Council of the European Union

Brussels, 1 June 2016
(OR. en)

9701/16

LIMITE

COPS 168
POLMIL 54
EUMC 63
CYBER 62
RELEX 466
JAI 503
TELECOM 108
CSC 167
CIS 15
COSI 94

**NOTE**

| | |
|---|---|
| From: | Politico-Military Group (PMG) |
| To: | Political and Security Committee (PSC) |
| Subject: | Six Monthly Report on the Implementation of the Cyber Defence Policy Framework |

Delegations will find in annex the Six Monthly Report on the Implementation of the Cyber Defence Policy Framework, as finalised by the Politico-Military Group on 31 May 2016.

# SIX MONTHLY REPORT ON THE IMPLEMENTATION OF THE CYBER DEFENCE POLICY FRAMEWORK

## REFERENCE DOCUMENTS

A. European Council conclusions December 2013

B. Council conclusions November 2014

C. EU Cyber Defence Policy Framework

D. EU Cybersecurity Strategy

E. Council conclusions May 2015

F. First Six-Month report on the implementation of the Cyber Defence Policy Framework (endorsed by the PSC in July 2015)

G. Second Six-Month report on the implementation of the Cyber Defence Policy Framework (endorsed by the PSC November 2015

H. EU Concept For Cyber Defence for EU-led Military Operations (of 2012, currently under revision)

I. Cyber Defence Capability Requirements Statement

## 1. PURPOSE

This document provides an overview of the implementation of the EU Cyber Defence Policy Framework (CDPF) for the period from 15 October 2015 – 15 April 2016. The objectives of the report are to:

- Specify and further describe the relevant activities in the implementation of the EU CDPF;
- Outline the way ahead for the next six months.

## 2. EXECUTIVE SUMMARY

Several priorities identified in the EU CDPF have already been implemented, and the work is ongoing on key objectives.

The integration of cyber defence and security into CSDP missions and operations will be supported by the extensive revision of the EU Concept on Cyber Defence, also taking into account the need for intensified civil-military cooperation, coordination, as well as broader information sharing.

Several successes can already be highlighted, notably the adoption of a Technical Arrangement between CERT-EU and NCIRC, the ongoing considerations of cyber aspects in operations and missions, as well as first efforts to install a strategic cyber threat assessments for CSDP planning, the ongoing development of several Pooling & Sharing (P&S) projects, the ongoing development of cyber training requirements for CSDP headquarters, missions and operations, and the integration of an effective cyber-dimension to Multi-Layer (ML) and MILEX exercises in 2016. The establishment of an internal EEAS cyber steering board will further mainstream both cyber defence and cyber security aspects in the crisis management structures' daily work.

As the implementation of the EU Cyber Defence Policy Framework moves forward, the Member States' involvement alongside the EU institutions will remain vital in all areas. It remains essential that, as the cyber threats develop, new cyber defence requirements are regularly identified.

## 3. CONTEXT

Since the adoption of the EU Cybersecurity Strategy in February 2013, cyber defence and security have been a priority on the EU CSDP agenda. Over the last decade, cyber has become a critical domain for military and security-related activities and in particular for the success of CSDP implementation through the CSDP structures, missions and operations. Following tasking by the European Council of December 2013, the EU CDPF was adopted in November 2014 by the Foreign Affairs Council. Two progress reports were presented by the European External Action Service (EEAS) in June 2015 and October 2015 and agreed by the Political and Security Committee in July 2015 and November 2015.

The overall context of cyber security and cyber defence continues to evolve rapidly. There is a cyber dimension to many conflicts, and also to hybrid threats and campaigns, for example in Ukraine and in some EU Member States. The threat of cyber-attacks, both by states and non-state actors, is growing. Cyber-attacks could be used as one lever or tool for disruption by perpetrators of hybrid threats and may become part of a well-orchestrated strategy, using multiple tactics simultaneously, aimed at influencing or destabilising an adversary.

