"Information Dominance and Cyber Security at various Crossroads – Challenges and Solutions in the Cyber-Physical World"

TechNet Europe 2019, 23rd and 24th October 2019, Crowne Plaza Hotel in Bratislava

Session 1: Securing the IT Supply Chain – Is it All We Need for Comprehensive Cyber Security?

Considering the immense risk of cyber terrorism, data theft, malware implementation and the exploitation of hacking opportunities, new approaches for cyber security throughout the IT supply chain must be found. Cyber security, of course, is much larger in its aspiration to secure the functioning of networks and systems, but there is a fundamental need to have a concise strategy, embedded into the national cyber security strategy, which reduces dependence of suppliers from potentially adverse countries and peer-competitors and safeguards intellectual property protection. Dealing with such challenges in a supra-national environment with global supply chains requires trans-national innovative security standards and a trans-national certification regime or process. It definitely will have an influence in how government is doing procurement. The private sector, being the technological leader in many places, can contribute significantly here as well.

Key questions that need to be addressed, amongst others:

- Are we aware of all vulnerabilities?
- Are we able to monitor the supply chain?
- Are there new approaches for built-in security?
- How to modify IT architecture to allow a secure supply chain?
- What to do if corruption of hard- and software is discovered?
- How to rebuild a system of trust?
- Who is able to test and verify compliance?

Panel 1: "Hidden Risks in Governmental IT – How to Overcome Them?" – *Concepts and Technologies against Hidden Threats in Hardware and Software*

Session 2: "Smart Perimeters" - What Border Security and Military Surveillance have in Common

Automation of surveillance and prediction of people's movements and behavior are the main focus area where modern data analytics and sophisticated algorithms play the most important role. While maintaining strictly separate responsibilities for external borders and military applications in the field, interchangeable concepts and solutions, provided by academia and industry, should benefit both sectors. Every wide- or near-area network requires sophisticated IT security solutions in order to safeguard its integrity and inviolacy. Cyber defence for the protection of systems with numerous desktop stations, automated high-resolution sensors, highly sensitive data bases, and humans in the loop is facing new challenges both with regard to the dimensions, time critical implications and the interaction of IoT components with mass data analytics.

Key Questions that need to be addressed, amongst others:

- How far away is the "Biometric Border"?
- What are the newest technologies for battlefield surveillance?
- How do we measure effectiveness in this field?
- Will Big data analytics needs to be adjusted with the confluence of IoT data and new expectations with regards to facial and behavioural recognition?
- How does Artificial Intelligence come into play?
- How can GDPR questions been solved?
- What role can smart perimeter capabilities and cyber forensic play in securing evidence for advanced law enforcement?

Panel 2: "Digitalisation at the Border" – *New Approaches to make Border Security even Smarter*

Panel 3: "Information Dominance in Support of Combat" – *Smart Perimeter Surveillance Contributing to an Agile Battlefield and Improving Situational Awareness*

Session 3: Securing Weapon Systems Operations by Deeper IT Interoperability and Increased Cyber Security

New, modern weapon systems, like 4th generation fighter aircrafts and more and more commercial-of-the-shelf devices, like future vehicles, will interact with the Internet of Things. A new approach for increased fleet or domain effectiveness is required. Seamless and secure exchange of information and effective and automated communication between all the elements will become vital for mission success, e.g. in a much deeper integrated sensor-to-shooter cycle. There is a need to analyze how improved interoperability can be achieved through common data standards. Communication networks will have to adapt to this new tasks in the age of digitization towards a "Military Internet of Things". While some applications like predictive maintenance are becoming standard already today, the integration of autonomous systems both as platform and as C2 tool and a new network centric collaboration in order to gain information dominance and thus mission effectiveness will pose the ultimate challenges.

Key Questions that need to be addressed, amongst others:

- How does the connection of weapon systems and communications networks affect mission effectiveness and how can they be protected?
- How will digitization of the battlefield shape the relationship between communications, command and control, and proprietary software of weapon systems, sensors, effectors in a new network centric approach?
- How to incorporate legacy elements into that system of collaboration?
- How to be prepared for the advent of autonomous systems?
- What are the effects on structure, human workforce, and procedures of the armed services and the police force?

Panel 4: "Let's Prevent Cyber threats to the Soul of Modern Weapon Systems" – *How to Defend Proprietary Weapon System Software against Cyber Attacks*

Panel 5: "Future Network Capabilities for Deeper Integration of Modern Warfare" – *Concepts, Methods and Technologies to Improve Weapon System Effectiveness through Cross-Domain Interoperability*