World Institute for Nuclear Security

AUTONOMOUS AND REMOTELY SYTEMS: BENEFITS AND CHALLENGES FOR NUCLEAR SECURITY

WORKSHOP REPORT

VIENNA, AUSTRIA, 2–4 APRIL 2019

BACKGROUND

The development of new advanced technologies in the nuclear industry is rapidly changing the management of security programmes. Although such technologies have many benefits, they also have some serious drawbacks, especially when it comes to security. For example, unmanned aerial vehicles (UAVs) are of significant concern for managers at critical infrastructure sites, including airports and nuclear sites. In addition, criminals and terrorists are making increased use of cyberattack tools and technologies, including encrypted communication, to coordinate their activities and avoid law enforcement detection and control measures.

In response, governments are implementing new strategies in the effort to protect the critical infrastructure that underpins vital public services. When it comes to the nuclear industry, regulators and operators are working to reduce facility vulnerabilities while simultaneously increasing resilience. Nuclear security protection has already progressed beyond the traditional domain of gates, guns and guards; now various stakeholders are investing in research and development of cutting-edge technologies and defence systems to protect facilities and minimise the risks and consequences should an attack occur.

Examples of such advances are remotely operated weapons (ROWs) and robotics that may help security professionals and law-enforcement agencies protect valuable assets by increasing the efficiency of deterrence and response. It is expected that remotely operated and autonomous technologies will gradually enter the portfolio of protective measures and provide significant improvement in the performance of security systems. Just one impetus for this is operators' desire to reduce security costs by replacing some personnel with semi or fully autonomous systems.

It is important to understand that new technologies present both a threat and an opportunity. It is the responsibility of regulators, operators, international organisations and law enforcement agencies to address the challenges of implementing advanced technologies in the nuclear industry in the most effective way possible.

WORKSHOP STRUCTURE

This workshop was divided into four main sessions, which enabled a wide variety of speakers to provide their perspectives on the topic.

OPENING SESSION

In the opening session, WINS Executive Director **Dr Roger Howsley** explained that the workshop would focus on technological changes, in particular those dealing with autonomous and remotely operated systems and components in the field of nuclear security, that might take place in the coming years. In particular, he said, the workshop would explore how nuclear organisations and other nuclear security stakeholders can strategically anticipate and benefit from such changes. The workshop drew on the major topics addressed in the WINS Special Report titled *Evolving Security Threats and Advanced Security Technologies*, which was published in 2018.

Dr Howsley explained that the workshop would cover:

- The evolving threat landscape and the intersection between threats and technologies.
- A comprehensive review of autonomous and remotely operated systems for security.
- Considerations for the adoption of advanced technologies.

Dr Howsley also shared the results of a survey that was conducted prior to the workshop:

- 80% of respondents think that terrorist groups already have the capability to perpetrate attacks on nuclear facilities with advanced technology devices.
- Around 50% think there is a clear trend among nuclear organisations to deploy autonomous and remotely operated systems.
- 70% believe autonomous and remotely operated systems will significantly enhance security arrangements at nuclear facilities.
- The majority of participants said that ROWs and drones are the technologies that will have the most significant impact on nuclear security.
- The main challenges for the effective deployment of autonomous and remotely operated systems will be cybersecurity and regulations.
- The major advantages that operators will experience when implementing these technologies are a reduction of security costs and better security performance.

PARTICIPANT INTRODUCTIONS AND EXPECTATIONS

The workshop facilitator, **Mr Julian Powe**, continued the opening session by asking participants to introduce themselves and share their expectations for the workshop. Examples included:

- Obtain a better understanding of the threat landscape and the impact on critical infrastructure industries.
- Learn which systems offer the greatest potential benefits in terms of technology and risk and how to benchmark them.
- Learn how nuclear industries should address regulations and how to deal effectively with regulatory requirements.

- Obtain professional insights and share practical experiences and best practices.
- Understand the role of human factors.
- Learn how to engage better with all stakeholders, including the best way to identify partnering and networking opportunities, share lessons learned, and work together more effectively.
- Learn how to influence advanced security technology industries.
- Obtain a view of what the nuclear security landscape might look like in 5-10 years.