Over the last few years, the need for international cooperation to improve transparency and reduce the risk of miscalculation has become clear. Useful first steps have been made by the international community to increase trust and confidence in cyberspace. The UN Group of Governmental Experts (UN GGE) on Developments in the field of Information and Telecommunications in the Context of International Security agreed in its 2013 report that existing international law, notably the UN Charter, applies to cyberspace. It also concluded in June 2015 a new report that was transmitted by the UN Secretary General to the UN General Assembly in August 2015, further clarifying the application of international law to cyberspace, stressing the importance of cooperation between States in safeguarding the functioning of critical infrastructures and Computer Emergency Response Teams (CERTs), and the necessity for States to refrain from using proxies and not knowingly allowing the use of their territories for harmful cyber activities against the critical infrastructure of another country.

At the European Council of December 2013, cyber threats were recognised as a significant new security challenge and the May 2015 CSDP Council Conclusions called for bold action to implement the EU CDPF. A primary focus of the EU CDPF is the development of cyber defence capabilities made available by Member States for the purposes of the Common Security and Defence Policy. Reinforcement of cyber defence and security capability and increasing the resilience of CSDP structures, missions and operations remain critical tasks for the CSDP, as well as being two of the main aims of the EU CDPF.

Cyber security and defence have also been in the focus within the development of the EU Global Strategy. For this purpose, the EU Institute for Strategic Studies (EU ISS) and International Center for Defence Studies organised on 3-4 February 2016 in Tallinn (Estonia) a conference entitled '*Cyber Security Conference - EU Global Strategy for Foreign and Security Policy*'. The conference dealt with issues concerning protecting EU interests in cyber space, EU cyber diplomacy, cyber norms, EU Cyber Security Strategy and digital single market as well as developing EU cyber defence for the CSDP.

Finally, in the context of raising awareness and sharing information on best practice, the PMG received an insightful briefing by the Head of the Cyber Command of the Dutch armed forces during its informal visit to the Netherlands on 4 March.

## 4. PROGRESS TOWARDS THE IMPLEMENTATION OF THE CYBER DEFENCE POLICY FRAMEWORK

### 4.1. Supporting the development of Member States' cyber defence capabilities related to CSDP

On 30 June 2015 the EDA Steering Board in R&T Directors format tasked the EDA to start the negotiations for the establishment of a holistic Cyber Defence Joint Program with interested EDA participating Member States (pMS). Negotiations with pMS are still ongoing and an initial draft for a related Program Arrangement is under preparation. This draft is expected to be discussed in the EDA Cyber Defence Project Team in June 2016.

On the projects that are funded from the EDA Operational budget, the following progress can be reported:

- The "Crypto Landscaping" project is expected to deliver its final results in May 2016. The approach, methodology, work progress and the results so far were presented in order to inform and align MS' expectations during a workshop on 18 February 2016 organised by the EDA. The presentation of the results to MS is planned for June 2016. A follow-on project for the development of a "Business Case for multi-crypto environment" has been contracted in December 2015. The results are expected in late 2016.

- The EDA commissioned and concluded a low-volume "Industrial Analysis for the Prioritised action of Cyber Defence of the Capability Development Plan". The results were presented to pMS by RAND Europe at the November meeting of the Cyber Defence Project Team. Based on the initial results, which only landscaped the Cyber Security/Defence industrial base in 13 EU Member States, the scope of the analysis was expanded to landscape also the remaining ones. The updated final report including the analysis of the overall EU industrial landscape with more than 500 companies engaged in the domain was delivered in March 2016.

Based on the 2014 Capability Development Plan (CDP) revision, which insists on capability development in terms of building a skilled Cyber Defence workforce for the military and ensuring the availability of state-of-the-art proactive and reactive Cyber Defence technology, the EDA three-year planning framework 2016-2018 contains the following cyber defence-related projects for 2016: support for the development of an OHQ/FHQ-level cyber defence pilot-exercise, development of the curriculum for a staff officers course for non-Cyber Defence specialists, development of a Cyber Defence Train-the-Trainer course; development of the Target Architecture & System Requirements for an enhanced Cyber Situational Awareness solution.

