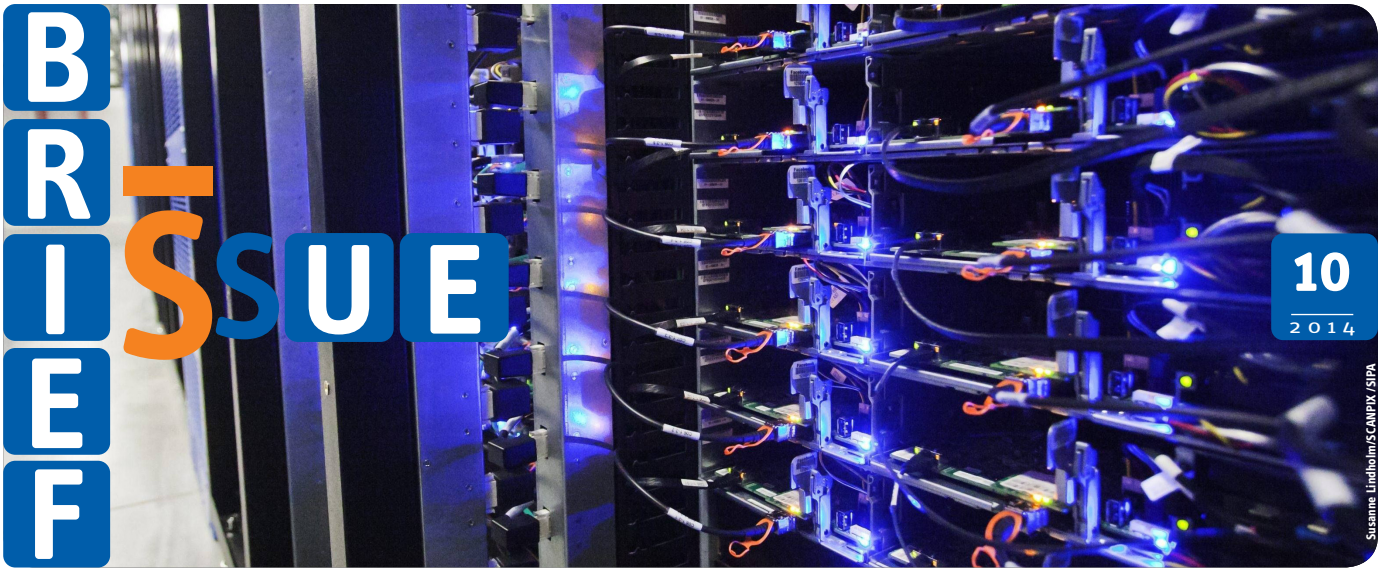

EU cyber-defence: a work in progress

by Neil Robinson

The EU's cyber defence agenda provides an opportunity to ask questions about what the EU could do in terms of setting security priorities. Furthermore, as a possible area for cooperation, cyber defence shares with military air logistics the peculiarity of being a common capability which does not require explicit war-like conditions to demonstrate its utility. Indeed, the diversity and complexity of the threat environment – coupled with challenges of attribution – suggests the opposite: military cyber defence capabilities might offer better value for money in peacetime rather than in times of war.

Becoming increasingly real

To a certain extent, EU action in this area may be seen as a response to a creeping realisation that there are important security implications of risks inherent to society's reliance upon cyberspace. The nature of these risks has been illustrated by familiar incidents such as the widespread penetration of multinational firms as part of the '*Gh0st RAT*' chain of attacks, or the disruption affecting the systems of Saudi Aramco in 2012.

Developing military cyber-defence capabilities is a relatively 'greenfield' area for the EU. The 2010 revisions to the Capability Development Plan (CDP) – endorsed in 2011 – reflected an agreement among the participating member states on the need to treat cyber defence as a top priority. Since then, the European External Action Service (and within it the EU Military Staff/EUMS), the European Defence Agency (EDA) and the European Commission have been working alongside other stakeholders – both within the EU and internationally – on a range of initiatives. The EDA and the EUMS, in particular, have been the main actors in driving these forward. Such initiatives have been to a large extent coordinated with the comprehensive EU Cyber Security Strategy (EUCSS), which celebrated its first anniversary in February 2014. The EUCSS made a major contribution to last December's European Council on defence as it grouped the various contributions of defence, criminal justice, resilience and foreign affairs to cyber security under a single, whole-of-government approach.

Key deliverables since the 2010 CDP have included a Concept for Cyber Defence for EU-led CSDP Operations and internal plans on what role the EDA should play in supporting the development of cyber-defence capabilities at member state level. In 2013, a snapshot of the landscape of national cyber-defence capabilities was published as the first public foray by the EDA into this 'greenfield'

domain. On a more practical level, various entities in the EU military community have been making progress in discussions on: piloting training and exercises; technical methods for information exchange between different players; and *de facto* as well as formal cooperation agreements with organisations like NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE). The EDA has also been playing its role in broader initiatives such as exercising observer status in experiments in implementing international doctrines.

