# Workshop on Countering Violent Extremism and the Insider Threat in the Nuclear Sector

# London, UK. 3-5 December 2019

# REPORT – Draft for Comments

## BACKGROUND

In the past few years, States around the world have faced an increasing frequency of terrorist attacks perpetrated by individuals claiming to have been inspired by, amongst others, religiously oriented groups like Islamic State and Al Qaeda, and by right-wing anti-government militias and white supremacist groups. These attacks have led to the death of innocent civilians and shocked society by their indiscriminate violence.

Often referred to as violent extremists (VEs), such individuals pose threats that are generally not constrained by international borders or necessarily limited to any single ideology. The term homegrown violent extremist (HVE) is also used frequently to indicate people who perpetrate a violent act in the country where they were born and/or raised. Such individuals are often lone actors who might have been radicalised by passively consuming violent extremist material online. They tend to have few, or any, connections to radical groups or individuals in other countries before they engage in solo acts of violence. There is evidence that some extremists have targeted nuclear facilities when considering which malicious acts to conduct. Because the threat to the nuclear sector is credible, security arrangements need to be reviewed and enhanced, if needed, in light of the ever-evolving nature of the VE threat as it affects different parts of the world.

It is clearly the responsibility of the State to protect society from the actions of violent extremists and to understand their causes, methodologies and potential targets. Doing so requires contributions from many different stakeholders at the national as well as international level, including international organisations (e.g. the UN), government officials, intelligence, law enforcement organisations, civil society and individual citizens. Highly sensitive information may need to be shared among different organisations, and processes need to be in place to support such exchanges.

From the perspective of the nuclear sector, one of the most serious security concerns is that employees could become radicalised—or that already radicalised individuals are hired—and subsequently use their positions of trust and authority to carry out a malicious act.

Nuclear operators, with the support of other stakeholders such as specialised law enforcement agencies, can take concrete actions to protect their materials and facilities from insiders who are—or who could become—violent extremists. For example, they can develop a comprehensive insider threat mitigation strategy that provides the foundation for effective implementation of plans and procedures. This includes implementing specific measures for pre-employment vetting, as well as during employment behaviour observation and aftercare. Effective insider threat mitigation programmes should also include measures to reduce the risk of an unwitting insider who unknowingly assists an adversary in performing a malicious act.

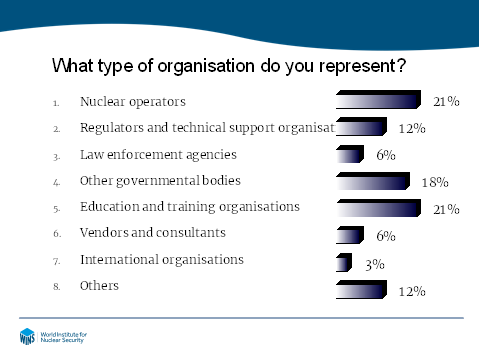
Countering VE requires that all individuals within the nuclear organisation play their part, not simply the Security Department. This begins with the commitment of leadership. Both executive and line management must demonstrate their belief that a credible threat exists and that nuclear security is important. They must lead by example. The human resources department also plays a crucial role by creating employment policies, procedures and programmes that support a security-aware culture amongst staff.

Due to the continuously evolving nature of the VE threat, the World Institute for Nuclear Security (WINS) periodically organises events to review the latest information on radicalisation matters and to listen to the experience gained by those who are implementing security arrangements against VEs.

Building on the main discussions and outcomes of its previous workshops related to violent extremism and insider threat mitigation, WINS decided to organise and conduct a three-day international workshop to review and discuss the latest developments on violent extremism and on all security matters related to VE and the insider threat.

## OBJECTIVES OF THE WORKSHOP

The key objectives of the workshop were to help participants:

* Develop a better understanding of the processes leading to radicalisation and violent extremism;
* Identify and discuss the motivation, intention and capabilities of VEs through real-life examples and applicable case studies;
* Understand the role of different stakeholders involved in the identification and mitigation of such threats with specific reference to the nuclear sector;
* Identify measures to ensure the reliability of personnel accessing critical areas and information;
* Assess whether the nuclear sector and its employment arrangements have any features that make it more or less vulnerable to becoming a VE target;
* Evaluate the resilience of the security arrangements against VEs; and
* Integrate best practices in countering VE threats from the aviation sector in their security programmes.

A total of 51 experts from 14 countries and three international organisations attended the workshop. They represented the main stakeholders involved in the mitigation of insider threats including nuclear operators, regulators, law enforcement agencies, civil society and security consultants. Participants were asked to have open discussions, express their own perspectives, and share their experience improving the security of nuclear materials and facilities against VEs.

The event, which was professionally facilitated by Mr Julian Powe, included expert presentations and various types of group discussions to provide maximum engagement. In addition, an instant electronic voting system was used to allow participants to anonymously share their views on selected questions. Some of the e-voting questions are included in this report.

