CYBER SECURITY AND CYBER DEFENCE IN THE EUROPEAN UNION

OPPORTUNITIES, SYNERGIES AND CHALLENGES

By Wolfgang Röhrig, Programme Manager Cyber Defence at EDA
and
Wg Cdr Rob Smeaton, Cyber Defence Staff Officer at EUMS CIS Directorate.

Information and communication technologies are a critical enabler for our economic growth and our societies now rely on the internet in many different ways and on many different levels. The digital world has brought not only enormous benefits, but also vulnerabilities. Cyber security incidents, either intentional or accidental, are increasing at an alarming rate and are impacting on societal norms; they could also disrupt essential services such as water, healthcare, electricity or mobile services.

The threat landscape covers everything from the internet vandalism to physical and criminal damage. The theft of intellectual property and economic or state-sponsored espionage lies somewhere in between. The capacity to destroy or damage physical property represents a strategic shift. Malware targeting industrial control systems (e.g. STUXNET), constitutes one example of this new type of threat. We can anticipate the development of more dangerous tools and, eventually, their use. The European Network and Information Security Agency, ENISA publishes an annual report on the development of the threat landscape reflecting recent technology trends. The picture ENISA paints with their latest report is quite alarming. Targeted attacks through Advanced Persistent Threat (APT) malware will become the most difficult threats to counter.

THE EU CYBER SECURITY STRATEGY AND THEIR IMPACT ON THE DEFENCE SECTOR

On 7 February 2013 the European Union (EU) published its "Cyber Security Strategy – An Open, Safe and Secure Cyberspace". Impressively, the Strategy takes, like other national cyber security strategies, a comprehensive approach. It addresses, within the remit of EU's responsibilities, the civil aspects of cyber security as well as Cyber Defence for the Common Security and Defence Policy (CSDP). In December 2013 at the EU Council on defence matters, the EU heads of state and government recognised cyber defence as a priority for capability development.

Cyber Space is now widely recognised by the military as the 5th operational domain besides land, sea, air and space. The success of conventional military operations in the other domains is enabled by, and dependent on the assured availability of, and access to, cyberspace. The difficult question for the military is:

- From where will the next attacks originate?
- What will be the attacker's motivation;
- What will be their target;
- How will they attack us?

What we can assume is that like us, the attackers will follow technological trends. The same technology that brings benefits also brings vulnerabilities and options for attackers to exploit. The threat landscape must be seen in the context of technological trends and military implications:

- Conventional military activity relies on ensured access to Cyber Space;
- The military is increasingly dependent on civil (critical) infrastructures – both home based and in the operational theatre;
- As the military become increasingly interconnected, using internet technologies, internet vulnerabilities get closer to individual soldiers and their weapon systems.
- The military can no longer afford the cost and performance penalties of not adopting commercial internet technologies for their expanding networks. Thus military capabilities are susceptible to the same threats, vulnerabilities and solutions as the civil sector.

... MILITARY CAPABILITIES ARE SUSCEPTIBLE TO THE SAME THREATS, VULNERABILITIES AND SOLUTIONS AS THE CIVIL SECTOR ...

The defence part of the EU Cyber Security Strategy defines four major work strands:

- Building of Cyber Defence Capabilities with EU Member States (MS),
- Building the EU Cyber Defence Policy framework,
- Promotion of the civil-military dialogue, and
- Dialogue with international partners like NATO and other major stakeholders.

CYBER SECURITY FOR CSDP - THE ROLE OF EDA AND THE EUMS

The EU is solely engaged in cyber self-protection and assured access to cyber space to enable conventional military activity. Offensive cyber capabilities have not been developed, or deployed, under the EU banner.

It is important to understand that the EU does not have standing military forces or EU- owned military equipment for EU operations. When the EU launches a military operation, the EU is wholly dependent on force contributions from EU member states or other force contributors.

This basic principle also applies to Cyber Defence, so the MS are the key to force generation. They will be the ones who will be asked to provide Cyber Defence capabilities for an EU-led Operation. It is, therefore, in the interest of the EU to encourage MS in their efforts to develop and maintain cyber inventories. The level of Cyber Defence capability varies greatly between Member States. They must all now invest, and continue to invest in cyber defence capabilities. In order to be effective, the EU and its member states must develop and deploy a robust inventory of in-depth (layered) cyber defence capability for the military, as part of their national cyber defence strategy and capabilities.

The EU Military Staff (EUMS) and the European Defence Agency (EDA) are working to improve EU cyber defence capabilities.

