World Institute for Nuclear Security

EVOLVING SECURITY THREATS AND ADVANCED SECURITY TECHNOLOGIES

19 – 21 March 2018

Vienna, Austria

INTRODUCTION SESSION

TABLE DISCUSSION - EXPECTATIONS

1. Learn 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. Identify gaps in current systems – where can technology help?
6. Benchmarking and networking
7. Explore performance based solutions
8. How can we leverage technology?
9. What is the regulator’s perspective?
10. What are the future threat factors?
11. What is the interface going to look like between safety and security?
12. Explore cyber and A.I.
13. How can technology help as a retrofit or for a new build?
14. What are the gaps in the technologies?
15. Societal considerations?

STAKEHOLDER DISCUSSION – START

1. What about the residual risk that we carry with us?
2. Are these threat trends applicable for other targets as well? What about soft targets?
3. Prediction models aren't always accurate or helpful.
4. Shouldn't discount risks that were previously disregarded – don't park these and turn away from those risks?
5. Emphasize revenue - Cost of prevention and clean up – link it to the risks.
6. Recognize that you can't predict the future – but the role of the insider seems key in terms of giving an opportunity.
7. Difficult to quantify the insider threat and defend against it.
8. Capability of the insiders – what is being done out there?
9. Do we know what the technology can do?
10. What are we protecting against.

Risk = "Threat x Vulnerability x Consequence"

James' response:

- What is really needed for improved analysis – insider technologies
- Focus also on the lower cost threats.
- Even the smallest attack is novel for adversaries.

SESSION I

EVOLVING THREATS

Plenary Discussion - Cyber

1. What is the coping mechanism?
2. Need for a cyber security regime?
3. Should we move back to analogue systems?

SESSION II

ADRESSING FUTURE THREATS – AN INDUSTRY PERSPECTIVE

“Can Security Keep up” Discussion

- **Agrees:**
  1. Fairly enough knowledge
  2. There is a real drive to do the job right
  3. Exchange of information

- **Disagrees:**
  1. Tactics of today are changing
  2. Prediction is a challenge
  3. Institutional inertia – reactive rather than proactive
  4. We aren't being “tested” properly.
  5. Demographics – younger generation – collective memory
  6. Availability of information helps the attackers
  7. Challenging to get ahead of cyber – can enhance physical threats.

IF WE WANT TO - WE WILL DO IT, IF WE CANT WE GET CLOSED DOWN!

“FUTURE“ DISCUSSION – SMRs / Horizon

1. ALARP concept for security?
2. Clean slate
3. Integration of safety and security can be improved
4. Outcome-focused risk based regulation is providing the necessary freedoms to design security differently from the beggining.

BREAKOUT DISCUSSION – 2025?

Group 1 (Gold Stars):

1. Cyber
2. Liability provisions for software
3. Partnering cyber security and nuclear companies
4. Clever regulations
5. Export controls set up by countries
6. Decisions by AI – where is the liability? – evolving landscape – can't be fully assessed.
7. Social media flash mob threats – chaos – can't see it coming
8. Risk – staff loyalty – different values
9. Regulate dual use technologies

BREAKOUT DISCUSSION – 2025?

Group 2:

1. Generation change
2. Need another set of controls that are complementary
3. 3 dimensions - quantum computing?
4. Beyond the perimeter – drones / radar – foresee potential risks
5. Open source intelligence – diverse threats – what is it going to look like?
6. “Lifi” technology – more secure than wifi
7. Look at this issue through the eyes of the operator
8. Leverage machine learning and A.I. and try and reduce the operators workload

BREAKOUT DISCUSSION – 2025?

Group 3:

1. What is the cyber landscape going to look like?
2. A.I. – what are the capabilities – offensive and defensive?
3. Transitioning some capabilities back to analogue but what is going to happen then?
4. What about the supply chain? What can be introduced to the supply chain?
5. Insider threat is a constant threat – what tools can we use to vet our employees better?
6. Radicalisation – what is the trend?
7. How can we better control our systems – „airgap systems“?
8. How can we leverage M&S tools?
9. Proportional response

Review of Day 1:
What stands out? / What needs more attention?

1. Cyber threat link with the insider threat
2. Cyber is a domain of warfare – pursuing a group isn‘t always allowed (nation policy considerations)
3. 3Ss – how do we make it sustainable? What is in it for me – to create buy in. Avoid clashes between the disciplines.
4. What principles do we need to make sure that we are achieving this – sustainability/culture?
5. Education of people – sustainability
6. People and the insider risk – how do we monitor insider risk?
7. Cross pollination on insider issues – Banks etc.
8. Stronger guidance on horizon scanning particularly around threats.
9. Cost benefit? Under a lot of scrutiny.
10. ”Missions to remove assets”- psychological aspects? Powerful lessons came out of pushing the boundaries.
11. Simplification
12. How do we build technical competencies?
13. What kind of cooperation is required?
14. Who takes the risks that come with the technology?
15. What is acceptable from a regulator’s perspective?