## WORKSHOP PROGRAMME AND KEY FINDINGS

**Day 1: Wednesday, 20 November 2019**

### OPENING SESSION

**Pierre Legoux, WINS Head of Programmes**, welcomed the participants on behalf of WINS, explained the objectives of the workshop, and provided a preliminary overview of the agenda. Mr Legoux also displayed and commented on the most relevant results from the pre-event survey.

#### Participant Introductions and Expectations

To start the discussions, participants were asked to introduce themselves at their tables and discuss their expectations in coming to this event. Examples included:

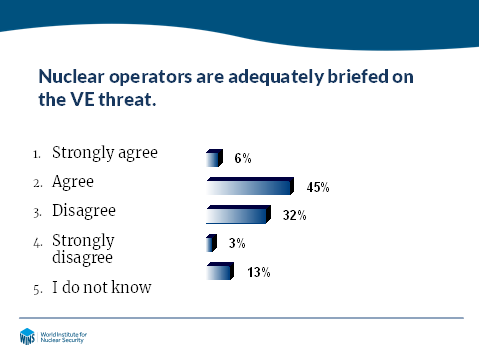
* Learning from others; increasing knowledge about mitigating the VE threat; transferring this knowledge back home;
* Sharing experiences and perspectives; adding value to the discussion;
* Expanding list of professional contacts in security and insider threat mitigation (networking); maintaining connections after the event;
* Benchmarking practices; understanding our strengths and weaknesses;
* Identifying best practices; finding concrete solutions to our challenges; developing a performance-based approach
* Better understanding behaviour observation programmes and how they need to take into account culture and regional matters;
* Discussing how to improve vetting procedures and adapt them to the VE threat;
* Reviewing methods to assess the effectiveness of the measures already in place.

## SESSION 1 – UNDERSTANDING THE VE THREAT AND THE RISKS TO NUCLEAR SECURITY

Session 1 was designed to clarify what we mean by “violent extremism” (VE) and how it relates to “terrorism” and “extremism”. It was also to review factors leading to radicalisation and violent extremism and develop a better understanding of the intentions and capabilities of violent extremists. The session was an opportunity to discuss lessons learned from real case studies involving extremists in the nuclear and non-nuclear sectors and to assess whether the nuclear industry is more or less likely to become a target of VEs. It was finally to identify a set of scenarios of concern to be kept in mind when discussing mitigation measures in the other sessions of the workshop.

**E-voting**

In order to initiate the discussions, participants were asked to answer an e-voting question related to the sharing of information on the VE threat.

A small majority of participants thought that nuclear operators were usually well briefed through different channels of communication with law enforcement and other specialised agencies. Some participants highlighted the fact that the quality and frequency of the briefings may vary a lot from country to country. It was finally agreed that the VE threat is difficult to predict and that the nuclear industry needs to understand the limitations of its knowledge in this area and implement flexible and resilient security arrangements able to adapt to this quickly evolving threat.

**Mr Samir Puri, King’s College London/Johns Hopkins University, UK,** opened session 1 with a presentation on *Trends in Terrorism and Violent Extremism: What is ‘Violent Extremism’, and How Does It Relate to ‘Terrorism’ and ‘Extremism’?* He started by describing the diversity of words and meanings related to terrorism and extremism and the difficulty to develop a common understanding. After summarising what could be consensus terminology, Mr Puri described the global trends in jihadist and far right terrorism and presented some key figures from the Global Terrorism Index 2019. He then continued his presentation by focusing on aspects of violent extremism and how it may relate to or differ from terrorism. Mr Puri also described possible radicalisation processes and associated factors. He concluded his presentation with the definitions of selected words that are used when characterising the radicalisation process and actions to mitigate violent extremists.

**Mr Diego Gambetta,** **Collegio Carlo Alberto, Italy,** then presented the key findings of his book *Engineers of Jihad*, which is an attempt to explain why so many engineers are among violent Islamists. Mr Gambetta started his presentation by introducing the initial data that indicated the over-representation of graduates, in particular engineers, among violent Islamists. He then explored possible reasons for this phenomenon, including the so-called relative deprivation factor and the personality traits which can make a person more susceptible to becoming a violent extremist. Mr Gambetta concluded his presentation with some guidance on how organisations can take actions to reduce the risk of disgruntlement among their workforces.