The EUMS comprises around 200 seconded national experts, based in Brussels as part of the EU External Action Service (EEAS). The EUMS is responsible for providing the EU High Representative with military advice and for providing EU Council bodies with military options should the MS decide on military action. The EUMS' role, in Cyber Defence, is to develop doctrine and policy to ensure that the different MS cyber protection elements operating independently, in support of an EU military operation, provide robust collective protection of the EU force so the collective nature of the defence does not become a threat or vulnerability for the EU Force.

The EDA is a small agency - with a staff of about 130 employees from different EU MS. The EDA supports MS in different areas of military capability development. In 2011 the EU MS participating in EDA had already raised awareness by making Cyber Defence one of the top ten priorities for EU military capability development. The immediate consequence, in late 2011, was the creation of a Project Team (PT) Cyber Defence gathering contributors from the Ministries of Defence (MoD) and relevant actors from the EU civilian world around one table in the EDA. The PT is a unique tool within the EU to identify options for cooperation between MS and for civil-military cooperation.

The 2013 EDA Landscaping Study provided a detailed picture of capacities and concepts already in place in MS and EU Institutions that could be drawn upon to make CSDP operations more "Cyber-resilient". The study also identified existing gaps and suitable opportunities for MS cooperation to close the gaps.

In terms of policy, the "EU Concept for Cyber Defence for EU-led Military Operations" was agreed in December 2012 and is the EU military policy and guidance for operational commanders to ensure that they create and maintain cyber situational awareness. The Concept outlines the need to adopt a risk based threat assessment methodology and to create coordinating structures to ensure that national cyber defence capabilities work coherently to protect the Force. MS augmented the concept in March 2013 with the "EU Cyber Defence Capability Requirements Statement".

CYBER DEFENCE COOPERATION BETWEEN EU MEMBER STATES INCLUDING POOLING & SHARING

Within the EU there is often a discussion between MS and the Institutions about what constitutes EU business, and what is sovereign, and therefore national, business? Sovereignty should not be seen as an obstacle for cooperation between MS in the area of cyber self-protection. The core sovereignty issues in cyber self-protection could be related to the ownership of information and information infrastructures. The owner has sole responsibility to protect and defend their information and infrastructures against threats and attacks. There are many ways to establish and maintain the effective defence capabilities and capacities. When financial efficiently assumes a greater importance, ruling out cooperation from the start, removes a potential tool to achieve capability synergies and financial savings. In the rapidly evolving cyber threat landscape, it may not be possible to establish, maintain and use a cyber defence capability effectively without cooperation. Nations are finding it difficult, or unaffordable, to continue to develop cyber capability on a national basis. For them cooperation, sharing development costs, is essential, rather than desirable, when developing and maintaining capabilities.

Cyber Defence is certainly an issue with much sensitivity. Cooperation in cyber

> ... THE CONCEPT OUTLINES THE NEED TO ADOPT A RISK BASED THREAT ASSESSMENT METHODOLOGY AND TO CREATE COORDINATING STRUCTURES TO ENSURE THAT NATIONAL CYBER DEFENCE CAPABILITIES WORK COHERENTLY TO PROTECT THE FORCE ...

defence is about trust amongst partners with shared interests and requirements. If there is trust, common interest and willingness to cooperate, many options for synergies become real opportunities. This approach is used elsewhere in Defence; for more than a decade Belgium and the Netherlands have operated their naval command together. This success should inspire us to tackle cyber defence in the same way. Whether to cooperate, with whom to cooperate and the extent of that cooperation are sovereign decisions; sovereignty itself is not the decisive factor; trust and shared interest are more powerful drivers when deciding on the degree of cooperation. The level of trust will determine the price for, and provide a clear understanding of the consequences of, a decision for, or against, cooperation.

In November 2012 the EU defence ministers agreed to put Cyber Defence on the Pooling & Sharing agenda. With the principle of Pooling and Sharing the EDA has established a framework for achieving more together without losing sovereignty over assets and resources. Projects in the areas of cyber defence training and exercise ranges and cyber situational awareness packages for headquarters have been initiated. More options are under evaluation. To get ahead of the threat, we must exploit all potential synergies.

... IF WE ARE TO DELIVER EFFECTIVE PROTECTION, THE MILITARY MUST BE PART OF THE CIVILIAN CYBER PROTECTION ACTIVITY AND BE ABLE TO SHARE INFORMATION WITH ALL ACTORS ...

CIVIL-MILITARY COOPERATION IN THE EU

The EU rightly prides itself on its ability to deploy civilian and military responses to global crises. It is important that the EU adopts a common civilian and military approach to self-protection in cyber space.