The 2016 EDA budget line for Cyber Defence in the EDA three year planning framework is 550,000 euro (including some funding for projects which were already launched in 2015. Within the given funding to above projects a new project was added to develop a “Deployable Cyber Evidence Collection and Evaluation Capacity” with the objective to have a technology demonstrator by end of 2017. Tendering procedures for above activities are in the preparation phase.).

In relation to the *Pooling & Sharing* agenda, several projects continue to develop and new initiatives were launched or are under preparation:

a) Cyber Ranges: The project arrangements (PA) and the Memorandum of Understanding for the usage phase are in final negotiation with the pMS interested to contribute to the project. Although due to unforeseen circumstances, the signature of the PA had to be delayed, it is still envisaged for the first semester of 2016. The realisation phase will start immediately after the signature of the arrangements.

b) Deployable cyber situation awareness packages for Headquarters (CySAP): on the 12 February 2016, EDA Steering Board officially endorsed the Business Case. The military requirements based on the Common Staff Requirement were agreed on the 27 November 2015. The agreed milestones will progress through simultaneous activities comprising: requirements and architecture development by 2016, definition of work package options within a Programme arrangement by 2017.

c) Pooling of Member States demand for private sector training and exercise: the initiative for the "Demand Pooling for the Cyber Defence Training and Exercise support by the private sector” (DePoCyTE) was launched in January 2016 and an exploratory workshop was organised in February 2016. An *ad hoc* working group to develop the necessary documentation for the pre-project phase will be established in April 2016 with the objective to conclude the Project preparation phase by mid-2017.

d) Advanced Persistent Threat Detection (APT-D): during a workshop on 18 February 2016 organised by the EDA in a joint format with the Crypto Landscape Study, Member States discussed options for follow-on activities in the continuation of the Military Multi-agent System for Advanced Persistent Threat Detection (MASFAD II). Member States were invited to opt into an *ad hoc* Cat B collaborative project which will aim to take the APT-D feasibility demonstrator to a higher technology readiness level. More detailed discussions with interested pMS will start in the 2nd quarter 2016.

With regard to certain actions under this work strand, more work still remains to be done, notably on improving the cooperation between military CERTs of the Member States on a voluntary basis to improve the prevention and handling of incidents.

Political agreement with the co-legislators was reached on the Network and Information Security Directive (NIS) in December 2015. The directive will enter into force this summer, and strategic and operational cooperation under the terms of the directive will commence six month later.

The Cyber work strand (Multinational Defensive Cyber Operations; MDCO) of the Multinational Capability Development Campaign (MCDC)[1] is progressing along the agreed campaign plan for 2015-2016. In December 2015 EDA hosted a MDCO workshop in Brussels and in March 2016 EDA, together with AT co-hosted a MDCO Senior Leader Strategic Review Seminar. A MDCO experiment will take place in May at the Austrian Military Academy. It will aim at stress-testing the draft products. For this experiment the design is led by EDA, while EUMS is contributing to the development of the products. The campaign results will be presented to the MCDC Executive Steering Group (ESG) in the fourth quarter of 2016. Once the products have been approved by the ESG, they will be available for CSDP structures, missions and operations, as well as for

1 The Multinational Capability Development Campaign (MCDC) series is a follow-on to the Multinational Experiment (MNE) series initiated by United States Joint Forces Command in 2001. It is designed to develop and introduce new capabilities to enhance the coalition force's operational effectiveness in joint, interagency, multinational, and coalition operations. While it maintains the foundational blocks that made the MNE series successful, MCDC incorporates significant changes in scope, mission, and governance that improve responsiveness, agility, and relevance.

