VAUBAN SESSION 2019

Summary of discussions

Nothing new under the military sun (not true)

Cyberspace is not a new military domain. While weapon systems and armed forces are increasingly digitalised, tactical challenges remain unchanged: commanders still have to manoeuvre and command troops on the battlefield. Digitalisation of the Armed Forces, illustrated among others by the French SCORPION modernisation programme, is however profoundly changing the way military corps operate, and creates a new realm of confrontation.

Armed Forces no longer drive the change in the digital era, and often struggle to master the cyber domain. More than 10 years after the cyber-attacks against Estonia and NATO's recognition of cyberspace as a domain of operations, military doctrine, tactics and training often lag behind fast-evolving technology. Capacity-building and cooperation are slow in this domain, with cyber described during the Vauban Sessions as the 'new intelligence', with everybody urging sharing but few actually doing so.

At the root of many technological breakthroughs, Armed Forces have in the last decades integrated information and communication technologies into their modes of action, equipment and weapons. Digitalisation extends to the entire military realm and impacts both Armed Forces' organisation and missions. On the battlefield, digitalisation further reinforces the crucial role of information, and the importance of cybersecurity and supremacy in ensuring military superiority. Cyber is an integral part of modern warfare which must be properly understood and leveraged at the strategic and tactical levels.

NATO Nations' Armed Forces share similar concerns and challenges in the cyber domain: they are under-staffed, under-funded and struggle to attract and retain skilled experts, with human resources pinpointed as a critical success factor throughout the day. There is clear political will to keep cyber high up on NATO's agenda to tackle these issues together. Despite the geographical fragmentation of initiatives, a coherence of action should allow Allies to make cyber expertise and capabilities available and actionable on short notice. The end goal for commanders is to use cyber tools to achieve effects on the battlefield. It must now be extended to all forces, as well as to the planning and deployment processes.

Trying to avoid overcomplicating an issue which often suffers from technological and technical complexity, discussions looked at how Armed Forces can build strategic coherence in the cyber domain as they did in the air and space domains. The integration of the cyber dimension could be made easier and quicker for tactical commanders by:

- Understanding the interpenetration of military command and cyber, bringing domains such as intelligence, communication and information control ever closer;

- Operating in cyberspace - i.e. securing access, protecting digital assets and producing effects in cyberspace;
- Organising and planning military capabilities accordingly.

Electronic warfare (EW) provides an interesting model for how Armed Forces should tackle cyber. While the scope of the cyberspace is wider than that of EW, one speaker argued that the mission of structuring and bringing coherence to the cyber domain should lie in the hands of the signal corps as they give access to the cyberspace, which is a prerequisite to any cyber operation. The concrete implementation of cyber operations will then be declined according to the needs of the different services and units of the forces: (cyber) intelligence, (cyber) operations etc. All in all, the cyber dimension must be incorporated in the military education and training frame.

Efficient cyber training is particularly important now that countries like Russia have significantly upgraded and improved their cyber capabilities, drawing lessons from their recent and ongoing operations. In Eastern Ukraine, for instance, Russian-backed forces used sophisticated jamming and interception tactics to interfere with communications and surveillance drones.

Armed Forces need a proactive and effects-based approach to cyber space

NATO Nations' Armed Forces share similar concerns about cyber weapons and therefore approached the cyber domain mostly defensively. Armed Forces are highly vulnerable to cyber threats because of their reliance on external providers and contractors, for instance with military logistics increasingly dependent on the Internet and thus Internet Service Providers. The importance of capacity redundancy was stressed, to avoid disruption of communication, as was Armed Forces' continued efforts to learn to work in degraded mode and in an environment constrained by military networks' bandwidth capacity along with other security requirements.

Cyberwarfare is however not only about building firewalls to defend military systems and assets. Armed Force now need to come up with a more offensive and effects-based approach to cyber capabilities. Forces must be able to understand and anticipate adversaries' behaviour and intent. Sniffing attacks were mentioned as an example of pro-active use of cyber capabilities during the session on exchanges of best practices.

France's recent decision - announced by the French Ministry of Armed Forces just a few days before the 2019 Vauban Sessions - illustrates the current shift from a strictly defensive cyber posture to offensive activities in cyberspace involving direct engagement with adversaries. With this new offensive cyberwarfare doctrine, France now considers cyber weapons as a fully-fledged operational asset and an adequate response to fight against increasingly digitalised systems. The new French doctrine is more than a mere guide to action for soldiers in cyberspace. It is a comprehensive policy on France's global perspective and ambition in cyberwarfare, and one of its pillars is Education and Training.

From words to action: Education & Training to capture and structure the cyber potential

At the strategic level, it is key to achieve a common understanding of cyberwarfare and digitalisation of the Armed Forces, hence the Vauban Sessions initiative. There is for now no common definition of a cyber command, nor of offensive or defensive cyber weapons. The visions, missions, mandates, functions, and capabilities of cyber forces across NATO Allies vary greatly, while all panellists, regardless of their country of origin, agreed that they face similar challenges and threats. A first step for NATO was to have a common perspective of the issue, which let the Alliance to implement a common maturity level model in 2017 with a range of metrics to assess progresses made by the Nations in cyber defence. This includes improving NATO planning processes to ensure that cyber is integrated and build up across the Alliance.

Actors such the Allied Rapid Reaction Corps (ARRC) and EUROCORPS shared lessons from recently conducted exercises, including the need to address the knowledge gap about cyber offensive capabilities at strategic level. Confronted with a relatively new issue, staff members must be trained to give commanders options for action on the battlefield. This also calls for the creation of cyber cells within military staff supporting the intelligence (J2), Operations (J3) and, of course, Communication (J6) functions.

