TECHNET INTERNATIONAL
6 - 7 June 2024
Brussels, Belgium

Support Operational Readiness and be Disruptive: New Imperatives for C5ISR Technologies in NATO and the EU

Programme Overview

While the long-term technological superiority in support of deterrence was at the top of the agenda for NATO and the EU for quite some time, operational readiness, improvement of warfighting capabilities, and short-term availability of technology in the C5ISR field gained significant importance in the wake of the current political and military situation in Europe. Tensions are high, war is around the corner.

Trying to keep up with the dynamic development in IT and Cyber technologies in the private sector and sustainable support via solid and secure supply chains add to the challenges of today.

Actual wars with high relevance for Europe, like the Ukraine war and the Gaza conflict, offer deep insights into the new elements of warfighting, and its rapidly changing requirements. Unconventional solutions and methods for implementing information technology in the broadest sense for defense may become the new standard.

There is a growing appetite for the immediate availability of sensors, data, and effectors, thus affecting architecture, computing systems, algorithms, software, and many more C5ISR elements. The inclusion of combat systems platforms widens the scope into an inter-connected C6ISR "world", the growing role of software is mirrored by the concept of Software Defined Defense.

The highly skilled community of defence IT experts in Brussels working in NATO and the EU institutions, national representatives, industry and academia may be aware of the current situation, relevant to their daily work. The exchange between them, however, on new developments, requirements, projects and possibilities in C5ISR, as a whole, would be most beneficial to these parties, in order to exchange views on the big picture beyond their institutional boundaries and would be supported by a networking conference and exhibition such as TechNet International. New faces may be welcomed, and upcoming business opportunities may be explored during the two days of the conference. Mutual understanding of chances, risks and challenges can be fostered.

Information about strategic initiatives, plans, and policies by NATO and EU officials will be complemented by updates on running projects such as DIANA and HEDI.

In order to encourage discussions and have exchanges on new developments, IT applications and technologies, the following topics will be discussed during sessions at TechNet International 2024. They should offer a broad basis for presentations, discussions, and ethical exchange in an exemplary way. While advancing with the programme, new elements may be integrated.

Sessions:

I. Tightened Situational Awareness Needs in Defence: A Tough Job for Today's C5ISR Technologies?

NATO's new strategy with its "zero-day-readiness" requirement puts an additional strain on providing a crystal-clear situational picture for leaders on all decision levels--strategical, operational, tactical, while under the current foggy conditions caused by a multitude of information and data from a myriad of sources. The emphasis NATO (and the EU) puts now on readiness in principle also provokes the expectations on enhanced predictability.

There are sensors in all domains, in many pieces of technology, which just begin to contribute to that stream of data, e.g. from operational technology (OT). Such drivers, sometimes multinational data harvesting, transport, integration, analysis, management are a few of many steps needed in order to achieve information and knowledge advantage through a true MDO C2, which challenge modern technology. In addition, AI-based or assisted analysis, processing mass data at the edge, and other operational needs require the acquisition and employment of fresh technology, both available and ready to deploy, or emerging from the fertile soil of the disruptive new technologies, such as quantum sensing.

At the core of this session are the needs and requirements for real-time situational awareness, and the solutions the C5ISR community can provide today and tomorrow.

Keywords:

Sensors and data, OT data, computing at the edge, AI based analytics, ML, LLM, Gen AI, edge management of data, C-JADC2, emerging and disruptive technology in sensing, surveillance and information sharing, anomaly detection, predictive maintenance.

II. Defence Clouds: Imminent Challenges and Solutions for NATO and the EU

NATO is developing its cloud strategy and urgently searching for solutions for a multi-security level cloud solution; EDA studied the benefits of a combat cloud for hybrid warfare. The parameters scalability, sustainability, and security are driving the specific needs for cloud solutions for military options, also on the tactical level. Software as a Service, Simulation, and other cloud-based technologies available in the private sector are of interest to military users. The very latest cloud solutions should be discussed in this session as

to how far they match the increasing demand on the military side, both on the strategical and the tactical level.

Keywords:
Cloud-strategy; NECOM; NR cloud security; resilience; multi-security level cloud; hybrid-cloud; connectivity; computing power, energy-efficiency; cloud security; information sharing;

III. Interoperability via Software Defined Defence and "Digital backbone": Making Principles Work in Practice

Not only since Multidomain Operations became the new conceptual driver, interoperability of national assets and capabilities have been at the core of NATO and the EU's efforts, especially in the field of information and communication. FMN stands for a successful endeavour to "integrate without dominate" IT solutions and, of course, to standardise. In parallel, the digitalisation process of the Armed Forces advances in Nations, NATO and the EU. With new technological options available today, this now reaches a new level: The desire for and infrastructural layout of the "digital backbone" of NATO as the basis for modern, secure communications throughout the digitally diverse Alliance has been discussed many times. The EU looks for coordinated solutions amongst member states in various aspects of information technology. The technological development of total virtualisation and almost completely "software defined" solutions meanwhile lead to the architectural concept of Software Defined Defence (SDD) which includes legacy systems and combat platforms in a C6ISR ecosystem. This session will deal with practical aspects and means through which e.g. industry can provide in order to support the ongoing transformational process and the fielding of modern components as components of NATO's digital endeavour.

Keywords:
SDD architecture; decoupling hard- and software; integration of legacy systems; NATO digital backbone; NATO Digital Transformation Implementation Strategy; IT infrastructure; SaaS; business process automation; NextGen communication; C2Fix/C2Next

IV. Cyber Defence: New Tools Have Arrived (Zero Trust, AI, Collaborative Elements)

The level of cyber threats by both criminals and state actors is constantly on the rise. Evermore sophisticated intrusions into defence IT systems, communication networks, and supply chains happen with an ever increasing frequency. AI augmented attacks as part of the war in the information space continuously evolve. On the cyber *defence* side, new technological tools are becoming available-- intensified research and implementation of best practice solutions provided by industry is helping government to catch up with the attackers' capabilities. Multinational cooperation and collaboration between government and industry take root in nations, NATO and the EU.

This session will focus on cyber defence technologies and organisational means, ready to be implemented, as well as new architectural designs with built-in security features where industry can help and contribute. New, emerging technologies should also be considered in order to foster future defence capabilities.

Keywords:
Cybersecurity standardisation and certification; situational awareness; AI in cyber; zero trust architecture and technologies; collaborative solutions; CIDCC; hybrid warfare; prevention, detection, attribution; cyber forensic; post-attack recovery.

List of technologies to be explored:

- 5G/6G
- Artificial Intelligence
- Cloud Computing
- Cloud Services
- Cyber Operations
- Cyber Security
- Data Analytics
- Data technologies
- Edge Computing
- Emerging Technologies
- Hybrid Cloud
- IT Modernisation
- Machine Learning
- Mobile CIS solutions
- Multi Domain Operations
- Zero Trust