Council of the European Union

**Brussels, 18 November 2014**

**15585/14**

**COPS 303**
**POLMIL 103**
**CYBER 61**
**RELEX 934**
**JAI 880**
**TELECOM 210**
**CSC 249**
**CIS 13**
**COSI 114**

**OUTCOME OF PROCEEDINGS**

| | |
|---|---|
| From: | Council |
| On: | 17–18 November 2014 |
| N° prev. doc.: | 15193/14 + COR 1 COPS 287 POLMIL 97 CYBER 58 RELEX 897 JAI 845 TELECOM 196 CSC 242 CIS 12 COSI 111 |
| Subject: | EU Cyber Defence Policy Framework |

Delegations will find attached the EU Cyber Defence Policy Framework, as adopted by the Council on 18 November 2014.

**ANNEX**

# EU CYBER DEFENCE POLICY FRAMEWORK

## Context and Objectives

Cyberspace is often described as the fifth domain of military activity, equally critical to European Union (EU) Common Security and Defence Policy (CSDP) implementation as the domains of land, sea, air, and space. The successful implementation of CSDP has been increasingly dependent on the availability of, and access to, a secure cyberspace. Robust and resilient cyber defence capabilities are now required to support CSDP structures and CSDP missions and operations.

The European Council Conclusions on CSDP of December 2013 together with the Council Conclusions on CSDP of November 2013 called for the development of an EU Cyber Defence Policy Framework, on the basis of a proposal by the High Representative, in cooperation with the European Commission and the European Defence Agency (EDA).

The objective of this document is to provide a framework to the European Council and Council conclusions, as well as to the cyber defence aspects of the EU Cybersecurity Strategy[1]. The document identifies priority areas for CSDP cyber defence and clarifies the roles of the different European actors, whilst fully respecting the respective responsibilities and competences of Union actors and the Member States as well as the institutional framework of the EU and its autonomy of decision-making. The implementation process of the EU Cybersecurity strategy has been agreed by the Friends of the Presidency Group on Cyber Issues.

[1] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", of 7 February 2013, and the related General Affairs Council conclusions of 25 June 2013.

A primary focus of this policy framework will be the development of cyber defence capabilities, made available by Member States for the purposes of the CSDP as well as the protection of the European External Action Service (EEAS) communication and information networks relevant to CSDP. In the area of training, emphasis is given to the development of programmes for different audiences in the CSDP chain of command. It is important that the cyber dimension is adequately addressed in exercises in order to improve the EU's ability to react to cyber crises in a CSDP context, to improve strategic decision-making procedures and to strengthen the information infrastructure architecture. Cyberspace is a rapidly developing domain where dual-use capabilities play an essential role; therefore it is necessary to develop civil-military cooperation and synergies with wider EU cyber policies to address the new challenges it presents, while respecting the Member States internal organisation and competences.

This paper outlines principles to facilitate cooperation with the private sector on cyber defence capability development, with a particular focus on strengthening Research &Technology (R&T) and the European Defence Technological and Industrial Base (EDTIB). Moreover, it also ensures coherence between the EU and the North Atlantic Treaty Organisation (NATO) cyber defence efforts and proposes areas for cooperation between them.

Finally, the objectives of cyber defence should be better integrated within the Union's crisis management mechanisms. In order to deal with the effects of a cyber crisis, relevant provisions of the Treaty of the EU and the Treaty on the Functioning of the EU[2] may be applicable, as appropriate.

[2] Articles 222 TFEU and 42(7) TEU, with due consideration of Art. 17 TEU.

**Priorities for the EU Cyber Defence Policy Framework**

**1. Supporting the development of Member States cyber defence capabilities related to CSDP**

In order to ensure the resilience of the networks supporting CSDP implementation, the focus shall be on both the improvement of the protection of EEAS managed CSDP structures' communication networks and on the Member States' development of cyber defence capabilities available for CSDP missions and operations. To this extent, Member States, the EEAS and EDA should work together to deliver effective cyber defence capability.

The development of cyber defence capabilities and technologies should address all aspects of capability development, including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability.

A continuous assessment of the vulnerabilities of the information infrastructures that support CSDP missions and operations is required, along with a near real-time understanding of the effectiveness of the protection. From an operational point of view, the primary focus of cyber defence activities will be to maintain the functionality of CSDP communication and information networks, unless specified otherwise within the mandate of the operations or missions.

As CSDP military operations rely on a Command, Control, Communications and Computer (C4) infrastructure provided by the Member States, a certain degree of strategic convergence when planning cyber defence requirements for the information infrastructure is necessary.