E-VOTE

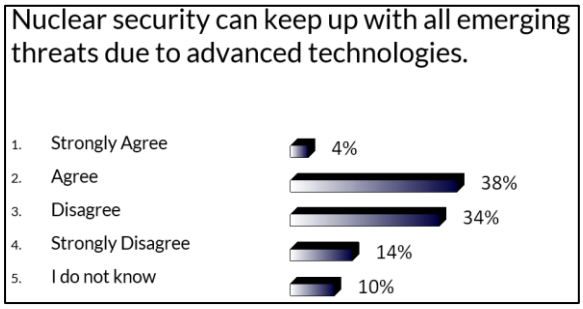
In an e-vote, participants were asked to indicate what kinds of organisations they worked for. Their answers indicated a wide variety of backgrounds.

KEYNOTE PRESENTATION

In the keynote presentation, **Mr Edward O'Neil,** Duke Energy (USA), addressed the topic of *Keeping Pace with Security Risks and Opportunities*. He highlighted how technological changes are transforming security operations, as well as the operating model. He also explained the differences between transformational change and disruptive change and reviewed several advanced nuclear security technologies.

Participant Discussion

After Mr O'Neil's keynote, participants had the opportunity to express their opinions about the following topic:



Some participants pointed out that nuclear power plants (NPPs) in the United States are responsible for security, not the government. This can influence the way nuclear security arrangements are addressed and the commitments of shareholders in new investments on security.

Participants also mentioned that operators need to think in a different way to survive in the evolving threat landscape. If the nuclear industry doesn't change, it will fall behind. Some operators said their organisations are training officers to respond to drones and that their facilities now combine classic

security systems with technologically advanced security systems. As a result of the overlapping and redundancy of the two systems, they believe that security effectiveness has been enhanced.

Some participants said that their security plan is still human-based, not machine-based, despite their use of advanced security technologies. This is changing, however. By 2030, they plan to significantly reduce human resources and increase the use of technology. Such a change requires that they focus even more strongly on cyber protection. The expectation is that moving away from a human-driven model to a machine-driven model will reduce security costs while keeping security performance at the same or higher level of performance.

SESSION 1: THE EVOLVING THREAT LANDSCAPE AND THE INTERSECTION BETWEEN THREATS AND TECHNOLOGIES

The objective of this session was to provide an overview of how technological changes in the next 10 years will influence the threat and what this means in regard to the protective measures that will be required for security.

FIRST PRESENTATION

Mr Zachary Kallenborn, independent national security researcher, delivered the first presentation remotely from Washington DC. Mr Kallenborn explained that emerging technologies are moderately reducing the barriers to CBRN weapons acquisition and offering new ways to carry out mass casualty attacks. (The technology that has captured most of the attention to date in terms of threat is the drone.) He also said that the threat landscape keeps evolving and that terrorist groups remain motivated to perpetrate such attacks, but that their capabilities are low.

Mr Kallenborn added that terrorism involving CBRN is hard (high costs, specialized equipment, significant domain and tacit knowledge); he also said that adversaries might not find CBRN worth pursuing due to the strategic costs and the fact that other kinds of attacks are easier to perpetrate. He explained that although emerging technologies are lowering some barriers to CBRN weapons acquisition and delivery, the major barriers remain. In addition, he said that emerging technologies such as drone attacks, cyberattacks and nanotech weapons offer new methods of generating mass casualties. It is also easier to acquire them and use them to carry out an attack than it is to acquire CBRN weapons.

Participant Discussion

In discussions following the presentation, participants emphasised that the nature of the threat is currently changing and will continue to do so in the future. Many of the technologies can be used in a variety of creative ways; therefore, the nuclear industry needs to change its baseline assumptions about security. Some participants wondered how to measure the threat and how much money would be required, but there was no general consensus on this. Participants did agree, however, that nuclear security stakeholders need to communicate more effectively with each other and work together when deploying such technologies.

Participants also discussed whether design basis threats (DBTs) are the best way to communicate evolving threats. They emphasized the importance of building a governance framework to discuss future threats and of educating senior management on the evolving threats from advanced security technologies. They also noted that public perceptions are a key influencing factor when talking about threats and critical infrastructure. Finally, participants gave examples of potential threat scenarios, including:

- The shutdown of a nuclear facility for a long period of time due to an aerial attack from an unmanned system.
- The use of a small drone loaded with chemicals that could contaminate the ventilation system.
- The use of social media to manipulate people's behaviours.
- An insider with the ability to perpetrate or facilitate a serious cyberattack.
- The use of a drone to steal nuclear material or radioactive sources while they are being transported.
- The use of a drone to study the security architecture of a nuclear facility and identify its security arrangements.
- Undertaking a blended attack that spoofs cameras and attacks cyber connections.
- The use of a drone to send signals to adversaries outside the nuclear facility.

