Link in with other technologies;
14. Conduct limited trials to help justify what you will implement – trial versions need to be available;
15. Accept independent validation;

SESSION 7: REGULATION AND OTHER CONSIDERATIONS

This session aimed at looking at the wider use of advanced security technologies and the impact such technologies have on employees and their privacy. It also explored the role of the regulator and other stakeholders involved in the implementation of such "new" tools and systems.

Presentations were made by:

- **Tom Parkhouse and Gareth Allsopp**, Office for Nuclear Regulation, United Kingdom - "Regulatory Opportunities and Challenges associated with the Evolving Threat and Advanced Security Technologies"

The discussion that followed both presentations focused predominantly on the following areas:

1. What is the value to the business?
2. Establish networks and partnerships;
3. Define effective performance thresholds;
4. "Modern workforce" - how do we integrate the future workforce with new technologies;
5. Modelling of future concepts;
6. Strategy for horizon scanning is needed;
7. Regulations should not be prescriptive;
8. Use a common language across the industry;

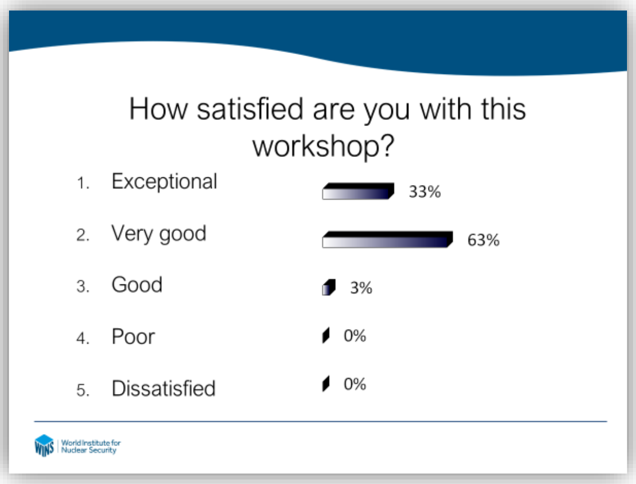
CONCLUSION SESSION

The final discussion aimed to identify and discuss tangible and realistic next steps and reviewed the role that vendors, regulators, industry, and international organisations must play. In addition, participants were asked to review what workshop topics were most relevant, which ones were directly applicable and which ones were not. Participants were also encouraged to identify what they had most appreciated during the workshop and what they would take away as key points. Below are some of the results:

1. Thinking about the regulation of advanced technologies;
2. Committing not to go forward separately – we have a duty to share;
3. Modelling of the potential opportunities;
4. Share experiences internationally;
5. Understand opportunities within our current structure: workforce, supply chain, etc;
6. Working with the international infrastructure (find out which sector is in the lead for which problem);
7. How to really test your cyber security and what does this really look like;
8. Horizon scanning.

E-voting

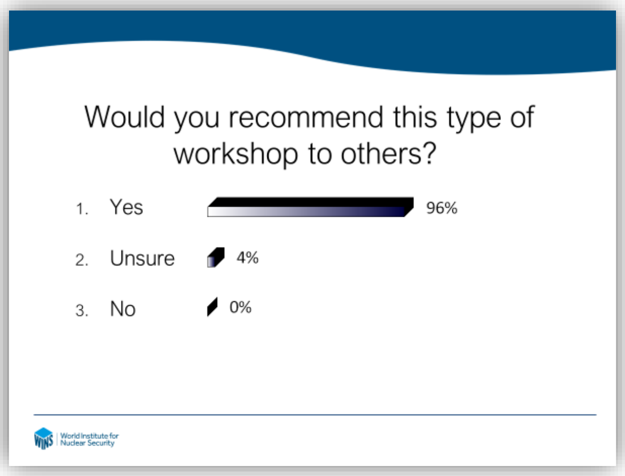
The e-voting system was used to obtain a final evaluation. Participants indicated that they were very satisfied with the event, that it had been an excellent and useful learning experience and that they would recommend the event to others. The results are illustrated below:



How satisfied are you with this workshop?

1. Exceptional 33%
2. Very good 63%
3. Good 3%
4. Poor 0%
5. Dissatisfied 0%

World Institute for Nuclear Security



Would you recommend this type of workshop to others?

1. Yes 96%
2. Unsure 4%
3. No 0%

World Institute for Nuclear Security

In his closing remarks, Dr Roger Howsley, emphasised that the success of the workshop was largely due to the active contributions of all participants. He praised the willingness of the group to learn from the speakers' team and from each other despite it being a challenging topic. He added that the discussions had shown that participants (and likely the stakeholders they were representing) had a strong appetite for further exploring the key themes of the workshop.

Dr Howsley also noted that the specially commissioned report on "Evolving Security Threats and Advanced Security Technologies" would be available on the WINS website by the end of April.