#### Discussion on understanding the VE Threat

In a group discussion following the presentations, participants further explored the VE topic and shared their perspective on radicalisation and violent extremism. Some of their main reflections are summarised below:

* Understanding of violent extremism is culturally specific. VE includes a “violent” component, not just extreme views;
* Poverty does not seem to be a direct cause for extremism. Certain personality traits seem more likely to radicalise;
* Evolutions of the threat are difficult to predict. We need to periodically refresh our assessment and acknowledge the limitations of our knowledge;
* Trends have radically changed over the past 20 years and will continue to evolve. (there has been a shift from traditional hierarchical groups with trained and skilled operatives towards “inspired by” actors, who are often individuals with no ties to the group. These are much less predictable and harder to monitor.);
* Fear of retaliatory cycles. Modern communication and travel capabilities may bring into the picture people who have no natural tie with the issues in play (e.g. Auckland attack in March 2019);
* The threat can come from an outsider who tries to infiltrate the system to become an insider, or through an employee who slowly changes his/her beliefs and attitude. Perceived lack of fairness within a group can lead to significant troubles;
* Mitigation measures exist! For instance, organisations can conduct a lot of engagement activities to create an appropriate culture amongst the workforce.

#### Group exercise on developing scenarios of concerns

Participants were then asked to form sub-groups and develop credible, realistic scenarios involving a radicalised violent insider. To introduce this exercise, Mr Puri presented five case studies on insider threats or radicalised individuals in the nuclear industry and elsewhere, including the aviation sector. The participants offered the following scenarios or situations for consideration:

* **Ideological threats**: An anti-nuclear movement wants to discredit the industry. An individual infiltrates a nuclear organisation (long-term strategy) to become an insider with access to sensitive areas and act when opportunity comes.
* **Emotional turmoil**: A significant emotional event could occur (such as the death of child, major financial issues, etc.), which gets attributed to an outside entity and causes an employee to engage in disruptive activity to find catharsis for their pain.
* **Revenge**: Desire for revenge for an illness perceived to be related to working conditions in the nuclear organisation (e.g. cancer) causes a worker to partner with a terrorist organisation and provide insider information facilitating access to the site.
* **Disgruntlement**:
* A worker has performance problems and is overlooked for promotion. They blame management and leadership and see it as an ethnic issue. Through social media, the worker thinks that a racial group is taking over the country, takes a gun to work and takes revenge on the company.
* The insider is a technician gradually disgruntled by lack of progression (discrepancy between what was promised and what was obtained). He joins a violent group and is used to sabotage assets.
* **Emerging technologies** in support of the malicious act: Insiders may use drones to bring equipment and explosive devices close to the target. This may include cyber-attacks.

## SESSION 2 – EXAMINING CURRENT BEST PRACTICE IN RISK MITIGATION AND EXPLORING THE REMAINING VULNERABILITIES

The objectives of Session 2 were to review the current strategies in place to mitigate the risk and better understand which stakeholders are involved. It was also to explore further the role of civil society in preventing the VE threat. Session 3 was finally an opportunity to listen to the aviation industry experience and discuss how to ensure the mutual transfer of experience (success stories) across various sectors.

**Presentations and discussion on developing a national strategy**

In order to initiate the discussion of Session 2, **Mr Abdulrazaq Olapeju Kazeem,** **Counter Terrorism Centre, Office of the National Security Adviser (ONSA), Nigeria**, presented the approach of his country to respond to and mitigate the threat of violent extremism, in particular from the Boko Haram group. Mr Kazeem described first some selected security incidents that have involved Boko Haram militants and how Nigerian law enforcement forces reacted to them. He then described some of the relevant regulatory framework for nuclear security in Nigeria and concluded his presentation with the main stakeholders and coordination mechanisms.

**Mr Gonçalo Simões, CBRN & Explosives Team, European Counter Terrorism Centre (ECTC), Europol**, provided a complementary presentation on *Mitigating Violent Extremism - R/N Law Enforcement Actions*. Mr Simões first reminded the group of Europol’s mission and how the CBRN and explosives team of the ECTC are supporting European countries to mitigate CBRNE criminality and terrorist threats. He also highlighted the importance of international coordination and how his team is cooperating with international organisations such as the IAEA and Interpol. Mr Simões then provided some information on terrorist incidents in the CBRNE area that occurred recently and on global trends in attacks and terrorist modus operandi. He concluded his presentation by describing some of the possible mitigation measures and key issues to be addressed to achieve effective CBRNE security against violent extremists.

**Follow up discussion on national strategies**

Reflecting on the key messages from the two presentations, participants were asked to discuss the main elements of an effective national strategy to counter VE. Participants offered the following list of actions to establish such a strategy:

1. Clearly define the role and responsibilities of each agency. Establish a chain of responsibilities. Be transparent and clear on who is supposed to do what.
2. Monitor the implementation of the strategy. Continuously review progress and reassess priorities. Consolidate lessons learned. What goes well, what does not?
3. Multi-support strategy (online; offline) with a risk-informed policy.
4. Include prevention and response measures in the overall strategy with a mix of hard and soft components. Also adopt a horizontal approach (not only top-down).
5. Establish a robust legal and regulatory framework.
6. Develop regional approaches and support international cooperation. Benchmark with other countries.
7. Assess and communicate the threat. Support awareness and understanding of the VE threat. Establish protocols for information sharing. Establish a good intelligence collection scheme to define the credible threat (DBT).
8. Ensure a national-level coordination mechanism. Assess impact of other State decisions on your strategy.
9. Provide the necessary financial resources.
10. Obtain leadership buy-in. Graded approach/focused approach/tailored to what is really needed.
11. Identify and engage with all stakeholders. Social/community responsibilities in raising red flags
12. Innovative vetting measures adapted to radicalisation
13. Develop training curriculum and exercises focusing on VE
14. Reward speaking out.
15. Support the development of competencies.
16. Do not forget that people in jail will be released. Anticipate!

