"Resilience in Sync with Digitalisation: How to Master this IT Challenge of NATO & EU Forces"

Programme Overview

18 September 2024

Pre-Session Keynotes

How to foster resilience while moving forward with digitalisation? Cross border contemplation Gov sector – private Sector – Defense and Security sector (or: Society – Economy – Military); themes (examples) relevant to all 3 sectors, technology plays a role in all the themes.

Pre-Session Panel: "Taking stock – High-level panel on the status of Digitalisation in Defense - Digitalisation and its relationship to resilience"

The panel focusses on the status of digitalisation in NATO and selected nations, on imminent steps for further implementation and on the actual impact on resilience in the respective Armed Forces.

Expected outcome: Understanding the relationship, identifying areas of concerns, providing information about actual programmes and activities.

SESSION 1: "Resilience is nothing without Critical infrastructure protection"

In the current times of war, a new yet old dimension of warfighting resurrects to life: Physical and Cyber attacks on critical infrastructure. Even in times of peace or increased tension, threats to the same core group of industry are present, although for different motivations like crime or de-stabilisation. Following the common understanding, this type of warfare is called Hybrid war. Information operations can be part of it.

Such warfare, occurring in a magnitude of various forms, on a wide scale and at manifold places, makes it challenging to react in an efficient and comprehensive way. The protection of the complex system of Europe-wide connected critical infrastructure against attacks is vital for the resilience of society but also for the functioning of the Armed Forces in any member state of the Western alliance. Harnessing the various branches against all types of threats, preventing attacks, and

recovery operations after attacks, rely on modern technology. The ongoing digitalisation, also in this infrastructure, increases the attack surface but also provides more precise situational awareness, fosters technical robustness, and supports resilience e.g. by network redundancy.

All the old and new forms of threats, like using cyberspace for disinformation or physical interference (disrupting underwater critical infrastructure, jamming space-based services like GPS, tinkering with industrial IoT, conducting aerial attacks on power plants) were emerging in the recent past at an alarming rate and call for organisational and technological means to counter these threats. Although civil emergency and protection is a national responsibility and is highly developed in the Nordics, NATO, and the EU have recently stepped up to provide overarching concepts and support, also in the interest of defence and security of the member states. Industry contributes with a large variety of technologies, from cyber defence tools, and electronic hardening of devices to information systems and situational awareness. Interconnecting such activities with governmental and open-source intelligence improves response efficiency and capacity.

This session is about interconnecting governmental agencies responsible for homeland security, military, research, and industry for deepening analysis, generating greater understanding, and exchanging views on concepts, needs, required actions, projects and technological solutions. The purpose is to resolve infrastructure security and resilience knowledge gaps, inform infrastructure risk management decisions, identify resilience-building opportunities and strategies, and improve information sharing among stakeholders through a collaborative partnership approach.

KEYNOTES

Panel 1: "Resilience in critical infrastructure – essential for defence forces as a whole"

Considering the content of the preceding keynotes, the panel will discuss the importance of secure and resilient critical infrastructure as a backbone for defence and for supporting military operations as well as for the stability of a nation. It may identify weaknesses (policy, practical) and will highlight actions undertaken. Key technologies to foster reliance will be addressed.

Expected outcome: Providing a clearer picture of responsibilities. Identifying areas of concern but also reassurance of progress and actions taken. Outlining future challenges and helpful technologies.

SESSION 2 (part A): "Artificial intelligence, automation/autonomy and data: Their ambiguous impact on resilience and digitalisation"

The year 2024 seems to have become a pivotal time for the implementation of Artificial Intelligence in Defence and security. Never have drones been so decisive in battle. Data policies for unearthing the immense potential of AI and LLM for decision advantage are jumping off the ground, and regulatory frameworks for the production and responsible use of AI applications are provided by the EU, NATO

and other nations. (Generative) AI seems to become a technology of everyday use for everybody. At the same time, risks and challenges are more obvious than ever: Fake news and videos, bots, intelligence-supporting tools, and cloud security are only a few elements of the current debate.

Against the background of the Ukraine war and war in Gaza, the role of AI and its implementation in a wide set of technologies for further bolstering digitalisation and increasing resilience, notwithstanding the adversarial effect that AI can be applied to reduce resilience and hamper digitalisation.

This session may discuss the newest aspects of the ever-increasing role of AI in intelligence, analysis, and decision-making, the requirements for the protection and provision of high-quality data, the governing and organisational impact of implementing AI in military processes, and the cultural consequences which come with transforming the workforce into an AI savvy workforce.

The essential role of standardisation and the intelligent use of data in Multi-Domain Operations across sources, domains, and partner nations is worth a debate.
It also may visit the various concepts and projects of the military journey to the cloud, both on NATO and national level, different approaches, and solutions, as well as security aspects for high-sensitive data whose necessity has become more obvious lately.

Ultimately, the progress in autonomy and automation on the battlefield may be discussed as well as the way ahead toward "The Future of Robotics". At the same time, it is inevitable also to present and assess protective technology against robotics (drones) and the economy of measures/countermeasures.