Member States. The first results are already incorporated in the EUMS mainstreaming process, as well as in the current drafting of the EU Concept on Cyber Defence. The planning for the 2017-2018 campaign has started and will most probably also include a cyber defence-related work strand.

### 4.2. Enhancing the protection of CSDP communication networks used by EU entities

The enhancement of EEAS communication networks protection remains a key priority for the implementation of the EU CDPF. The EEAS internal information technology security capacity has reinforced the EEAS' cyber defence and security posture, by improving its capacity in prevention, intrusion detection, incident response and information sharing, without prejudice to the role of CERT-EU. Despite the high priority, serious resource constraints have delayed the delivery of the EU CDPF objectives.

Following the launch of the cyber hygiene initiative and its pledge signed by the HR/VP and other Member States[2] on 18 May 2015, work is ongoing to implement the guidelines related to the mitigation of cyber risks related to end-user behaviour, as well as the e-learning platform developed by Estonia in cooperation with Latvia.

The EU Intelligence and Situation Centre (EU INTCEN) and the Intelligence Directorate of the EUMS are jointly mandated to provide strategic intelligence, inter alia in support of CSDP. This responsibility includes the identification and the analysis of current and new cyber threats targeting the EU. Further, in support of the planning and implementation for each CSDP operation or mission, EU INTCEN and the EUMS Intelligence Directorate provide updated strategic Threat Assessments that include a section on cyber when appropriate. In the process of enhancing strategic cyber threat analysis, cooperation with EU bodies such as CERT-EU and Europol is being strengthened with a view to regularly sharing insights and information.

In the context of CSDP, it should also be noted that the EU INTCEN is currently setting up the EU Hybrid Fusion Cell in order to enable the early identification of hybrid threats affecting the EU's

[2] Estonia, Latvia, Lithuania, Austria, Finland and the Netherlands

strategic activities and interests. Many hybrid threats include a cyber element. The Hybrid Fusion Cell was one of the main initiatives of the recent Joint Communication on countering Hybrid threats. It will provide analysis and early warning to the EEAS, the Commission and Member States.

The cell will shortly have an initial operating capability in June 2016. It will draw on existing expertise within EU INTCEN, as well as developing a better understanding of hybrid threats through consulting a network of national points of contact from Member States as well as CERT-EU.

EUMS continues the process of "mainstreaming" cyber into the EUMS and thereby to operationalise the EU CDPF for future CSDP activities within the EUMS. The intent is to incorporate the consideration of cyber defence aspects into routine processes and procedures, to ensure active engagement and contributions to enhance awareness of all EUMS staff. The revision of the cyber concept, cyber lessons learned and previous work on this topic will provide a good basis. Contents of this process may be beneficial also for other structures within EEAS and EU institutions and agencies, and shall therefore be coordinated with similar approaches within the EEAS.

In order to strengthen the implementation of the objectives of the EU CDPF in relation to the protection of the CSDP communication networks used by EU entities, the EEAS is currently establishing an EEAS cyber steering board, which aims at guiding the response to cyber-attacks in a CFSP/CSDP context and to steer relevant activities of the EEAS directorates in a preventive manner. Moreover, the development of a joint EU diplomatic response ("diplomatic toolbox") in case of large-scale cyber-attacks, should be further discussed.

The Cyber Defence Team of the EU Military Staff is currently rewriting the EU Concept for Cyber Defence in EU-led Military Operations (2012), adapting it to the EU CDPF and broadening the scope to include also civil/military aspects, aiming to provide guidelines and to determine minimum requirements for the development of cyber defence capabilities for military CSDP missions and operations, as well as to define terminology, principles, procedures and responsibilities. The

Concept is therefore targeted at CSDP military structures, missions and operations, as well as EU Members States and third parties, participating in the CSDP missions and operations. The draft is intended to be finalized for approval by the EUMC by September.