SESSION 2: INTRODUCTION TO AUTONOMOUS AND REMOTELY OPERATED SYSTEMS RELEVANT TO NUCLEAR SECURITY

This session explored some of the major autonomous and remotely operated systems that are currently available. Examples include drones and other unmanned aerial vehicles, remotely operated weapons, automatic control access systems, surveillance roots and unmanned ground vehicles. The session also addressed the most important advanced security technologies and when they might be implemented in the nuclear industry.

FIRST PRESENTATION

In the first presentation of Session 2, **Mr Pierre Legoux,** WINS, gave a brief overview of remotely operated and autonomous systems for security. He also posed several important questions that nuclear security stakeholders need to answer:

- What is the need? What security function do we want to achieve?
- What technologies are currently available? What is likely to come online over the next 5-10 years?
- What is our experience to date with these technologies? Do we have enough opportunities for sharing lessons learned?
- What would a process look like that identifies a new technology, assesses its possible benefits, and integrates it effectively into existing security arrangements?
- What are our incentives for adopting new technologies?
- What are the remaining barriers to effective integration in our security programmes?
- How do we demonstrate these technologies are protected against misuse?

In addition, Mr Legoux discussed some of the benefits and challenges of the main technologies and pointed out three key points that need to be considered in this regard:

- Security budgets are under greater scrutiny at the same time as potential new threats and new facility designs are raising new security challenges.
- The insider threat is a more important issue than ever before and must therefore receive even greater attention.
- Regulation must become more agile to allow for responsiveness to changes in threats and benefits brought by advanced security technologies.

Participant Discussion

Participants then discussed these different technologies and how important it is to describe the security requirements accurately in order to identify the systems that operators need and how to deploy them effectively. Participants also pointed that the greatest resistance to ROWs comes from the fact that the larger calibres can shoot far—even into nearby residential areas. For this reason and others, ROWs face regulatory challenges and social acceptance issues.

SECOND PRESENTATION

In the second presentation, **Mr Paul Reither**, Diamond Advisory, talked about *A Global Approach to Critical Infrastructure Protection*. He provided an overview of the oil and gas sector, including its value chain and characteristics. He then addressed the threat landscape, including its dynamics and capabilities, and described the comprehensive Security Risk Assessment (SRA) that the oil and gas industry uses for risk reduction. Mr Reither emphasised that threats are dynamic and constantly changing, so an SRA requires continuous effort and is not simply a periodic exercise. Perpetrators only have to get it right one time, but security has to get it right every time.

Threats will clearly differ from country to country, region to region and location to location. However, an intelligence-led approach will ultimately lead to appropriate and cost-efficient solutions. (If there is no threat, no protection is required.) Another issue with oil and gas operations is that they often take place in remote and isolated areas where law enforcement and the ability to intervene are lacking. Consequently, the operations are self-contained to a large degree.

Participant Discussion

In the discussion that followed, participants and the speaker pointed out that the "right" level of protection depends on the threat, e.g. on the adversary's intent and capability. Different adversaries have different objectives; therefore, the attractiveness of a particular target will vary accordingly. If protection falls below a certain level of attractiveness, it leaves facilities unprotected. However, if protection falls too far above this level, it wastes money. Achieving the right balance of physical protection is a challenge.

Participants ended the discussion by agreeing on the need to use multiple sources of information to identify threats to critical infrastructure. Examples of such sources included professional associations, operators, regulators and intelligence organisations. They also emphasised that the relationship among different stakeholders should be less rigid and more proactive in terms of identifying potential threats.

THIRD PRESENTATION

In the third presentation, **Ms Marie-Caroline Laurent,** Lham Lha (France**)**, talked about *The Aviation Sector and Advanced Security Technologies*. She confirmed that the threat has also evolved in the aviation industry—from hijacking, airborne threats and explosives to hazardous materials and CBRN. She explained that adversaries use different vectors to carry out their malicious acts, including passengers, staff (insiders), freight (shipments) and drones.

Ms Laurent also mentioned some key security challenges in the aviation industry, including the growth in traffic and the costs of disruption. (One minute of delay costs airlines about 100 EUR.) In addition, she mentioned several advanced technologies, such as chemical detection for explosives, the potential of artificial intelligence, behaviour detection, flow management, identity management, drones and cybersecurity. However, she also said that technology is not the only answer and that the sharing of more information is vital to ensure effective risk-based security.