**Break-out groups on stakeholder engagement**

After reporting on the table discussions, participants were asked to form six stakeholder groups (nuclear operators; regulators and other governmental bodies; law enforcement and intelligence agencies, including vetting agencies; civil society; academia; international organisations) and discuss good practices for engaging all stakeholders. A summary of the collective recommendations for a better engagement is provided below:

*Cross-cutting approach*

* Embrace diversity. Recognise different needs. Do not exclude anybody.
* Stakeholder mapping, education and engagement. Verify that strategy has been received and understood by various stakeholders.
* Avoid overlap and duplications (e.g. multiple expert groups on the same topic). Use resources effectively!
* Collaboration between not just state actors but also industry, private sector etc.
* Work is still in progress! It is a very complex issue and things are still very fragmented globally.
* Multiple actors. Coordination is a challenge. (e.g. 65 different organisations in Brazil).
* Try to get everyone at the same table to discuss protocols, develop relationships and ensure effective lines of communication. Provide the coordinating body the authority to oblige people to be there.
* Exercises in support of coordination. People gain by knowing each other.

*Strengthening Stakeholder Engagement*

|  |  |  |
| --- | --- | --- |
| **Operators**  Responsible for the implementation and effectiveness of the mitigation measures  Must ensure trustworthiness of the staff (with help from state agencies). Need to receive data in a timely manner but must then act on it  Responsible for recruitment, vetting, training, continuous evaluation and post-employment checks  Must ensure the development and integration of policies and procedures relating to the VE threat  Need to have openness in sharing experiences and incidents with other operators and countries (within appropriate fora) | **Regulators**  Set the framework, including embedding a VE component in the DBT, and ensure compliance with the requirements  Record incidents and support sharing of lessons learned at national and international levels  Support collaboration amongst different stakeholders and dissemination of threat information  Create a clear understanding of roles and responsibilities | **Law enforcement**  Develop a better understanding of behavioural matters in the nuclear context  Raise awareness and propose training on how to deal with RN matters and respond at facilities  Share threat data between operators and law enforcement. Ensure that the communication goes both ways and is listened to and acted on in a timely manner |
| **International organisations**  Their Member States need to:  Ensure that the mandate of these organisations is in line with the need.  Make the necessary human and financial resources available.  Verify that they effectively implement their mandates.  Multilateralism is essential in the development of a comprehensive international approach. | **Academia**  Good at facilitating dialogue (asking right questions, research at individual and geo-political level)  Can help to ensure diverse voices are heard  Can empirically test policies to check for effectiveness | **Civil Society**  Possibly one of the most critical and underutilised actors in mitigating VE threats  Can contribute to education, training, public awareness, act as an advocate for nuclear and good security  Create social networks and associations to support people combatting extremism  Can provide employees access to support outside of their work (including post-employment)  There are opportunities to strengthen cooperation between civil society (e.g. local communities) and operators. |

**Further exploring the role of the civil society**

Building on the findings of the break-out groups, Mr Powe dialogued with **Ms Farah Pandith, Council on Foreign Relations, USA**, to explore the role of civil society and other non-governmental stakeholders in mitigating the VE threat. Ms Pandith’s key messages were as follows:

* In the area of civil society engagement, limited progress has been made since 9/11.
* The ideology of “us vs. them” is on the rise.
* Three big players who could effectively improve the situation:
* Governments, including the public sector and multilateral efforts, could show leadership around soft power, funding opportunities and in setting the “tone” of the discussions.
* Corporations could ensure that resources and support are in place. Developing a corporate lexicon is important. As with governments, leadership tone is essential;
* Civil society – how you treat people on an everyday basis can make a big difference. Grassroots initiatives can have a real impact. Government can facilitate but they don’t know what is happening in the community itself – they need to find out what those communities need to puncture the us vs them mentality. They need to build resilient communities.
* Primary target is those under 30. What do we know about what they think about themselves? How does it affect their perspective and actions? How can we partner with local community groups to contribute to their sense of identity?
* Supply chains are affected by extremism - corporate money can be granted to NGOs to help keep these supply chains safe. Not all corporations will have the capacity for this, but they could collaborate or partner with other organisations and effect change.
* No difference between national and international strategy due to the digital world. How can we use all data positively to build global resilience and create online spaces to support positive views?
* No one predicted ISIS – we were focusing on specific regions of the world, and that was the wrong thing to do. The threat is now global.
* Social media: we need to understand how to teach children about the internet and also design and build the counter content. The number one idea is former extremists.

