Revised 9 March 2021

Challenging Times for National Security –
Technologies for Better Cyber Defence and Battlefield Resilience

Event organised by AFCEA Europe in cooperation with the AFCEA Portugal Chapter
and
held under the patronage of the Minister of Defence, Portugal.

Session Overview

Pre-Session keynotes

The important introductory keynotes prepare the groundwork not only for the following discussions during TechNet Europe, but will also turn the spotlight onto the foreseeable future of security and defence in Europe, interlinked with the trans-Atlantic community. Some of the common elements in all the chaotic and unprecedented times in which we are currently living are that cyber security of a nation is challenged at a higher frequency, and the push for digitalisation in society and government, also the military, has gained momentum.

Session 1: *A Nation's Cyber Defence – Never Successful Alone*

A nation's cohesion and resilience with regard to defending its values and resources in a holistic Governmental approach is more at stake than ever. Even prior to the pandemic, there were growing challenges. The newest initiatives for improved cyber defence capabilities together with revised strategies and new organisational approaches should contribute significantly to a better stand against today's attacks from state and non-state actors. Intensified cooperation beyond stovepipes, at national level as well as between nations, is key. Presenting and discussing the various aspects of the right mix of technological and non-technological means necessary and available for the defender is at the core of this session.

Subjects (amongst others) to be covered during the keynotes and panels:

- New hybrid threats (in particular, the increased role of fake information)
- Recent increase in sophisticated cyber attacks during the pandemic
- Artificial intelligence working in favor of the attacker
- Priority shift in technology and budgets (nationally, internationally) post-COVID

- Impact of disruptive technologies like Quantum-safe encryption, Artificial Intelligence, Blockchain
- New European cyber security strategy,
- How to push agility with new organisations, like the PESCO project of the Cyber Innovation and Knowledge hub (Portuguese initiative)
- Renewed international cooperation in Cyber defence, also between NATO and EU.
- A new transatlantic technology partnership?

Session 2: *Digital Resilience on the Battlefield – It Is a Must!*

Digitalisation of the Armed Forces clearly is an undisputed necessity, it proceeds with high speed in all domains, at least conceptually. Part of this inevitable process is the progressing digitisation of equipment on the battlefield. Beyond equipping forces with software-defined radios and introducing new battle management systems, however, digitalisation goes as far as using artificial intelligence in support of situational awareness and decision making. It all requires new, much more capable, and secure communication systems and technologies such as 5G and combat cloud. At the same time robustness and resilience are of increasing importance and should be an indispensable, mandatory ingredient of any technology employed at the tactical edge. Will digitalisation enhance resilience? Given the pace of digitalisation in industry, what are the obstacles for fielding new technologies more swiftly in the military?

Subjects (amongst others) to be covered during the keynotes and panels:

- Military communication standards (5G) as a driver for interoperability
- Mobile CIS solutions
- Edge computing and combat cloud
- A Chief Digital officers' experience
- The new NATO OpNet approach for efficient digitalisation
- Data analytics on the battlefield and at Headquarters level
- Multi-domain operations and its requirements on the way from concept to reality
- The JADC2 concept