Participant Discussion

In the discussion that followed, participants discussed the differences and similarities between the nuclear and aviation security sectors and how much they can learn from each other. One example of this is how the two industries adapt to new technologies and the role of regulators in the process. In aviation security, the most important objective is to keep the aircraft from exploding or being used as a weapon, not to protect the airport. After recent attacks at the Brussels airport, however, there are some initiatives to better protect airport facilities. The main objective now is to better understand the actual threats and how traffic moves around the airport rather than to simply deploy a system that protects the airport from a specific threat.

Participants also identified the main decision-making criteria for deploying advanced security technologies in a nuclear facility: security performance, costs and risk management. Some of the main decision-making criteria included:

- DBTs
- Risk assessment, risk probabilities
- Total costs of operation
- Lifecyle costs/benefits
- Impact of the technology
- Impact of the incident
- Regulatory considerations and legal considerations
- Impact on public opinion and degree of social acceptance
- The interface between safety and security

PANEL EXPERT DISCUSSION

At the end of day one, an expert panel discussion took place on how emerging technologies are impacting security strategies and how nuclear security will change in the future. Some main points include:

- Security will need to be flexible and agile to address the evolving threat.
- Security arrangements will become more machine-based and less human-based.
- The focus on cyber protection will be continuous.
- Dynamic monitoring networks will develop.
- To identify possible insiders, higher numbers of background and cross-data checks will take place.
- The entire technology supply chain will need to be secure.
- The security industry needs to make the public more aware about how to avoid malicious attacks stemming from advanced technologies.

SESSION 3: A COMPREHENSIVE REVIEW OF AUTONOMOUS AND REMOTELY OPERATED SYSTEMS FOR SECURITY

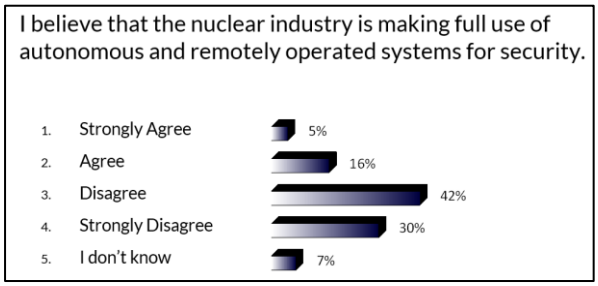
Session 3 focused on the different kinds of autonomous and remotely operated systems that already exist and how they present both opportunities and threats to nuclear security. The session also addressed how to ensure the cybersecurity of advanced technologies, the prerequisites that are necessary for their deployment, and what the nuclear industry can learn from past experience.

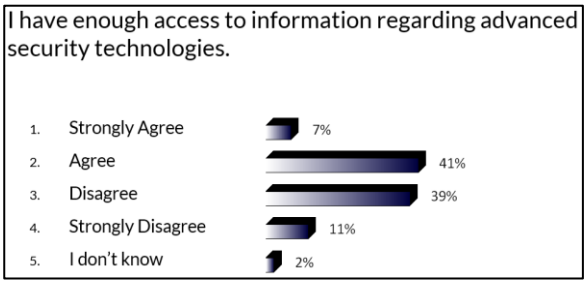
In addition, participants reflected on the key findings from Day 1 and affirmed that the nuclear industry does not know what the threat will look like. Just one example is the use of electromagnetic pulses for attacking nuclear facilities, which is still an unexplored path. They concluded that a lot of work still needs to be done to identify threats and prepare for the future.

Participants also agreed that cybersecurity and insider threat are critical aspects of security and that operators still need to improve in these areas. Moreover, nuclear security stakeholders must address the impact of drones and how the security aspects intersect with public awareness.

E-VOTE

In an e-vote, participants shared their opinions on two topics:





Some participants said that they already have on autonomous, remotely operated system, but that it is out of date. Others remarked that they do not understand how advanced security systems actually perform under certain conditions and exactly how to apply them. They also said there is little public information available from early adopters of the technology because organisations generally do not report on this. Finally, they said that there is a fine line between research and development and between commercial use and military use.