**Experience from the aviation sector**

**Ms Marie-Caroline Laurent from LAM LHA, France**, delivered a presentation on *Violent Extremism and Insider Threat in Aviation*. Ms Laurent opened her presentation by highlighting a few insider cases that happened recently in the aviation sector and providing some perspective on the diversity of potential insiders in the aviation sector and their possible motivations and tactics. She then described the applicable security requirements and the main elements of insider mitigation measures. Ms Laurent provided further details on some of these measures. She concluded her presentation by describing the arrangements for reporting and investigating suspicious activities and for sanctions and exit measures.

Answering some questions from the audience, Ms Laurent indicated that insider threats are one of the top priorities for the aviation industry and that most cases relate to theft for financial gain. She stressed the very broad range of possible insiders (Employees and subcontractors) and mentioned that aviation has international security standards (mandatory measures) in place. As a prerequisite to success, she stressed the need to identify all stakeholders and build a common understanding around insider threats. The insider mitigation programme needs to be integrated across departments.

Ms Laurent encouraged participants to build a company culture that makes them appreciate where they work and unwilling to harm colleagues. Ensure that you don’t leave your staff feeling that you think they are the bad guys. She finally mentioned that the HR and legal departments have a significant role to play, in particular when it relates to implementing background checks or when a person is repositioned whilst an investigation is underway.

**Closing remarks for day 1**

**Mr Mark Albon, Head of the Countering Violent Extremism Division for the Commonwealth Secretariat**, was invited to join the event cocktail and to deliver some closing remarks for the day. In his speech, Mr Albon reminded the group of the true nature of violent extremists: They use violence to achieve their goals; they are criminals and should be dealt with accordingly. He indicated that mitigation measures were available and encouraged participants to follow the MOM approach (motivation, opportunity, means). Although organisations have a limited grip on motivations, they can effectively act on opportunity and means. In conclusion, Mr Albon highlighted experience sharing with other sectors as a prerequisite to designing and implementing successful mitigation programmes.

## SESSION 3 – OPTIMISING VETTING AND BACKGROUND CHECKS IN A RAPIDLY CHANGING WORLD

The objectives of Session 3 were to review the best practices for an effective vetting regime and for ensuring the trustworthiness of individuals accessing sensitive materials or locations. It was, in particular, to assess whether changes or evolutions in our practices are necessary to take into account modern VE threats. The session also served as an opportunity to discuss the role of various internal stakeholders in mitigating the VE threat and how to strengthen their coordination and cooperation.

**Mr Eric Lang, PERSEREC, USA**, opened session 4 with a presentation on *Science-based Insights for Understanding & Mitigating Insider Threats*. Mr Lang started his contribution by reminding the group of the essential role of human factors in nuclear security and, in particular, to understand and mitigate insider threats. He then described how motivations and behaviours of insiders may vary a lot and the challenges in developing a reliable social science model for predicting individual insider threats. Mr Lang continued his presentation by providing some examples describing the magnitude of the insider threat and its relevance to all activities and sectors. He then offered some rationales explaining how a person may become a risky insider, detailed behavioural indicators of potential risk, and finally suggested some general mitigation rules and some more detailed measures to overcome barriers to reporting red flags and other suspicious matters.

**Follow up discussion on characterising the insider threat**

Participants were asked to reflect on the presentation and discuss their perspective on insider matters. Their consolidated perspective is described below:

* Technology is necessary but not sufficient. Human factors are essential.
* Need to consider both intentional and unwitting threats
* Motivations and behaviours are so varied that no model can reliably predict an individual’s reaction to a given scenario. People work to their own reward system.
* Behavioural indicators are useful, but also trust your judgement.
* Be reasonably transparent with employees about measures in place (develop organisational trust, e.g. no covert monitoring, tell them if their email is being monitored). You need to create active partners.
* Supervisor/co-worker reporting is one of the best sensors. They need to trust the organisation that issues can be reported and will be appropriately followed up.
* It isn’t uncommon for people to feel relatively deprived. Doesn’t matter if the perception is not true. You need to listen to their concerns.
* Manage expectations or a dangerous gap arises and creates disgruntlement.
* Attitude of management is critical. The way they act and communicate every day will make a difference.
* Ensure staff knows what the red flags are and that the responsibility to act is on them.
* The golden triangle (HR; Occupational Health and Safety; Security) needs to be addressed.
* Establishing a mitigation programme takes time. Speak to representatives of those with mature programmes.
* Culture matters. No “one size fits all”.

