TechNet International 2026

20 JULY 2026

Andrea Guidotti and Valerio Borgo

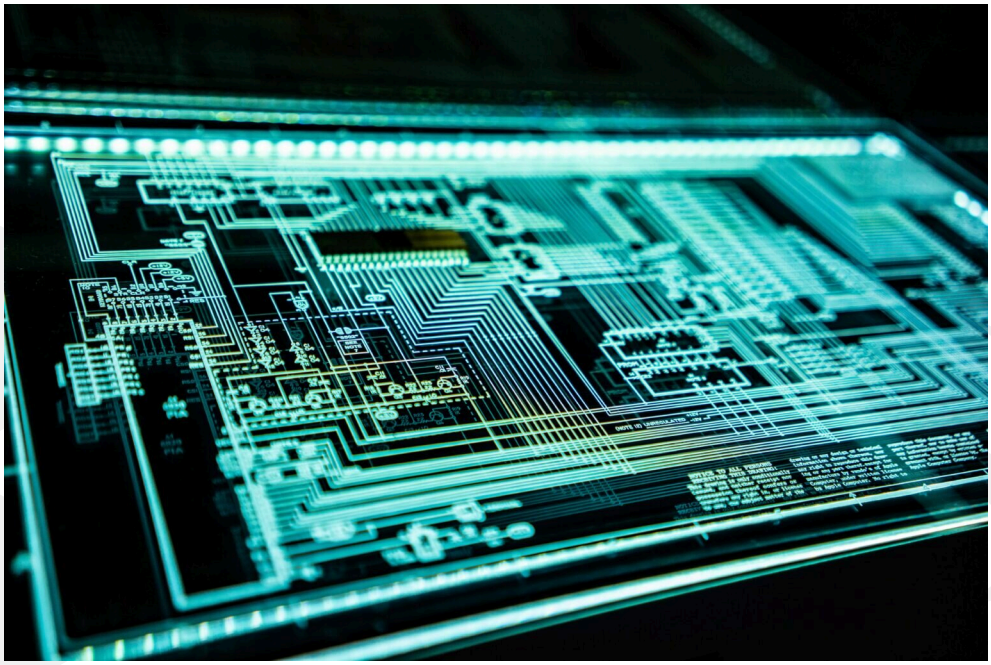


Photo by Adi Goldstein on Unsplash

Introduction

The 2026 edition of AFCEA's TechNet International in Brussels confirmed the importance of data-centricity and security. Across high-level sessions, gathering together representatives from the North Atlantic Treaty Organization (NATO), the European Defence Agency (EDA), industrial leaders, and research centres, the event set the tone for a new shared agenda: data requires protection throughout its entire lifecycle, and human judgment should be guided rather than displaced by the application of AI-powered solutions in multi-domain operations. Strategic advantage depends on the ability to innovate and adapt faster than adversaries. The seamless integration of new doctrines, command structures, and operational capacities with frontier technologies must be the main concern.

Massimo Esposito, AFCEA Europe International's general manager, highlighted the importance of connecting the defence industry with the military and academia. He emphasized the increasing pace of technolog-

ical change and suggested that everyone in the industry should embrace innovation as a mindset. For industry, interoperability is a must, while for academia, a longer-term perspective on innovation is the key. The key question is less about which technologies to acquire and more concerned with how quickly its institutions can absorb them.

From perimeter to data: the data-centric security turn

One of the central themes of TechNet International is the need to migrate from network-centric to data-centric security (DCS). In his keynote speech opening the DCS Deep Dive on day three, NATO HQ's Gernot Friedrich — Head of Interoperability and Standardization — introduced a refined data maturity ladder: basic labelling (DCS-1), enhanced labelling with attribute-based access control (DCS-2), and full cryptographic protection in which the data itself is encrypted (DCS-3); with each layer mapping to concrete NATO standards. The guiding principle was summarised with the slogan "control, protect, share". Security needs to be seen as a property travelling with the data rather than an encompassing feature of the network itself. As Airbus Defence and Space Cyber's Strategy & Portfolio Manager, Paul-Emmanuel Brun, put it, the conceptual shift needs to be from the idea of defending the places information navigates throughout to defending the information itself. The focus should be on four key components: data protection, data access control, data loss prevention, and process governance.

The zero-trust logic behind this framework connected many interventions. The guiding principle: applying classification techniques and encryption as close to the data source as possible. Stormshield's Head of Business Development, Jocelyn Kryslik, presented an encryption platform based on peer-to-peer architectures and designed to withstand post-quantum technological threats. Kai Rehnelt, CEO of SECLOUS, explained how to leverage non-visible data (NVD) technologies and protect information at every step of the transmission chain, making it unreadable without the authorised applications. The same NATO interoperability standards were highlighted by Paolo Pezzola, Principal Account Manager at INFODAS. Deep content inspections, including validation schemes, semantic filtering, and metadata sanitization, can enhance security and enable cross-domain solutions that allow the movement of OSINT (Open-Source Intelligence) data into classified environments across NATO members. These insights recall a collective invitation: to build products for the ecosystem, not for the individual enterprises.