SESSION III

ADVANCED TECHNOLOGIES AND THEIR IMPACT ON NUCLEAR SECURITY

UAVs

1. Can UASs be used as a deterrent? Perhaps more on the delay side of things?
2. Forensic studies on captured drones – wealth of information can be mined.
3. No silver bullet
4. Fast paced market
5. Neutralisation aspects require specific areas

Robotics

1. Is there potential of a lot of information capture? What is the residual data on this? Does it become an asset that needs to be safeguarded?
2. Modelling and Simulation helps support the robot but it can also map the site after a few times. 3D scanners are on the device.
3. Power management?
4. Automated inspection schedules

TABLE DISCUSSION – VR

1. Voice recognition will increase – instruct the machines what they should do.
2. What threats and vulnerabilities do we have once VR is introduced more?
3. What does it cost to develop such VR lessons? With a high cost involved it must have a broad application.
4. How can we activate other senses with VR?

Panel and table discussion – UAVs, Robotics and AR/VR

1. Regulations can't keep up – partnerships across industry and vendors to speed this process up.
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. Democratisation of technology – what are the trends?
5. When do we jump into a technology?
6. Anxiety when a technology becomes a type of "compendium" of your assets.
7. A lot of unknowns.
8. The less people touch the "material" the lower the insider threat is.
9. Best practices for use and best practices on the dangers.
10. Technology which helps safety and security – helps their implementation at sites
11. Build a model for assessing, tracing and deciding on investment in different technologies
12. More help (WINS, IAEA etc.) in supporting this
13. Reputational damage – enormous risk for the operator
14. Diffusion of access – certain information becomes broadcast via AR training materials

SESSION IV

EXPLORING THE ROLE OF ARTIFICIAL INTELLLIGENCE IN NUCLEAR SECURITY

A.I./ Data Analytics

1. Both sides (good and bad) will be doing something – that's for certain.
2. Data analytics – been around a while
3. Searching for who is who and what is what can create trouble.
4. State priorities vs. Business priorities
5. How far have we gone with data analytics in business?
6. What about the aftercare?
7. Analytics may cross laws.
8. If it is more efficient let's do it. And our networks.
9. How do smaller nations/organisations deal with data analytics and A.I.? Are they even capable of running such systems?
10. What is the maturity of the nuclear sector? Are we leaders? Fast adopters? Slow adopters? Will we be forced into it?
11. If we are slow - we need more partnerships with other sectors (banking etc.)
12. Apply these tools to supply chain management and other areas
13. Might be a stretch in the rad. security world
14. If they deliver important answers – what are the important questions?
15. People aspects

SESSION VI

MODELLING AND SIMULATION TOOLS IN SUPPORT OF RISK MANAGEMENT

Plenary and table discussion – M&S

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’ – why are you putting something in.
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. Cyber requires live databases as these things change. Physical systems don’t change in their breach times. Cyber keeps changing.
9. Cyber realm is opinionated vs. real data in the physical realm.
10. Modelling isn’t absolute.
11. Not every event starts with a “bang” – sometimes there is a lack of imagination.

Plenary and table discussion – M&S

If we are going to do a really good job on M&S in the next few years, nuclear security needs to …..

- Interlink safety and security in models rather than testing them separately.
- Create a justification beyond money
- Understand softer issues
- Account for varied adversary intentions
- Utilisation of a variety of tools to identify the problem, train for the problem
- Globally accepted
- Consistent regulatory guidance
- Good data in – good data out
- Defence in-depth on safety and security needs aligned
- Honest and transparent on the results
- Information modelling
- Recognise the strengths and limitations
- Address airborne threats (Drones)
- Make it useful for the operators (ex. demonstrate usefulness during an outage) - easier to sell
- Make sure the threat is real and credible - not something random
- Link in with other technologies
- Cost to join the party is high – conduct limited trials to help justify what you will implement – trial versions need to be available.
- Independent validation
- Empirical validation
- Tool simplicity required

CONCLUSION SESSION

Themes for the report

- What is the value to the business
- Establishing networks and partnerships
- Defining effective performance thresholds
- Modern workforce, how to integrate the future workforce with new technologies
- Modelling of future concepts
- What next?
- Strategy for horizon scanning is needed
- Not too prescriptive
- Common language across the industry
- How to engage the public
- Is the current understanding and description of cyber readiness shared between the regulator, operator, vendors, etc.

What are you going to attend to (group thought) when you get back:

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