ISSUE ALERT
24
2017

MOPIC/ADOBESTOCK

The cybridisation of EU defence

by Daniel Fiott

While the issue of cyber*security* is pervasive, cyber *defence* is not. Not only are documents such as the EU Global Strategy replete with references to the challenges emanating from cyber, but EU member states and institutions are taking important steps (such as greater investment in cyber capabilities and the establishment of dedicated national authorities) to ensure Europe's cybersecurity. Yet less attention has been paid to the specific *defence* dimensions of the EU's cybersecurity efforts. Although this is perhaps to be expected, cyber defence cannot be overlooked, not least because it has treaty implications related to EU solidarity (Article 222 TFEU) and mutual defence (Article 42.7 TEU) in case of an attack aimed at EU member states.

Cyber defence is an important part of protecting European forces during EU-led operations under the Common Security and Defence Policy (CSDP). Cyber-attacks against militaries during operations may compromise command, control, communications and computer (C4) channels (i.e. hacking of space infrastructure), disclose or mimic troop movements and tactical intentions (i.e. create at-sea collisions), sabotage and/or take control of capabilities and logistics (i.e. drones and power outages), etc. These threats are particularly important in an era of 'network centric warfare', where emphasis is placed on connecting military units during operations with sophisticated C4 technologies.

Given that cyber is referred to as the 'fifth domain' of warfare alongside air, sea, land and space, it is worth analysing how the EU is integrating cyber into its broader operational and doctrinal approach to crisis management. This is a particularly salient question given the recent table-top exercise on cyber defence, the revision of the EU Cyber Security Strategy and the 2018 Capability Development Plan (CDP). Yet, more than just simply looking at the operational and doctrinal aspects of EU cyber defence strategies, it is also an opportune moment to reflect on the technological and industrial aspects of cyber defence; especially in the context of the ongoing development of the European Defence Fund (EDIF).

A 'firewall' for defence

So far, much of the EU's response to cyber defence relates to training and exercises. This matters, not least because cyber quite clearly represents a different strategic or operational category to the conventional services of the military. Not only are the capabilities and technologies needed to defend against cyber-attacks different to the planes, ships and tanks used by armies, navies and airforces, but cyber defence is integrated into each of the traditional services in a way that may make it difficult to place it into its own doctrinal and operational silo. While recognising that traditional services increasingly operate in a 'joint' fashion, one cannot identify a 'cyberwar' in the manner that it is possible to do so for air, sea or land battles. Training and exercises therefore allow the EU to develop its cyber defence doctrine and to ensure effective response.

Following the adoption of the 2014 EU 'Cyber Defence Policy Framework', it was recognised that cyber defence training and exercises should be intensified. To this end, the European External Action Service (EEAS) has integrated cyber defence into its regular crisis management exercises (e.g. MILEX 2015 and MULTILAYER 2016). Additionally, the European Defence Agency (EDA)-led 'Cyber Situation Awareness Package' [CySAP] (or the 'how to' guide on cyber defence) has already been used to train staff on CSDP missions. More recently, on 7 September 2017, the EU held its first ever 'table-top' cyber defence exercise [EU CYBRID 2017] for defence ministers – they were presented with a fictitious scenario of a cyber-attack on EU-led maritime operations' headquarters and assets. Finally, from 1 September to 11 October 2017, the EU is holding a parallel exercise (PACE 17) with NATO to test each organisation's crisis management response in a hybrid threats environment.

An added benefit of the EU's cyber defence exercises and training is to ensure institutional coherence. In this vein, because cyber defence is dual-use in nature – not just technologically but also in terms of civil-military interaction – great effort has been put into establishing a coherent chain of command and response system across the EU's institutional system. To this end, the European Commission and the High Representative/Vice-President have jointly published an EU Operational Protocol for Countering Hybrid Threats (the so-called 'EU Playbook'), which maps all relevant EU bodies (civil and military) responsible for countering hybrid threats. Even some EU member states have taken important steps to harmonise approaches to cyber defence. Eleven countries have initiated a 'pooling and sharing' agreement under the auspices of the EDA for the common usage of 'cyber defence ranges'.

Encrypting EU cyber defence

A focus on training and exercises is, of course, to be commended but these operational elements of cyber defence raise questions about cyber capabilities and industry. Although the EU Directive on Network and Information Security (NIS) seeks to improve national cyber preparedness, and notwithstanding the fact that many EU member states are investing in cyber Research and Technology (R&T) and cyber capabilities, there is more scope to harmonise cyber defence capacities and R&T programmes. Even if the private sector is largely responsible for the development of cyber defence capabilities, ensuring that the European Defence Technological and Industrial Base (EDTIB) represents a secure and innovative cyber technology supply chain is of paramount importance if CSDP is to rely on effective cyber technologies now and in the future.

The recently published Joint Communication on EU cybersecurity [JOIN(2017) 450 final] explicitly recognises that the 'high level of resilience required in cyber defence calls for specific targeting of research and technology efforts'. Here, the EDIF could play a vital role. Accordingly, it is instructive to note that a share of the €25 million allocated in 2017 to the first call for proposals under the Preparatory Action on Defence Research (particularly those projects related to improving naval situational awareness and force protection) will have strong cyber defence elements. The European Commission has also made cyber defence a key element of its proposed regulation for a European Defence Industrial Development Programme (EDIDP) [COM(2017) 294/905208]. The EDIDP would be a preparatory phase for the capability investments made under the EDIF.

The EDIF could potentially lead to a much-needed breakthrough for interoperability in and harmonisation of cyber defence capabilities. Yet, as the EU Cyber Defence Policy Framework makes clear, because CSDP military operations rely on national contributions of equipment and C4 systems, it is vital that greater national convergence on cyber readiness and capabilities is ensured, too. Conceivably, in addition to the cyber defence shortfalls and vulnerabilities already identified as part of the 'Cyber Defence Research Agenda', the planned Coordinated Annual Review on Defence (CARD) may be an ideal platform to assess and share cyber defence planning and investments. The 2018 revision of the EU's CDP could also be a mechanism through which to ensure greater convergence in cyber defence.

Finally, there is also some recognition that if Permanent Structured Cooperation (PeSCo) is triggered before the end of 2017, cyber defence could play a role in any of the eventual PeSCo projects agreed to by the member states. There is, therefore, increasing political attention paid to cyber defence in the EU: in addition to exercises and training, the Union is now increasingly in a position to financially *invest* in cyber defence as well. This is welcome given the fact that, in cyber defence, one is only as strong as the weakest link.

Daniel Fiott is the Security and Defence Editor at the EUISS.

© EU Institute for Security Studies | QN-AL-17-024-2A-N | ISBN 978-92-9198-531-9 | ISSN 2315-1129 | doi:10.2815/058809