**Mr Wayne Jones, EDF Energy, UK**, provided a complementary perspective derived from operational experience in a presentation entitled *Personnel Security*. After providing some background information on the EDF Energy Hinkley Point C (HPC) Project, Mr Jones clarified some definitions around insider and personnel security. He then detailed the regulatory framework relevant to personnel security matters in his organisation, the strategic approach to personnel security risk assessment, and the five levels of pre-employment checks and vetting applicable to the workforce involved in the HPC project. Using a case study on the 2015 Germanwings flight incident, Mr Jones then challenged the participants and their organisations about their capabilities to notice and react to signs potentially reflecting an issue with a staff. He then stressed the importance of a strong security culture and the need for robust aftercare (post-employment), trustworthiness checks and fitness-for-duty programmes. Mr Jones concluded his presentation by displaying a video from the UK Centre for the Protection of the National Infrastructure (CPNI) highlighting the importance of reporting suspicious behaviours.

**Follow up discussion on possible insider mitigation measures**

In conclusion of session 3, participants were asked to continue the initial discussion on insider matters and to start proposing some measures to mitigate this threat. Some of their suggested fixes are listed below:

* Define expectations for the staff. Increase their awareness. Offer necessary training and education opportunities.
* Conduct role-based risk assessment linked to VE.
* Leadership training for managers (often they are technical experts) - Make sure they know the expectations and are educated in how to respond to concerns and create security culture.
* Adapt to different generations in the workforce: They deal with information differently and might have different indicators of what is the norm.
* Transparent communication is vital.
* Make sure each individual understands how important their role is in maintaining security.
* Share anonymised cases of incidents within the organisation. Dispel the “it’ll never happen here” thoughts.
* Conduct monitoring of social media and employees’ actions in public fora.
* Create a safe environment. Ask employees how they think the personnel security and insider threat system works and what concerns them and build on that dialogue. (What is their role? Is it intrusive? How could it be better?).
* Bring together safety and security.
* Team building outside the office environment: The more processes to connect with each other, the more we will be able to see any deviations.
* If resources are limited, go for low-hanging fruit.

## SESSION 4 – RED FLAGS AND THE ART OF THE POSSIBLE IN THREAT MITIGATION

Session 4 was organised to review good practices for designing and implementing behavioural observation programmes and how to educate managers and staff to detect red flags and effectively report their concerns. It was also to explore the legal and ethical challenges with human reliability programmes and how to keep a balance between security needs and privacy rights.

**Ms Wendy Anyster, Occupational Psychologist, The Leadershipvine**, opened session 4 with a presentation on *Behavioural Assessments: Processes, Practices and Tools*. Ms Anyster started by defining what behaviour is and explaining that only a small part of it is visible while the vast majority of our behaviour influencers remain invisible. She then described some personality traits, highlighted the main questions to be considered when assessing a workforce, and described some of the personality attributes that are core to safe, secure and effective performance. Ms Anyster continued her presentation by describing the process to follow to conduct objective, valid and reliable behavioural assessments and explained how to use such assessments during the recruitment of personnel for sensitive positions. She concluded her presentation with an introduction on the upcoming IAEA publication on *Guidelines, Methodology & Practices to Assess Behavioural Competencies for Safe, Secure and Effective Performance throughout the Employee Life Cycle*.

**Discussion on behaviour observation programmes**

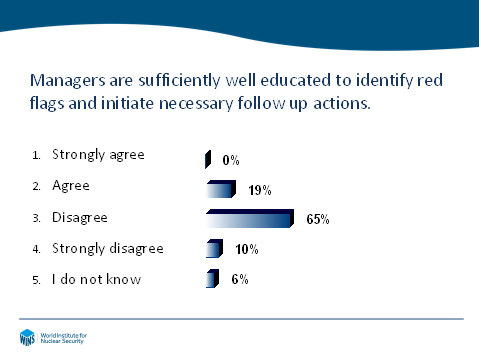
As with some previous speakers, participants were then asked to have discussions at their tables to reflect on the key messages of the presentation and share their perspective on the topic. They reported the following issues:

* Visible observable behaviours are the tip of the iceberg: We need to dig deep to understand what is influencing behaviours (beliefs, motivations, personality, competencies, etc.).
* People are complex. You will never fully understand people.
* Often individuals don’t recognise their own early warning signs, which can help with self-awareness.
* We need to define what good behaviour means and looks like.
* In job descriptions, define not only roles and responsibilities but also competency requirements (not just tech skills but soft skills). Core personality attributes required need to be reflected in hiring and training.
* Organisations need to use multiple forms of assessment to identify behavioural patterns. Follow an integrated multi-level approach and combine different bits of information.
* Periodic assessments are crucial: People change over time and their situations change over time!
* Inclusive and engaged work environment: If these needs are not met, it doesn’t matter how good your processes are.
* To facilitate behavioural change in an organisation, set clear expectations, role model (right behaviour), give feedback and positively reinforce.