Training and exercises such as Trident Juncture 18, Locked Shields 2018 and Citadel Bonus 2018 (CIBS 18) are a privileged way to test, learn and improve. They also provide a good opportunity to incorporate the cyber dimension into traditional military training schemes. CIBS 18 was held in late 2018 Poland and France (Marseille) simultaneously and brought together some 850 soldiers from 17 nations in a command-post exercise. The 2018 edition assessed the cyber capabilities of the Rapid Reaction Corps - France (RRC-Fr), host of the 2019 Vauban Sessions. CIBS 2018 aimed to develop the CRR-Fr staff's cyber capabilities in a complex attack scenario and the set-up of a specific cell to coordinate all the tasks in the cyber domain, from the defensive to the production of effects. The next step will be to develop a virtual network able to simulate social media and military communication and information systems to further study the conduct of cyber operations and assess their effects. It is also to integrate red teams in exercise animation.

A key challenge for the Armed Forces is to define rules of engagement in cyberspace, including the circumstances, conditions, degree, and manner in which to use cyber weapons and conduct cyber actions. The lack of rules of engagement - and the risk of new vulnerabilities and threats - should not however prevent Armed Forces from investing and practicing more in the cyber domain. With cyber, Armed Forces are entering new era, which may profoundly change the way warfare is conduced, as aviation did a century ago.

While Armed Forces are likely to stay on the back foot in the digital realm, a first step to adapting to this new paradigm, should be to practice and identify needs and opportunities before defining the right processes and staff structures to systematise and extend these opportunities and to prevent potential risks.

Train, test & share

In the digital era, interoperability is key and has a double purpose: at the operational level, to ensure the effectiveness of Armed Forces fighting together on the battlefield; at a technical level, to ensure digitalised systems and tools operated by different Forces can work together. Representatives from several NATO Nations recalled the importance of sharing information and planned developments in the cyber domain with their NATO counterparts.

Interoperability is at the heart of NATO, whose Federated Mission Networking (FMN) concept aims to enable improved Command & Control, decision-making and information-sharing by connecting forces in a coalition environment. But while FMN has been the object of discussion for years, a lack of interoperability at the tactical level persists, in particular for Land forces. Practically, FMN is translated into a number of different initiatives, raising the risk of fragmentation of efforts and resources.

Joint training provides one answer to the challenge of interoperability. Interoperability must however start with procurement and the expression of common requirements to ensure the purchase of interoperable equipment. The search for greater interoperability soon raises the industrial challenge: Allies must ensure the industry complies to standards. This in turn has severe operational consequences, as highlighted by the recent sinking of a Norwegian Navy vessel, where initial findings showed that the Spanish-built ship did not conform to the required damage stability standards.

In the digital domain, the NATO Communication and Information Agency (NCIA) supports both individual and collective military training by providing a comprehensive training course catalogue covering the entire spectrum of CIS and Cyber Security. NCIA is in the midst of a 3 billion EUR tech refresh which will lead to a massive demand in staff training. The NCIA is soon to inaugurate a C4ISR training academy in Portugal, and recently launched a fully functioning NATO cyber range in Estonia to meet this increasing training demand. Their experience shows that a major challenge is to deliver proper training in an increasingly technologically complex world while understanding that cyberspace is much broader than a simply technical issue.

In this context, staff members and soldiers should train with cyber teams directly. By training IT experts and non-experts together, commanders will increase their understanding of cyber capabilities and how they can contribute to their troops' operational superiority. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) provides a multinational cyber defence hub for cyberdefence training for all hierarchical levels. In 2018, Locked Shield - an annual exercise, organised by CCDCOE since 2010 -

brought together 24 Blue Teams responding to cyber-attacks against a major civilian internet service provider and a military airbase.

Solution demonstrations

The Vauban Sessions' dynamic technological solutions session showcased some innovative, easy-to-deploy and sometimes inexpensive technologies to support the training of Armed forces. The objective was to demonstrate what industry can provide to support training in a digital environment by leveraging innovative technologies. This session also showed the role of industry - together with the military - in addressing the challenge of the new generation of fighters who want to "train as they play". As training evolves into continuous learning, technology offers different and ever more realistic ways to train.

Manzalab presented a proof-of-concept developed for the French Army. Using Mixed Reality, the solution allows high-level staff members in different locations to join a virtual war room and attend a simulated rescue mission briefing. The system uses low bandwidth, making it suitable for military encrypted networks and for use in the field. Relying on similar visualisation technology, Virdys 3D virtual content creator allows to quickly create realistic and immersive training environments. This solution is already found in a number of military training applications such as support to briefing & debriefing, acquisition of field gestures and procedures and assembly & dismantling operations. Agueris (CMI Defence) presented some of its military simulation solutions for weapons systems and vehicles, illustrating the extent to which technology enables to "train as you fight" with simulators embedded in and connected to real equipment. In trying to capture the future of the digitalised battlefield, Thales shared its vision of how the digital may impact the information and operational environment of the fighter in a 5 to 10-year horizon by creating an ever-closer link between training, planning and conduct of operations.

The 2019 Vauban Sessions were hosted on January 24th by the French Rapid Reaction Corps (CRR-Fr) in partnership with CEIS. More information at www.vauban-sessions.org or contact Pauline Massart, CEIS EU Office: pmassart@ceis.eu.

With the support of

CMI DEFENCE THALES AIRBUS