Military networks, both classified and unclassified, depend on internet technology – the same hardware and software used by civilians for their networks. To protect them the military must ‘do’ cyber security and use civilian training and civilian standards. There are many common aspects of civilian and military cyber self-protection. EU military operations have a high dependence on civilian actors. For example, the EU military operation recently launched to the Central African Republic aims to establish a secure environment for the civilian humanitarian aid organisations to distribute aid and establish basic facilities for the internally displaced population. In order to do this successfully, effective engagement at the unclassified/internet level is essential. There is no difference between military and civilian actors in this area. If we are to deliver effective protection, the military must be part of the civilian cyber protection activity and be able to share information with all actors.

The organisational set-up of the EU lends itself to close civil-military cooperation in Cyber Security and Defence. Many defensive capabilities developed for Cyberspace either on the civil or the military side, have dual-use potential. Just as we strive to ensure our government and national critical infrastructure within the EU is resilient to the cyber threat, we must protect the equipment and systems deployed on EU-led CSDP operations and missions outside of the EU.

COOPERATION BETWEEN NATO AND EU

Twenty-two nations are members of both the EU and NATO; each of these 22 nations has a “single set of forces” at readiness that is available to serve on operations. In today’s world we cannot, and will not, invest in capabilities that can only be used by one organisation. The EU and NATO have started to develop a dialogue in areas of common interest, such as converging NATO and EU standards in cyber security and defence, but the engagement must be intensified.

CONCLUSIONS ON THE WAY AHEAD IN VIEW OF THE FUTURE EU CYBER DEFENCE POLICY FRAMEWORK

The Council on defence matters in December 2013 tasked the EEAS to develop a Cyber Defence Policy Framework, including a roadmap, in 2014, and is anticipated to focus on;

- Development of MS' cyber defence capabilities, research and technologies through the development and implementation of a comprehensive roadmap for strengthening cyber defence capabilities;
- Reinforced protection of communication networks supporting CSDP structures, missions and operations;
- Mainstreaming of cyber security into EU crisis management;
- Raising awareness through improved training, education and exercise opportunities for the MS;
- Synergies with wider EU cyber policies and all other relevant actors and agencies in Europe such as ENISA;
- Cooperation with relevant international partners, notably with NATO, as appropriate.

The public perception is that cyber protection primarily is a technological rather than human, issue. Technology is moving quickly to remove technical vulnerabilities so human factors are rapidly emerging as the priority, displacing technological issues.

For once, technology is unlikely to be a significant issue in terms of military cyber defence. The synergies with civilian cyber defence (is there a substantive difference?) ensures a constant stream of technology that will be used by military and civilian defenders to counter identical, or very similar, threats. The catch is the cyber defenders. The military are unlikely to have unique cyber defence capabilities, so they will be in direct competition with civilian (pay packets) for people.

Following the findings of the EDA landscaping study, the EU placed emphasis on human factors in cyber defence; behind every cyber-attack is an astute mind. For the time being, humans are our first (users) and our last (Cyber Defence Specialists) lines of defence. For both attackers and defenders the technology is the means with which they try to fulfil their objectives and achieve their aims. In that sense there is no difference between the cyber domain and the physical ones.

A challenge for the military, both today and in the future, will be growing and retaining sufficient high quality cyber trained people in our armed forces. While the Cyber Security Technology market is broad and developing, the pool of young cyber talents, which have the potential to become cyber specialist, is small. In this competitive market the military must find new and innovative ways to make the military an attractive option for talented individuals if we are to have the right people available.

The challenge is not limited to cyber specialists; all personnel at all levels require an increasingly sophisticated understanding of cyber space and how to operate effectively in cyber space. The ICT users, these days consisting of almost everybody in an organisation, has a role to play in cyber defence. So they must have up-to-date knowledge and awareness of the threat environment and how to react in the event of an incident. The decision makers must understand the cyber options and the impact of cyber operations against us when making decisions. A cyber defence focus during education, training and exercises is vital if we are to achieve an adequate operational cyber defence capability.

The human being is, and will continue to be, our most precious cyber defence asset. The knowledge and expertise of our people is a fundamental requirement for a European Cyber Defence culture and to enable acceptable operational capability in today's technological epoch. ■

Disclaimer

This article is a product of the two authors. It represents neither the opinions nor policies of the European Defence Agency nor of the EU Military Staff and provides an independent view.

ABOUT THE AUTHORS

Wolfgang Röhrig entered the German Navy in 1985 and graduated from the Bundeswehr University Hamburg as MBA in 1990. Until 2012 he served in several positions for the Bundeswehr and for NATO SHAPE. Since March 2012 he is appointed to EDA and became programme manager cyber defence beginning 2014.

Wing Commander J P R Smeaton CEng BEng (Hons) MIET RAF was commissioned into the Royal Air Force as an Engineering Officer (Communications and Electronics) in 1990. In 2012 he was seconded as a National Expert to the EU Military Staff, and is the Action Officer with responsibility for Cyber policy.