**Exploring the role of social media**

**Mr Jakob Guhl from the Institute for Strategic Dialogue (ISD), UK**, made a presentation on *Social Media and Violent Extremism*. Mr Guhl started his presentation by exploring the role of social media and extremist content as possible causes for radicalisation. In particular, he described the geographic hubs of jihadist recruitment and reviewed social bonds and the potential role of pre-existing networks. Mr Guhl then provided some statistical information highlighting the importance and increasing role of social media during the radicalisation process, especially for lone actors, and its possible contribution to reducing the duration of this process. In the second part of his presentation, Mr Guhl presented selected content of online materials related to extremism and radicalisation. In the final part of the presentation he explored possible actions by tech firms hosting such content and presented some guidance documents supporting an effective response to extremist online materials.

During the follow up discussion, it was agreed that the role of social media had increased since 2011, but it was considered that it was rarely the primary driver of radicalisation. It was agreed that overall governments should be held accountable for regulating social media but it was also noted that disinformation tactics (e.g. fake news and bots) are complicating the landscape. Looking at what nuclear organisations might do, it was stated that social media monitoring is an expensive and complicated thing for a company to do and that it may raise privacy and data protection issues.

**Educating staff and managers to identify red flags and reporting serious concerns**

**E-voting**

To build on the discussions conducted around behaviour observation programmes, participants were asked through e-voting to indicate if they believed that managers were sufficiently educated to identify issues (red flags) and take follow up actions. Participants expressed a strong disagreement and indicated that a lot of barriers were still preventing effective detection and reporting by managers.

Participants noted that these managers are primarily held accountable for delivery and performance and don’t always have time for other matters. It is also hard to measure their actual contribution to the detection and reporting of problems and to make them accountable against a quantified objective (which is a strong driver for their actions and attitudes). It was also mentioned that managers are not a static group (high turnover on many projects) and that long-term actions and engagement are difficult to implement.

Participants also mentioned that many managers face social pressure, which limits their capacity to take coercive actions against a member of the group. Some managers might be reluctant to deal with these things because of potential consequences (e.g. sacking people). Participants also agreed it was rather easy to hide behaviours from line managers and that direct colleagues often have a more representative view of how people really feel, especially in big teams.

**Improving detection and reporting**

* Branding can make a difference to ensure it isn’t perceived as a punitive programme. Things happen in life, and people sometimes need support. We are all “insiders”. We only become a threat when certain things happen.
* Create a culture which emphasises all aspects of an organisation (operations, safety and security) equally.
* HR are the first line of defence – they need to be educated properly.
* Culture always supersedes policy: No policy can succeed if you haven’t got the right culture in place.
* We need to hold people accountable for the culture they instil and not just for their work deliverables.
* Insider threat isn’t a great term: insider assurance might be better.
* Some people do not like the term red flag. It can be aggressive and make people feel like they are targeted.
* You need to frame your terms around the result you want.
* Psychological safety is a pillar of nuclear security. We need to make a safe space where people are willing to be vulnerable and say what they think and feel, and this needs to be modelled by managers.
* Managers need to be trained to communicate concerns in a caring way. Tools should be available to help managers get more specific about their concerns.

**The role of the human resources department**

**Ms Alison Bell, King’s College London, UK**, provided the last contribution of day 2 with a presentation on *The Role of HR in Mitigating Insider Threats: Reporting of Behavioural Indicators*. Ms Bell first reminded the group of the personnel security controls and measures implemented by an organisation during the full employment period to ensure the trustworthiness of a staff member. She then described the specific role of the human resources department in supporting the detection of changes in behaviour, facilitating the reporting of the information and ensuring proper follow up actions. Ms Bell concluded her presentation by highlighting the complexity of the insider threat, the influence of human factors and the importance of bringing all internal stakeholders together.

Participants were then offered a final opportunity to reflect on the key issues of the day, and in particular on the role of the human resources department in supporting the security function and the entire organisation in mitigating the VE threat. Participants reported the following key points:

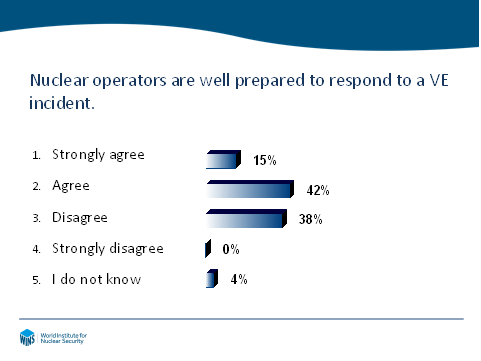
* HR plays an important role in mitigating the insider threat, and in particular can act as a hub for reporting, but it needs to be combined with other functions (e.g. security, legal, etc.).
* During recruitment, consider who gives the interviews and whether they have had training regarding what to look out for, how to check any gaps in CVs, etc.
* HR has a role when people move, change job roles or have any grievances; organisations need to ensure it is not just line managers who do this.
* People are reluctant to believe their colleagues are planning something bad.
* Seniority of the actor can inhibit reporting (fear of reprisal).
* Relationships are vital for the procedures to work, but these relationships can be strained due to the different targets and priorities of the different departments.
* Anonymity can facilitate reporting but can also inhibit action because of lack of evidence.
* Sometimes security breaches are due to an unfortunate situation rather than the deliberate misbehaviour of an individual.
* Organisations need to ensure people leave well and not create disgruntlement at the end of employment.
* HR’s function should be to manage the human resources, not just recruiting and salaries but also career development etc. We have to remember that they also have budget constraints.
* Security and HR need access to shared IT systems to see the relevant information including security clearances.
* HR needs to have a better understanding of the threats.
* HR may have devolved many of their responsibilities to line managers and may have very little interface with the actual people in an organisation.