FIRST PRESENTATION

In the first presentation of Session 3, **Mr Martin Kovar** and **Mr Ondrej Svec,** Cogniware (Czech Republic), talked about biometric and facial recognition technology, including how it works and what some of its strengths and weaknesses are. They also showed participants a live demo of their technology in the following situations:

- Monitoring the entry gateway to a facility using face recognition, tracking and anti-spoof detection (door open use case).
- Monitoring numerous entry points to a facility involving large numbers of people and detecting tailgating.
- Monitoring the surroundings of a facility using face recognition and perimeter monitoring cameras with validation of the access to monitored area, plus investigation of individuals' movements as a surveillance officer.

Participant Discussion

Participants then discussed the opportunities and limitations of biometric and facial recognition technology in nuclear security. Some of the main points included:

- The two main factors are the costs and benefits of the technology.
- The technology has to be fast and efficient.
- Data protection issues are key.
- Facial recognition is meant to be another layer of security; its combination with iris technology is extremely beneficial.
- Security is not supposed to be convenient for everybody.
- Facial recognition can not only be used to control access, but also to continuously monitor people going into certain areas.

One participant asked what would happen if a serious nuclear security incident takes place and the technology to prevent it was available but had not been implemented. Could the operator be prosecuted based on a cost analysis of the implementation of the technology? Participants agreed that this kind of question helps the nuclear industry become more efficient when deploying new technologies.

SECOND AND THIRD PRESENTATIONS

In the second presentation, **Mr Richard Gill,** Drone Defence Services (UK), talked about *How Nuclear Operators Can Respond to the Threat from Drones, and What Can Be Done about Them.* He started with an overview of the current drone threat, explaining that military drones came first. He also said the public has a negative perception on drones and that the narrative needs to change. A supportive legislation framework needs to be developed that addresses legitimate security concerns. Mr Gill ended his presentation with suggestions for how to detect drones.

In the third presentation, Mr Yuan Zhe, SNERDI (China), talked about the *Practice of Low Altitude Aircrafts, Counter System in China*. He explained the current status of airborne threat, the types of low altitude aircraft being used in China, and the regulations on restricted areas. In summary, he said that:

- Aircraft other than drones should be taken into consideration.

- Standard UAVs are easy to stop by setting a restricted area.
- Non-electromagnetic cooperative aircraft is the most dangerous type of threat.
- Regulation supports countering UAV in NPPs, but it is not clear how to deal with illegal aircraft.

Mr Zhe also described aircraft counter systems that some Chinese NPPs (PWR AP1000) are currently using.

Participant Discussion

During the follow-up discussions, participants remarked that there are no industry standards on drones, the market is very young and has a lot of new entrants, and the legislation for aviation security, wireless telegraphy, prisons and police needs to move forward. Furthermore, nuclear security stakeholders need to better understand the capabilities and impacts of drones. Participants also discussed the risks and opportunities of drones. Some major points included:

- Cybersecurity, insider threat, and dealing with non-state terrorist risks are the biggest challenges.
- Emergency response protocols can benefit from the use of drones. Drones might replace some first responders' actions.
- Drones can introduce major risks for nuclear material and radioactive sources during transport. They represent a threat for physical security during transport.
- Drones could be a force multiplier as well.

EXPERT PANEL DISCUSSION

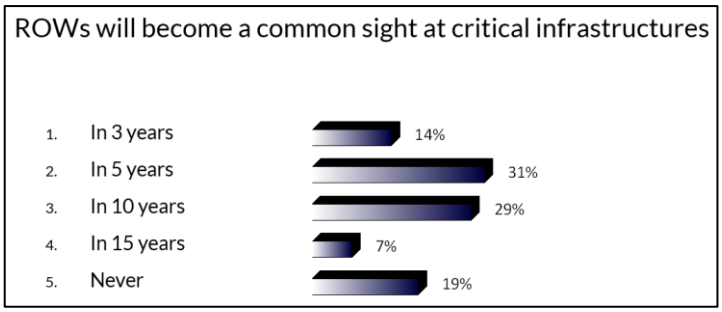
Before the fourth presentation, a discussion was held that involved a panel of experts. Five individuals drawn from operators, regulators and law enforcement organisations addressed what licensees and regulators should be thinking about in the next five years. Some of the main points from the discussion include:

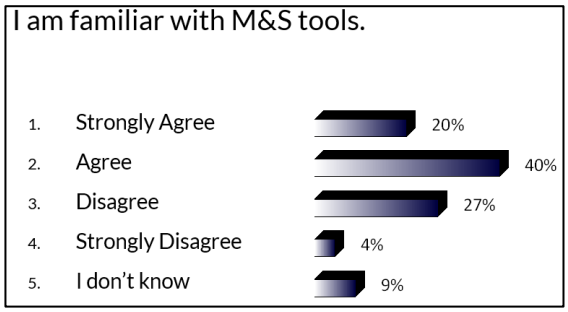
- Interaction with aviation administrators is key for the use of drones.
- Nuclear stakeholders should contribute to the draft legislation for drones. Just one benefit of doing so is that they will better understand what the laws are addressing.
- The UK has stablished a working group to work on UAVs. In this case, the regulations will emerge from operators and not from the regulatory body.
- Countermeasure systems are not yet regulated.
- Physical destruction of a drone is not an option. The industry needs to conduct research and hold discussions so they clearly understand what they want to protect and how to protect it.
- Regulation should be more proactive and work on standards. The regulation of airspace is a good starting point.

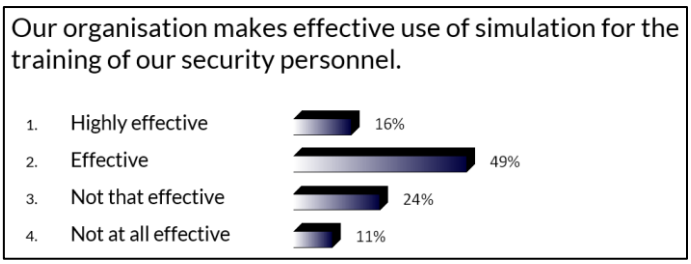
- The systems used to detect drones are very expensive and not fully effective. In addition, there are a lot of legal barriers, and the framework is not clear.
- Operators are looking at technology from the military to defend themselves from drones.
- Some EU countries have well-developed legislation on drones. For example, Spain forbids drones from flying closer than 8 km to an airport and 500 metres from critical infrastructure. The problem is not the regulation itself, but the public's lack of awareness of the rules.

E-VOTE

Following the panel discussion, participants were asked to express their opinion on the following topics:







FOURTH PRESENTATION

In the fourth presentation, **Mr Robert Scott,** Ares Security (USA), talked about *Modelling the Use of Remotely Operated Weapons*. He explained the Ares Security modelling and simulation (M&S) engine and said this technology is currently being used by 60% of the commercial nuclear market in the United States. He also said that the technology is highly customizable and enables users to change adversaries and guards based on certain events. This gives users a wide range of possibilities. He also explained the capabilities of lethal and non-lethal ROWs and UAVs and how to model them in a nuclear facility.

After the presentation, an interesting dialogue took place between Mr Scott and the participants. Some comments included:

- Modelling and simulation can decrease costs while still being effective.
- M&S is not used as extensively in Europe as it is in the US.
- It can take nuclear operators around three to four months to learn the technology and customise it for their own purposes.
- It is important to integrate the concept of insider threat into the simulation tool.

- Operators can enhance their security performance through multiple simulations with diverse cases and probabilities.
- M&S can improve the nuclear industry's ability to imagine and develop threat scenarios.

FIFTH PRESENTATION

In the fifth presentation of Session 3, **Mr Matthias Biegl,** Taurob (Austria), talked about *The Use of Robots in Case of Emergencies*. He said that the Taurob robot can be used in hazardous conditions in critical infrastructures, including nuclear power plants. He pointed out that such robots are being used by fire-fighters, disaster-relief units and search and rescue teams, as well as in such applications as maintenance and inspection. He also said that the robots are equipped with cutting-edge technology that enables them to perform dangerous tasks without putting human health at risk. Such technology can be used remotely and is multidisciplinary and flexible.

Participants mentioned that linking a robot to a drone would greatly improve remotely operated actions. The approach would be to have several robots and highly technological, advanced tools that can cover the entire spectrum of nuclear security requirements, not simply one robot that can perform every task.

SIXTH PRESENTATION

In the sixth and final presentation of the second day, **Mr Edgar Weippl**, SBA Research (Austria), talked about *Securing the Development Lifecycle in Productions Systems Engineering.* He explained the importance of securing the entire supply chain of a product, as well as the challenges and barriers when doing so.