It was no surprise, therefore, that cyber defence was one of two specific proposals agreed at the European Council meeting last December (the other concerned maritime security). At the meeting, HR/VP Catherine Ashton, in cooperation with the European Commission and the EDA, was tasked to prepare an EU Cyber Defence Policy Framework during 2014. This would seek to promote six areas:

- Improving member state capabilities, research and technologies through the development and implementation of a comprehensive roadmap;
- Reinforcing protection of Communications and Information Systems (CIS) in support of CSDP structures, missions and operations;
- Mainstreaming cyber security into EU crisis management;
- Improving training as well as education and exercise opportunities;
- Creating synergies with other relevant cyber-security actors in Europe;
- Reinforcing cooperation with relevant partners.

Developing national capabilities

There is a growing consensus that – although many member states have made great strides in developing their cyber-defence capabilities – there is much room for improvement. Efforts to support this are crucial, especially given the unique nature of capability development in a European context whereby military force generation and readiness are a national (rather than EU) area of competence. Many countries are still grappling with the conceptual and doctrinal underpinnings of the role of the military and armed forces in defending cyberspace. Aside from their responsibility to protect their own infrastructure, there are divergent views as to which is the right policy portfolio for traditional national security actors in the cyber age. The relationship between national cyber security strategies (which may outline the role of the armed forces) and cyber defence doctrines and strategies developed within the armed forces themselves is also somewhat unclear. Nonetheless, many militaries have created military Computer Emergency Response Teams (milCERTs) and a few – like the Dutch, the French and the British – are evaluating or implementing more organic cyber-defence organisations.

As for training, there is still much to be done: efforts currently appear to be either too general (aimed at promoting general cyber-security awareness amongst the average end user) or highly specific (individual and collective courses for personnel staffing milCERTs). The debate around issues of recruitment is also slowly intensifying, in particular with regard to ways of gaining access to this limited talent pool and maximising retention of military cyber defenders *vis-à-vis* (more profitable) civilian domains.

Regarding material and logistics, the role of the private sector in both supplying requisite equipment and supporting it through life has yet to be fully explored. The extent to which member states make use of the private sector varies, and can include extensive reliance upon privately owned and operated telecommunications (which might even include in-service support in a combat zone). In relation to facilities, too, many countries are looking into the idea of more formal tools to simulate the effects of attacks in a safe environment. For example, a number of well-known defence contractors now offer cyber test-ranges to test defensive capabilities. The role of the military in responding to crisis situations is also unclear – and highly dependent upon the specific arrangements in each country. Finally, as can be seen in other policy fields related to the use of technology in public administrations, many questions of interoperability remain unanswered.

Protecting critical infrastructure

An additional priority revolves around reinforcing the protection of communication networks for CSDP structures, missions and operations. There are some highly intractable and complex issues in this area, ranging from how to reconcile member state responsibility for critical infrastructure (CIS) protection in home and deployed contexts, to how to engage with the private sector.

A particular set of issues arises here because, unlike NATO, the EU does not possess its own organic

assets. Therefore, during the strategic planning and force generation phases, it is essential to understand how infrastructure used during CSDP missions can be adequately protected – with input either from participating member states or with support from the private sector. When it comes to the need for robust, available, and clear communications channels for operations deployed in hostile environments, in fact the private sector often proves to be a valuable partner by providing either satellite, terrestrial fixed line or mobile means of communication. From a cyber-security standpoint, this raises challenges with regard to risk management, application of security standards and assurance of service to critical applications. At the European level, continuous upgrades of operational CIS security capabilities in the EUMS and Council, alongside the growing maturity of the CERT-EU, demonstrate progress on organisational capabilities.

Embedding cyber security into crisis management

The proposed Cyber Defence Policy Framework will also need to address cyber security during crisis management, in particular through its incorporation into the CSDP planning process and through civil-military aspects of crisis management planning. Noting the complex framework in CSDP planning processes – which involves extensive interactions between different strategic committees and the Operational Commander designate – cyber security would need to be addressed in both the strategic appraisal phase (where the intentions and possible courses of action of actors are evaluated) and in the force generation phase.

> 'Understanding if, why and how possible actors may seek to exploit cyberspace in order to influence or affect an EU-led CSDP operation is key.'

Understanding if, why and how possible actors may seek to exploit cyberspace in order to influence or affect an EU-led CSDP operation is key. This understanding should be derived from a mix of classical intelligence work and sophisticated technical analysis. Concerning force generation, once the decision has been taken to conduct an operation, the Operational Commander must coordinate offers of assets from other contributing member states. In this particular domain, the Operational Commander must thus strike a satisfactory balance between the cyber security facets of the operational context (including local, regional and global cyber security actors and their possible motivations); the relative maturity of cyber-defence capabilities of those member states offering assets; and the overall mission objectives. Ultimately, any policy framework will need to establish clear accountability for how the Operational Commander decides to manage possible cyber-security risks to a crisis management operation.