Artificial intelligence and decision-making in multi-domain operations

A second strand examined how AI is reshaping multi-domain operations and the way commanders can retain decisional control. Colonel Arnel's David exemplified this approach with the presentation of NATO's MAVEN

programme, a smart system based on an N-MSS Ontology that leverages generative AI to work on different sorts of data – from land to sea, space, and special operations. Such a solution allows a common operational, intelligence, and logistic framework, enabling the integration of several private LLMs and open-source solutions within NATO's ontology, which in parallel provides the context, instructions, and rules to be aligned with. What is the recipe for institutional success? Build small, talented teams, where action takes over unanimous consensus, and everyone refuses to take "no" for an answer when facing external constraints.

Cristina Caballé from IBM offered an operational demonstration. While kinetic effects are predictable and measurable, non-kinetic effects are harder to track, thus creating a "reliability gap". AI can help bridge this gap and integrate the latter into modern warfare operations, replacing guesswork with mathematical data provenance and predictive modelling. A demo replicating a real-world scenario grounded in the Strait of Hormuz demonstrated the utility of IBM's multi-domain operation tool, which provides an LLM-agnostic, agentic platform based on a decentralised, neural-like network collecting the data and feeding real-time information to AI agents to be elaborated and provided to inform commanders' decisions on the battlefield. The future of deterrence belongs to the militaries that can effectively orchestrate all the domains. Cognitive overload is becoming a strategic advantage: everyone should be able to thrive in chaos.

Hybrid threats and the contest for the grey zone

A third topic of discussion focused on strategy. David Song-Pehamberger from the European Centre of Excellence for Countering Hybrid Threats offered an explanatory framework on hybrid threats and campaigns. For interested readers, we discussed the issue in a separate interview we conducted with him alongside the conference. Within the cyber domain, speed is not the only binding constraint. There is a strong need to concentrate on the visibility of threats. A demo offered by CONET clearly demonstrated this through a Red Sea simulated scenario, where civilian commercial vessels are targeted by drones while "phantom" radar contacts interfere with the electromagnetic field to disrupt the available defence systems. In such a situation, military operators cannot visualize what they are confronted with. The solution lies in connecting otherwise isolated data spaces into a shared picture that is organized by the relevance and risk of threats.

From an operational standpoint, the approach must move from a reactive to an anticipatory one. Dmytro Plieshakov from Osavul, a company active on the battlefield in Ukraine, offered a usable formula, accounting for opportunity, intent, and capability. He clarified that every important factor leaves observable signals behind, thus allowing analysts to simulate scenarios and quantify risk before an attack rather than after it. As Alan Hill, Director EMEA Defence & National Security at Splunk, distinctly

diagnosed, misalignments can produce delays when organisations arranged by domain build on a mismatch with effect-led hybrid campaigns. To avoid downfalls, systems correlating data and strategic options need to be designed.

Sovereignty, speed, and the politics of technology adoption

The final thread revolved around sovereignty. Enrique Oti, Chief Strategy Officer of Second Front Systems (2F), clarified why sovereignty and interoperability shouldn't be pitted against one another. In his opinion, sovereignty is about proper access to data and virtual spaces. Change requires three conditions: sovereignty defined by operational outcomes; zero trust logic delivery; automated deployments, reciprocal compliance, and scalable and portable capabilities. Angel Smith, President of the Global Public Sector at Virtru, built on this by stating that data sovereignty is technical, rather than territorial. Authority and autonomy are respected when data are highly encrypted, and the access keys are controlled by the owner, no matter the data location. Retaining national sovereignty means implementing data-centric interoperable networks, where everyone with the proper rights has proprietary access to the data.

Institutional arguments echoed industrial actors. Anders Sjöborg, Deputy Chief Executive of the European Defence Agency, discussed the current developments of the EU-Defence Cooperation Planning and the organization's mandate to support the EU Readiness 2030 Agenda, tracking low investment areas and current dependencies. Yelyzaveta Boiko, Program Manager from the Center of Innovations and Defence Technology Development at the Ministry of Defence of Ukraine, guided the audience into the advancement and deployment of DELTA, Ukraine's battle-tested digital combat ecosystem. On the transatlantic side, the Head for Innovation and Technology Adoption, Claudio Palestini, presented NATO's Rapid Adoption Action Plan. The program aims at compressing the adoption window of new technologies to a maximum of 24 months, while sharing objectives and best practices internally.

Key takeaways

One point was central at the conference: the future of defence lies in the protection, movement, and exploitation of data, rather than hardware solutions. Actors should prioritise ecosystemic thinking, moving away from the defence or proprietary silos, and focusing on the development of common standards. While generative AI is increasingly important in operational terms, human judgment should stay at the centre of decision-making and act as a design constraint.

In the European context, some implications stand out. First, sovereignty is complementary to interoperability when defined as control over data rather than by physical territory. Second, resilience and rapid iteration

can outperform perfectly planned systems. Third, institutional speed is a binding constraint: Europe must adopt, integrate, and trust advanced technology rapidly. Those who will incorporate and deploy the available tools at the pace required by contemporary threats will have a strategic advantage.