Participant Discussion: Comprehensive Review of Days 1 and 2

At the end of the day, participants summarized the main ideas of the day and the major things they had learned about using autonomous and remotely operated systems for nuclear security. Examples include:

- It is crucial to stay current on the developments taking place in autonomous and remotely operated weapons; if you don't, you fall behind.
- Security needs to be flexible and agile to address the evolving threat.
- Security arrangements are becoming more and more machine-based rather than human-based.
- Although implementing such systems is expensive, it is not nearly as expensive as the costs of damage to reputation should an incident occur.
- Modelling and simulations tools can have a significant impact on drones.
- Procedures for drones are necessary.
- Operators should place less emphasis on recruiting security staff with a police or military background.
- Cybersecurity is becoming more and more important, and operators need to continually focus on cyber protection.

- Digital security systems are critical digital assets.
- Operators need to develop dynamic monitoring networks.
- Operators need to carefully vet potential employees to help protect against insider threat.
- Attack scenarios involving drones are different for NPPs than for airports.
- Drones could be useful from a forensic point of view.
- Advanced technologies in conjunction with fake news could be a malicious tool for creating public insecurity.
- Virtual reality is taking over. Anything can be simulated for a news story.
- Complex threats need cooperation among governments, industry and other stakeholders.
- Information sharing needs to be improved.
- The nuclear security industry should conduct vulnerability assessments and conduct legal analyses in this area.
- The approach toward mitigating vulnerabilities is changing. There is now more emphasis on weapons, explosives, contraband, contaminants and distraction and less emphasis on data collection, hostile surveillance, photography and communication relay devices.
- Drones have plenty of positive benefits, not just drawbacks. For example, it is estimated that they will contribute 2% of GDP to the UK economy by 2030.
- Advances in battery technology will have a major impact on drone capabilities.
- Drones can already work autonomously and automatically; they can also replace each other when the power is low and hook up to self-charging stations.
- A radar system for cost detection could cost around $1.5 million.
- Stakeholders need to create a DBT for drones, and regulation should be more proactive.
- The security industry needs to educate the public about advanced technologies and how to protect themselves from malicious attacks.

SESSION 4: BROADER CONSIDERATIONS FOR ADOPTING ADVANCED TECHNOLOGIES

The purpose of Session 4 was to address the principles for adopting new technologies in nuclear facilities and the associated regulatory challenges. It also addressed the ethical and legal considerations of autonomous and remotely systems and ended with a practical case study about the deployment of autonomous and remotely operated weapons at the Sweetbriar NPP in the fictional state of Ruritania.

Before the first presentation of the last day, participants shared some of their major conclusions from the first two days:

- We need technology to counter technology. This requires investment and commitment.
- The use of modelling and simulation is very beneficial from a security point of view. It helps us understand our capabilities.
- Nuclear stakeholders should work together to address the adoption and implementation of advanced technologies. Operators cannot do it on their own.
- A paradigm shift is taking place in the field of nuclear security due to the extensive use of drones.
- Advanced security technologies can be used to enhance nuclear security and address insider threat.
- We are cautiously optimistic about such technology.
- Cybersecurity is extremely important.
- We need to have a continuous behaviour observation programme. We also need to commit to developing trust throughout the organisation and to developing an effective nuclear security culture.
- Security should be considered first.
- Legislation should move forward. Regulations should not inhibit the development of new technologies.
- Advanced technologies create new opportunities; they also introduce new threats and vulnerabilities.

E-VOTE

After the discussion, participants were asked their opinion about the following sentence:

Participants said that regulators may take the lead, but they were not sure how effective this would be. Some participants also commented that people at the forefront of technology often do not understand the ethical and legal considerations. Others said that it is not a matter of who is leading but how effective the partnership is among key stakeholders.

FIRST AND SECOND PRESENTATIONS

In the first presentation of Session 4, **Mr. Swen Göring**, Austrian Ministry for Transport, Innovations and Technology (Austria), talked about *Regulation of Unmanned Aerial Vehicles*. He discussed national regulations, EASA regulations, and different categorizations for

drones and new procedures. New EU regulations on such vehicles will start to apply in mid-2020 and become fully applicable in mid-2022.

In the second presentation, **Ms Meghan Claire Hammond,** Pillsbury Law (USA), talked about *Ethical and Legal Considerations Associated with the Use of Advanced Technologies*. She said that whether one is adopting advanced technologies or establishing security protections against them, it is important to take legal and ethical considerations into account. She also explained the legislative and regulatory framework in the US for advanced technologies at nuclear facilities that use ROWs and UAVs. In addition, she addressed some of the ethical considerations regarding biometrics and monitoring, the human workforce and responsibilities when technology outpaces regulation.