KEYNOTES

Panel 2.A: "Where are we right now? Examples of use cases"

- End of programme day one -

18:30 – 20:00 Reception by the Mayor of Helsinki (City Hall)

19 September 2024

Pre-Session Keynotes

SESSION 2 (part B): "Artificial intelligence, automation/autonomy and data: Their ambiguous impact on resilience and digitalisation"

Panel 2.B: "Where are we heading towards? Challenges and opportunities…and security risks"

Considering the content of yesterday's and today's keynotes, the panel will focus on the dependencies of advanced autonomy on AI, data quality and supporting technologies. It may discuss future forms of automation/autonomy in warfare and the procedural and technological prerequisites.

Expected outcome: Understand the relevance of advanced robotics for future warfare; get an impression of future developments; develop candour towards unconventional means of employment and use cases. Discuss new effective technologies for protection against new threats from drones, robots etc.

SESSION 3: "Cyber security: New threats, new solutions - who has the upper hand?"

The geostrategic tensions increase the activities of malign state and non-state actors in cyberspace. Attacks are becoming even more sophisticated and targeted, using AI as an enhancement, and exploiting vulnerabilities in the ever more complex software stacks. VPNs are no longer immune to hacking. Supply chain attacks have gained high visibility in recent years. SCADA/IoT devices in (strategic) industries are now perceived as highly vulnerable.
On the other hand, using Gen (AI) in various security use cases, for threat analysis, Pen-testing, and expert training gives the defence side some urgently needed support. Zero trust architecture is gaining a foothold in many defence organisations and Armed Forces, permanent awareness training helps to sensitise the workforce. In addition, classifying data and information in a smart way and using quantum-safe encryption technology helps the defender. Trans-national interchangeability of classified data needs procedural and technical improvement.

The peer-to-peer competition with China in particular re-surfaces another topic which has vast security and economic consequences: Supply Chain Security, both for hard- and software components. Commercial electronic parts are widely used in military and governmental services, and not a few were originally manufactured in the People's Republic of China. To protect unimpeded functioning and also the resilient flow of supply, Western allies are resourcing more and more costly certification schemes for OEMs and their subcontractors.

Digitalisation with an inherent, built-in cyber security architecture and resilience against the increasing numbers of attacks with relevance to the Security Forces of a Nation is at the core of this session. All the technological, human resources and organisational aspects mentioned above are the subjects of this session. International organisations and governmental agencies will display their newest policy documents, and in exchange industry will showcase their approach and solutions in a wide range of applications. The most important outcome of this session, however, is the solidified understanding that only deeper cooperation between governmental bodies, the military and the private sector will foster cyber defense and societal resilience.

Keynotes

Panel 3: "Cyber Defense from a military standpoint; Experts on Threat and the Art of the possible"

Considering the content of the preceding keynotes, the panel may want to draw a conclusion how successful Cyber Defense in defense has been in the past years and how the auspices are, given the ever-increasing intensity of sophisticated cyber attacks. It will debate the level of cooperation both among nations and with

other shareholders in cyber security. In the light of the deepened digitalisation what new challenges are about to arise in cyber security?

Expected outcome: Understanding for an even more increased readiness and resilience against newest threats; paving the way for a more pro-active cyber defence posture. Identifying new challenges and potential solutions.

Keynote: "Securing the Hardware Supply Chain"

Considering the content of the preceding keynotes, the panel will discuss new technological, architectural, and procedural approaches towards increased cyber security. The specific challenges to introducing zero trust in a joint and combined operational environment may be addressed. Also the practicability and administrative impact of national or standardized certifications for soft- and hardware security needs to be debated in the light of sovereignty questions and how a complex supply chain over the life cycle of a product can be managed securely.

Expected outcome: Understanding the importance of a secure supply chain in the age of global dependencies. Discuss experiences with classical approaches towards security and practical steps to improve it.

SESSION 4: "Next-generation communication networks (beyond 5G) and their effects on defence"

The current implementation of 5G technology and the auspices to move on to new standards, which are data transfer rates 50 times higher with latencies that are 10 times lower in the decade starting with 2030, have created high expectations. Some already developing technologies, like smart textiles, digital twins, real autonomous driving, and augmented reality may actually need this communication capacity and technology to be implemented in order to become a complete reality. AI applications will get another boost. It might be the prerequisite for an integrated network from space to the sea seabed. The level of safety and security as a general governmental responsibility will increase. The use for communication with avatars in the metaverse and the support for Big Data, IoT, and deep learning applications is obvious.

We will learn about this new technology, its implications, opportunities, and challenges, and discuss preparation for its applications, both cultural and technological. The changing technology ecosystem around these new communication standards may be also of interest. Miniaturisation, high data exchange rates, and new types of microchips will affect industry and military systems. Situational awareness and communication underwater, above ground and in space can be revolutionised.

Above all, the questions of enhanced security in such a new global network must be addressed with high priority. Vulnerability, misuse, and failures should be minimised during the design phase. With data volume and complexity, the risk of cyber-attacks increases-- including the ever-dominant challenge of how to secure connectivity. Therefore, encrypted post-quantum communication and robust security protocols

are subject to be discussed as well… Those who will advance the most in research and fielding these technologies will be the ones who set the standards.

Keynotes: **Lessons from 5G implementation in military installations**

Panel 4: **"Potential military applications and use cases for 6G and beyond; including security in communications aspects"**

Farewell