## SESSION 5 – RESPONDING EFFECTIVELY TO A VE INCIDENT

Session 5 was organised to share actual experience in responding to insiders or VEs and to exchange perspectives about good practices for responding to a violent extremist. In particular, it was to assess whether response practices for VE should differ from practices for other threats and if security arrangements should reflect these differences.

**Mr Gleiber Banus and Mr Cesar Romão, National Security Cabinet, Presidency of Brazil**, delivered a presentation on *Brazilian Experiences in Violent Extremism and Cybersecurity*. After summarising the overall Brazilian approach to nuclear security and stressing the importance of involving all stakeholders in the protection of nuclear installations, Mr Banus and Mr Romão described a series of incidents that occurred in the vicinity of a nuclear site or nuclear transport. They also provided some details on the cybersecurity arrangements implemented for the nuclear sector. They concluded their presentation by highlighting the importance of sharing experiences and transferring lessons learned from the past to build sustainable and resilient security regimes.

**E-voting on the** **preparedness of nuclear operators to effectively respond to a VE incident**

In order to initiate the group discussions on response arrangements, participants were asked to provide their opinion on the preparedness of nuclear operators to effectively respond to a VE incident. A majority of them indicated that most operators were well prepared and already had strict procedures in place to react to numerous situations, including active shooters and other violent incidents. They indicated that Security Departments are more and more encouraged to think dynamically about the different ways in which a threat might materialise and what immediate actions are needed to interrupt and neutralise the adversary.

Participants nevertheless suggested some areas for improvement such as better communication between the different internal and external players involved in the response procedures. They also stressed the time to respond as the key element of success and the value of training and exercises, including “red teaming”, to practice arrangements and ensure an effective integration of various players. Participants reiterated the importance of working closely with the intelligence community to understand the trends in the VE threat and get actionable intelligence.

## SESSION 6 – MEASURING THE EFFECTIVENESS OF MITIGATION PROGRAMMES

The last technical session of the workshop was organised to discuss how the different elements of a human reliability programme can be measured for their effectiveness individually and in their entirety. It was also an opportunity to identify and discuss some performance indicators that may characterise an insider mitigation programme. Finally, the session offered participants the possibility to discuss good practices for integrating the insider/VE risk into the overall risk management structure of an organisation.

**Ms Karen Kaldenbach, Oak Ridge National Laboratory (ORNL), USA**, delivered a presentation on *Assessing the Performance of Security Arrangements Against Insider and VE Threats*. Ms Kaldenbach started her presentation by detailing the main components of a security programme and offered a structured process to conduct a security assessment (identify, analyse, mitigate and manage). She then focused on the human aspects of the security programme and described the steps to be followed during the assessment of human reliability programmes, including behaviour observation programmes. Ms Kaldenbach concluded her presentation by describing the main outputs of the HRP assessment process (statistics and performance metrics; incidents of concern/investigations; corrective actions).

As a follow up to the presentation, participants were asked to form small groups and prepare a presentation to the Board of Directors of a nuclear facility that is asking for evidence that the insider mitigation programme would be robust enough to counter a violent extremist. Participants were asked to offer some insights on performance indicators, the role of vulnerability assessments, and the level of integration of the insider risk programme in the overall risk management structure.

## WAY FORWARD AND CONCLUSION

In the last activity of the workshop, participants were asked to form small groups based on their country of origin, reflect on what they had heard and discussed during the previous two days, and identify concrete steps they would personally or collectively take to improve security arrangements against VEs. Participants then discussed the main findings of the event as a whole group and shared a few of their takeaways and possible follow up actions.

In his concluding remarks, Mr. Legoux thanked the participants for their active contributions, which made the event a success. He encouraged them to build on the key findings of the event and to contribute proactively to the strengthening of nuclear security at all levels. He also committed WINS to building on this success and to update WINS’ programme of work to reflect the priorities expressed by the participants. Mr Legoux also indicated that WINS will complete the revision of its international Best Practice Guide 3.8 on *Countering Violent Extremism and Insider Threats in the Nuclear Sector* based on the findings of the workshop and will release it in early 2020.

During the evaluation session, 100% of attendees expressed satisfaction with the event and the facilitation process. 93% of them indicated they would recommend this type of event to others. In their individual comments, participants confirmed a high level of satisfaction and said they particularly valued the quality of the speakers, the expertise of the participants, the amount of information shared during the three days, and the overall atmosphere of trust and exchange.