Participant Discussion

In discussions following the two presentations, participants commented that:

- The costs that have been mentioned during the workshop do not take regulations into account.
- When operators register a drone, they also need to acquire insurance.
- Operators need regulations if a malicious attack should occur. What should the operator do in a drone attack? What are the penalties of violating the regulation?
- Force (either lethal or non-lethal, depending on the country) may be used if operators are protecting a radiological source. However, the considerations may be different if it is a government-run or commercial facility.
- Every new technological system increases cybersecurity vulnerabilities and adds complexity.
- Having the mindset of just complying with the regulator in terms of security could be dangerous.
- Regulators may inhibit the deployment and success of new technologies.
- Regulators may not know what to do about cybersecurity because it is moving so quickly.

HYPOTHETICAL SCENARIO

Participants then had the opportunity to participate in a hypothetical scenario involving autonomous and remotely operated weapons. In the role of Security Director, they were asked to consider how they would develop a business case for implementing the new technologies, the factors they would need to consider, and the potential obstacles and risks they might encounter. The objective was to identify the top five factors that could be used to justify the investments.

Some of the major points and considerations generated by this exercise included:

- Security people cost more money every year.
- In reality, the shift to make an investment in security comes when there is an event.
- We need to be innovative in the field of security and commit to moving forward.
- People in cybersecurity open the eyes of experts in physical security. The nuclear industry needs to listen to its experts.
- There should be open communication and sharing of information. If there is an event, such communications will increase the workforce's ability to respond effectively.
- The modelling process is very relevant for the nuclear security industry and a game-changer when doing business. M&S in the wrong hands, however, could be dangerous.
- Operators can't simply cut all personnel. For example, trained people will be needed to operate the ROWs, and they will be more expensive. It is also important to consider the lifecycle of such technologies, as well as the additional costs for maintenance and operation.
- When introducing a new technology, the first 6-9 months will be used for evaluation and modelling simulations. Who should be involved in this process? Who will have the personal liability? All of this requires a change of management and the need to put a new programme in place.
- When introducing a new technology, operators need to demonstrate to the regulator how it will increase effectiveness, decrease costs, and remain compliant with the regulations.
- The nuclear industry needs to learn from other organisations and industries that have already deployed advanced technologies.
- Implementing ROWs will lead to cuts in the guard force. This can generate staff resentment, protests and even sabotage.
- Educating people about fundamental security requirements is key.

CONCLUSION AND WAY FORWARD

At the end of the workshop, participants were divided into small groups according to their job functions to share their thoughts on the way forward. Below are some of their conclusions:

Regulators

- The key thing is regulatory consensus.
- We need more education so we can better understand where the responsibilities and liabilities lie.
- Who is responsible for what? (WINS can help with this.)

Law Enforcement

- We need robust interagency cooperation, along with a good DBT.
- We need to understand the threats and consequences to deploying such technology.
- A solid legal framework is necessary.
- There needs to be a smooth interface between law enforcement, civil society and private industry.
- A media campaign is important.
- Making this happen requires political will, so government agencies need to be involved.

International/Government

- Such technologies require that everyone thinks out of the box.
- We need people who are capable of innovation. We also need to better understand how these innovations interact with regulation and how the bad guys are innovating.
- Such technology may be tested, but it isn't trusted. There needs to be a lot of assessment, forecasting and planning first.
- We need people who can communicate about such issues among different communities. (WINS can play an important role here.)

Operators/Licensees

- A balance between operators and regulators is necessary.
- Operators should pay more attention to the diversity of potential threats.
- Operators need to share their operational experience about this topic with each other.
- It is crucial to understand the feedback, avoid a defensive attitude, and be open to criticism.

Vendors/Consultants:

- We need to ensure that we understand the technology, requirements and regulatory process.

CLOSING REMARKS

Dr Roger Howsley closed the workshop by emphasizing that security is complex. It can no longer stand alone, but must integrate with safety. He also said that the industry is underestimating the speed of change and that the fact that stakeholders are increasingly unable to understand technology could be a big risk. In addition, Dr Howsley said that monitoring (of everything) will increase in near real time, making it much more difficult to plan complex missions without being detected. He reminded participants that ROWs also have weapons that are not lethal, such as sonar, lasers and pulses. He concluded by saying that advanced technologies should embrace social engineering and *weaponized psychology* and that big data analytics will be essential to handle the vast amounts of data.