Generating opportunities for training and exercising

Various EU member states have articulated the need to expand measures for training and education activities. Currently, the picture across the EU is rather mixed: EU-level organisations such as the European Security and Defence College (ESDC) run general training courses on cyber defence. Other actors in the civil or law enforcement domain, such as the EU Agency for Network and Information Security (ENISA) or the European Cybercrime Training and Education Group (ECTEG), also produce technical and operational training products and run a variety of courses aimed at different audiences. These include individual and collective training and simulations based on realistic scenarios.

ENISA has been particularly visible in the preparation and conduct of a series of cyber-security exercises and, in 2014, it will host the third pan-European exercise Cyber-Europe 2014, with 29 European countries participating from the EU and EFTA.

At a member state level, numerous EU countries have been running bilateral or small exercises with other like-minded nations. At NATO, too, the Cyber Coalition exercise in 2011 tested the Alliance's ability to respond to large scale cyber-attacks – involving 23 NATO countries and six partners (including the EU as observer). The CCDCoE, affiliated to NATO, is a key provider of training and education outputs, especially in the area of exercises. Leveraging these opportunities, especially through a framework of Pooling and Sharing, constitutes an opportunity for quick wins in an area that is relatively uncontroversial and where there is significant demand from member states.

Liaising with the broader EU framework

The EU Cyber Security Strategy provides a common framework for a comprehensive approach, bringing together the policy fields of resilience

and network and information security, defence and CSDP, criminal justice, and foreign affairs. The existence of a relatively homogenous set of policy instruments across these different portfolios could aid in the delivery of such a concerted effort. In particular, overlapping or mutually supportive cooperation will need to be identified, for example, between CSDP actors and the European Cybercrime Centre (EC3) or ENISA. Sources of synergies might be found in sharing products such as training and exercise material, access to expertise and the exploitation of national level practice identified, collected and disseminated by other actors.

There are also examples of discrete instruments such as forensic analysis capabilities or cooperation agreements that exist between EU level actors and private sector cyber-security providers that could be leveraged in order to benefit common pan-European efforts. Other areas which lend themselves to cooperation include attaining a better understanding of how all actors stand to profit from developing a coherent research agenda (which explores dual use cyber-security technologies) and facilitating more efficient cooperation between critical infrastructure owner-operators and different EU actors.

Nonetheless, achieving this requires successfully aligning the complex inter-institutional wiring of the EU. It also requires ensuring that any cooperative efforts are consistent with European values such as freedom of expression or the right to the protection of personal data, whilst respecting the separation of intelligence, law enforcement, and defence domains. This will be especially sensitive given the increasing political interest in – and scrutiny of – state-level capabilities in cyberspace.

Cooperating with international partners

Finally, and more broadly, the EU is slowly building on its contacts with other international partners, both bilaterally and through other regional organisations. These contacts have largely been expanded through three mechanisms. First, bilateral cooperation with third countries, notably the EU-US Working Group on Cybersecurity and Cybercrime and other bilateral engagements with India, Brazil, and China.

Second, engagement in other international platforms, for example the so-called 'London Process' that has so far seen three high-level diplomatic conferences (London 2011, Budapest 2012 and Seoul 2013) convened to discuss norms in cyberspace and 'rules of the road'. Such platforms are attractive because they offer a cost-effective way to further cooperation with a range of international actors and, for some issues (such as reinforcing the idea of the cyberspace as a globally free domain), they can support the projection of key messages on the international stage.

Third, the EU Cyber Defence Policy Framework will need to further strengthen nascent cooperation with NATO. As a pre-eminent national security provider that is itself undergoing some sort of identity crisis, NATO has been building up its cyber-defence capabilities with a specific concept and a detailed action plan. Institutionally, NATO has established cyber defence Rapid Reaction Teams (RRTs) and brought its Computer Incident Response Capability (NCIRC) to full operational capability to work alongside its Cyber Defence Management Authority (CDMA) structure.

Outside of formal NATO command and control structures, the CCDCoE is being strengthened with additional contries joining, and the Centre itself published a landmark document (known as the 'Tallinn Manual') on the interpretation of the Law of Armed Conflict as it relates to cyber defence. A key aspect of the proposed EU Cyber Defence Policy Framework will be to identify how cooperation can be established given these types of existing and emergent capabilities within the Alliance, and for how areas of complementarity between the two actors can result in a better use of limited resources. Exploiting 'Berlin-plus'-type agreements with regard to the EU accessing NATO organic cyber-defence capabilities for operations might be one such avenue for practical cooperation.

Those charged with building upon the Cyber Defence Policy Framework will undoubtedly need to hit the ground running if they are to translate these ambitions into reality. It would be naive to suggest that some of these are not without their challenges (especially regarding cooperation within Europe but also between the EU and NATO), but a successful completion of the Framework in 2014 might be enough to silence criticism that the landmark December summit was, in this respect, a missed opportunity. The next Defence Summit scheduled for 2015 will provide an occasion for the new EU leadership to review progress on this elaborate agenda.

Neil Robinson is Research Leader at RAND Europe and a member of the EUISS Cyber Task Force.