**Building upon the work of the EDA Cyber Defence Project Team to develop cyber defence capabilities, the EEAS/EDA and Member States will:**

- Use the Capability Development Plan and other instruments that facilitate and support cooperation between Member States in order to improve the degree of convergence in the planning of cyber defence requirements of the Member States at the strategic level, notably on monitoring, situational awareness, prevention, detection and protection, information sharing, forensics and malware analysis capability, lessons learned, damage containment, dynamic recovery capabilities, distributed data storage and data back-ups;
- Support current and future cyber defence related Pooling and Sharing projects for military operations (e.g. in forensics, interoperability development, standard setting);
- Develop a standard set of objectives and requirements defining the minimum level of cybersecurity and trust to be achieved by Member States, drawing on existing EU-wide experience;
- Facilitate exchanges between Member States on national cyber defence doctrines, training programmes and exercises as well as on cyber defence oriented recruitment, retention and reservists programs;
- Improve cooperation between military CERTs of the Member States on a voluntary basis, to improve the prevention and handling of incidents;
- Consider developing cyber defence training in view of EU Battlegroup certification.
- To the extent that the improvement of cyber defence capabilities depends upon civilian network and information security expertise, Member States may request assistance from ENISA.

**2. Enhancing the protection of CSDP communication networks used by EU entities**

Without prejudice to the role of the CERT-EU as the central EU cyber incident response coordination structure for all Union institutions, bodies and agencies and within the framework of the relevant rules concerning the Union budget, the EEAS shall develop an adequate and autonomous understanding of security and network defence matters and develop its own IT security capacity. It will aim to improve the resilience of the EEAS CSDP networks, with a focus on prevention, detection, incident response, situational awareness, information exchange and early warning mechanisms.

The protection of EEAS communication and information systems and the development of Information Technology (IT) security capacities are led by the EEAS MDR (Managing Directorate for Resources). Additional dedicated resources and support will also be provided by the European Union Military Staff (EUMS), Crisis Management and Planning Directorate (CMPD) and Civilian Planning and Conduct Capability (CPCC). This IT security capability will cover both classified and unclassified systems and will be an integral part of the existing operational entities.

There is also a need to streamline security rules for the information systems provided by different EU institutional actors during the conduct of CSDP operations and missions. In this context, a unified chain of command could be considered with the aim to improve the resilience of networks used for CSDP.

**In order to improve the protection of CSDP communication networks, the MDR, EUMS, CMPD and CPCC, in cooperation with INTCEN, will:**

- Strengthen IT security capacity within the EEAS, based on existing technical capability and procedures, with a focus on prevention, detection, incident response, situational awareness, information exchange and early warning mechanism. A cooperation strategy with the CERT-EU and existing EU cyber security capabilities shall also be developed or, where available, further enhanced;
- Develop coherent IT security policy and guidelines, also taking into account technical requirements for cyber defence in a CSDP context for structures, missions and operations, bearing in mind existing cooperation frameworks and policies within the EU to achieve convergence in rules, policies and organisation;
- Building upon existing structures, strengthen cyber threat assessment and intelligence capability to identify new cyber risks and provide regular risk assessments based on the strategic threat assessment and near real-time incident information coordinated between relevant EU structures and made accessible at different classification levels;
- Promote real-time cyber threat information sharing between Member States and relevant EU entities. For this purpose, information sharing mechanisms and trust-building measures shall be developed between relevant national and European authorities, through a voluntary approach that builds on existing cooperation;
- Develop and integrate into strategic level planning, a unified cyber defence concept for CSDP military operations[3] and civilian missions;
- Enhance cyber defence coordination to implement objectives related to the protection of networks used by EU institutional actors supporting CSDP, drawing on existing EU-wide experiences;
- Review regularly resource requirements and other relevant policy decisions based on the changing threat environment, in consultation with the relevant Council working groups and other EU institutions;

[3] In the case of military operations, the current EU Concept for Cyber Defence for EU-led Military Operations should be updated in the light of this Policy Framework.

**3. Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector**

Cyberspace is a rapidly developing domain where dual-use capabilities play an essential role and where this framework will improve the synergy between CSDP and other EU horizontal policies (such as space and maritime security policies) and strategies, such as the Maritime Security Strategy and its Action Plan. Without prejudice to Member States' internal organisation and legislation, civil-military cooperation in the cyber domain will benefit from dual-use cyber capability development, R&T, exchange of best practices, information exchange and early warning mechanisms, incident response risk assessments and awareness raising. Joint activities in the field of training and exercises will enhance cooperation and reduce costs across different policy areas.

**EDA, European Network and Information Security Agency (ENISA)[4], European Cybercrime Centre (EC3), together with other relevant EU Agencies, as well as the Member States are encouraged, in the CSDP environment, to enhance their cooperation in the following areas:**

- Develop common cyber security and defence competence profiles based on international best practises and certification used by EU Institutions, taking also into account private sector certification standards;
- Contribute to develop further and adapt public sector cyber security and defence organisational and technical standards for use in the defence and security sector. Where necessary, build on the ongoing work of ENISA and EDA;
- Develop a working mechanism to exchange best practice on exercises, training and other areas of possible civilian-military synergy;
- Leverage existing EU cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyber defence capabilities;

[4] Within the mandate of ENISA and aligned with ENISA's multi-annual Working Plan, without overlapping with Member States' competences.

Improving civilian cyber security is an important factor which contributes to overall network and information security resilience. The proposal for a Directive on Network and Information Security (NIS) is expected to increase preparedness at the national level, and strengthen cooperation at Union level between Member States both at strategic and operational level. This cooperation should involve both national authorities overseeing cybersecurity policies as well as national CERTs and CERT-EU. The public-private NIS platform aims to identify technologically neutral best practices to enhance cybersecurity and develop incentives to adopt secure ICT solutions.

**Research and technology in cooperation with the private sector and academia**

Operators of infrastructure and Information and Communication Technology (ICT) services for civilian and defence purposes are confronted with similar cyber security challenges, as a result of common technology and operational capability requirements. Common R&T needs and common requirements for systems are anticipated to improve the interoperability of systems in the long run, as well as to reduce the costs of solutions development. Achieving economies of scale is a necessity in order to face the ever increasing number of threats and vulnerabilities. This should in turn facilitate the preservation and growth of a competitive cyber defence industry in Europe.

Cyber defence capability development has an important R&T dimension. Within the framework of the Cyber Defence Research Agenda (CDRA) the EDA has provided a sound basis for the prioritisation of future R&T spending and capability development in both national and European environment.

The development of strong technological capacities in Europe to mitigate threats and vulnerabilities is essential. Industry will remain the primary driver for cyber defence related technology and innovation. So it will be crucial to maintain close cooperation with the private sector, seeking synergy with civilian solutions, services and capabilities wherever possible (in particular in cryptography, embedded systems, malware detection, simulation and visualisation techniques, network and communication systems protection, identification and authentication technology areas). It is also important to foster an assured and competitive European industrial cyber security supply chain by supporting the development of a robust European cybersecurity sector including through involvement with Small and Medium sized Entreprises (SMEs).

**To facilitate civil-military cooperation in cyber defence capability development and to strengthen the European Defence Technological and Industrial Base[5] in line with the EU approach on cyber industry, the EDA together with the Commission services, as well as the Member States will:**

- Seek synergies of R&T efforts in the military sector with civilian Research & Development programmes, such as HORIZON 2020, and consider the cyber security and defence dimension when setting up the Preparatory Action on CSDP related research;
- Share cyber security research agendas between EU institutions and agencies (e.g. Cyber Defence Research Agenda) notably through the European Framework Cooperation, and share resulting roadmaps and actions;
- Support the development of industrial eco-systems and clusters of innovation covering the whole security value chain by drawing on academic knowledge, SMEs innovation and industrial production;
- Support EU policy coherence to ensure that policy and technical aspects of EU cyber protection remain at the forefront of technology innovation and are harmonised across the EU (cyber-threat analysis and assessment capability, "security by design" initiatives, dependency management for technology access etc.);
- Contribute to improve the integration of cybersecurity and cyber defence dimensions in the programmes that have a dual-use security and defence dimension, e.g. SESAR.
- Actively support synergies with the civilian cybersecurity industrial policy development undertaken at national level by the Member States and at European level by the Commission.

[5] Communication "Towards a More Competitive and Efficient Defence and Security Sector", COM (2013) 542

**4. Improve training, education and exercises opportunities**

**Training and Education**

In order to develop a common cyber defence culture at all levels of CSDP chain of command, including missions and operations, there is a need to improve cyber defence training opportunities. Moreover, during a period of shrinking defence expenditure, it is crucial that education and training budgets are used efficiently while delivering the best possible quality. Pooling and sharing cyber defence education and training at the European level will be of key importance.

**The EEAS will set the following CSDP training priorities, together with EDA, the European Security and Defence College (ESDC) and Member States:**

- Based on the EDA Cyber Defence Training-Need-Analysis and the experiences gained in cyber security training of the ESDC, establish CSDP Training and Education for different audiences, including EEAS, personnel from CSDP missions and operations and Member States' officials;
- Propose the establishment of a cyber defence dialogue on training standards and certification with Member States, EU institutions, third countries and other international organisations, as well as with the private sector;
- Based on the EDA feasibility assessment, explore the possibility and rationale to set up a cyber defence training facility for CSDP;
- Develop further EDA courses to meet the CSDP cyber defence training requirements;
- Follow the established ESDC certification mechanisms for the training programmes in close cooperation with the relevant services in the EU institutions, based on existing standards and knowledge. Consider the possibility of setting up cyber specific modules in the framework of the Military Erasmus initiative;
- Create synergies with the training programmes of other stakeholders such as the ENISA, Europol, European Cybercrime Training and Education Group (ECTEG) and the European Police College (CEPOL);
- Explore the possibility of joint ESDC-NATO Defence College cyberdefence training programmes, open to all EU Member States, in order to foster a shared cyberdefence culture;
- Engage with European private sector training providers, as well as academic institutions, to raise the competencies and skills of personnel engaged in CSDP operations and missions.

**Exercises**

There is a need to improve cyber defence exercise opportunities for military and civilian CSDP actors. Joint exercises serve as a tool to develop common knowledge and understanding of cyber defence. This will enable national forces to enhance their preparedness to operate within a multinational environment. Conducting common cyber defence exercises will also build interoperability and trust.

**The EEAS and the Member States will focus on promoting cyber defence elements in CSDP and other exercises:**

- Integrate a cyber defence dimension into existing exercise scenarios' for MILEX and MULTILAYER;
- Develop, as appropriate, a dedicated EU CSDP cyber defence exercise and explore possible coordination with pan-European cyber exercises such as *CyberEurope*, organised by ENISA;
- Consider the possibility of participating in other multinational cyber defence exercises;
- Once the EU has developed a CSDP cyber defence exercise, involve relevant international partners, such as the OSCE and NATO, in accordance with the EU exercise policy.

**5. Enhancing cooperation with relevant international partners**

In the framework of international cooperation there is a need to ensure a dialogue with international partners, specifically NATO and other international organisations, in order to contribute to the development of effective cyber defence capabilities. Increased engagement should be sought with the work being done within the framework of the Organisation for Security and Cooperation in Europe (OSCE) and the United Nations (UN).

There is a political will in the EU to cooperate further with NATO on cyber defence in developing robust and resilient cyber defence capabilities as required within this Policy Framework. Regular staff-to-staff consultations, cross-briefings, as well as possible meetings between the Politico-Military Group and relevant NATO committees, shall help to avoid unnecessary duplication and ensure coherence and complementarity of efforts, in line with the existing framework of cooperation with NATO.

**The EEAS and EDA, together with the Member States, will develop further cyber defence cooperation between the EU and NATO, with due respect to the institutional framework and the EU's decision-making autonomy:**

- Exchange of best practice in crisis management as well as military operations and civilian missions;
- Work on coherence in the development of cyber defence capability requirements where they overlap, especially in long-term cyber defence capability development;
- Enhance cooperation on concepts for cyber defence training and education as well as exercises;
- Utilise further the EDA liaison agreement with the NATO Cooperative Cyber Defence Centre of Excellence as an initial platform for enhanced collaboration in multinational cyber defence projects, based on appropriate assessments;
- Reinforce cooperation between the CERT-EU and relevant EU cyber defence bodies and the NCIRC (NATO Computer Incident Response Capability) in order to improve situational awareness, information sharing, early warning mechanisms and anticipate threats that could affect both organisations.

**With regard to other international organisations and relevant EU international partners, the EEAS and the EDA, together with the Member States, will, as appropriate:**

- Follow strategic developments and hold consultations in cyber defence issues with international partners (international organisations and third countries);
- Explore possibilities for cooperation on cyber defence issues, including with third countries participating in CSDP missions and operations;
- Continue to support the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in State behaviour, by promoting the ongoing establishment of international norms in this field.

**Follow-up**

A six-monthly progress report, that includes the five areas outlined above, should be presented to the Politico-Military Group and to the Political and Security Committee and other relevant Council working groups, in order to assess the implementation of the policy framework. It is essential that, as the cyber threat develops, new cyber defence requirements are identified, and then included in the Cyber Defence Policy Framework.