Looking forward to the next reporting period and in parallel to the revision of the EU Concept for Cyber Defence in CSDP Military Operations, CMPD will begin the drafting of a concept on integrating cyber security in the planning and execution of civilian CSDP missions. This civilian concept will be drafted in close cooperation with the concept for military operations.

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

Cyber remains a dual-use sector which offers many opportunities to develop synergies. These potential synergies cover several aspects of cyber, from competence profiles to research. The study launched by the Commission on "*Synergies between the civilian and the defence cybersecurity markets*" in which both the EEAS and the EDA were participating, was finalised in February 2016. This study found examples of synergies between civilian and defence cybersecurity markets both on the supplier and the consumer side. It concluded that over the last few years, the majority of the synergies originated from the civilian market and civilian products and services were used at the defence market. The final report of this study is expected to be published in spring 2016.

The Commission has also launched two other cyber-related Framework Programme 7 projects: *PANOPTESEC*, whose third technical review was undertaken in December 2015, and *CyberROAD PANOPTESEC* is expected to conclude its work in October 2016.To explore potential dual-use opportunities, the EDA is a member of the External Advisory Boards of these cyber security projects.

A key objective of the European Defence Action Plan announced by the Commission (2016 work programme) is to examine ways of using Commission programmes to support European military capability priorities as identified by Member States. This could include measures in the cyber area,

as part of the ongoing implementation of the 2013 commitments (EUCO and Defence Communication). This is indeed one of the sectors deemed as critical to maintaining European technological and operational superiority in the next decade and where an EU approach could add value.

EU Structural and Investment Funds (ESIF) for Dual Use Technology: In 2015 EDA within its broader activities to support defence stakeholders to access ESIF for dual-use projects launched a "Request for Projects (RfP) on Dual-Use Technologies to Access European Structural and Investment Funds (ESIF)" aimed at selecting dual-use R&T projects to provide them high-level technical assistance and ultimately submit them to access co-funding from European Structural and Investment Funds (ESIF). Six projects out of more than 30 projects were positively assessed to be further supported.

### 4.4. Improving training, education and exercises opportunities

Education and training: As highlighted in the EU CDPF, several gaps have been identified in the training modules of EEAS, Commission and Member State end-users, in the framework of CSDP implementation.

*Member States' initiatives*

France and Portugal have launched a project as Discipline Leaders, with the support of the EUMS, and building on the existing EDA Training-Needs-Analysis, to identify the CSDP Military Training Requirements for cyber defence. Two workshops were organised in February and March 2016 to set up the framework associated with the development of a Cyber Defence Curriculum. Significant progress is expected by the end of 2016.

In the framework of the Military Erasmus initiative, an "EU module on cyber defence" was conducted as a pilot activity by France in November 2015, with the support of Portugal and Belgium. A second one will be organised in November 2016. Additionally, under the same Initiative a draft curriculum for a new Common Module on cybersecurity and defence has been

developed by the Budapest National University of Public Services. A "Cyber Security Module" will also be integrated in the "International Semester". This proposal will be further discussed in the context of the International Military Academic Forum in June 2016 and then by the Implementation Group to be adopted as ‘Common'.

*CSDP training provided by the EU*

The ESDC network remains the only dedicated civilian-military training provider for CSDP structures, missions and operations at an EU level. The ESDC has continued to conduct cyber awareness courses and mainstreamed cyber defence and security, as a horizontal subject, in several standard courses, including through the ESDC's e-learning platform. Discussions have been taking place on cyber security and cyber defence, both on the Member States' (Steering Committee) and training provider's (Executive Academic Board) level. Very close co-operation mechanisms were established between the ESDC, the EDA and EEAS/SECPOL3. The ESDC organised a meeting to identify further synergies with the European Cybercrime Centre within Europol (EC3), CEPOL, ENISA and other relevant entities regarding the development of common civ-mil training standards and curricula. A new Member of the ESDC Network (Open University of Cyprus) engaged in the creation of ESDC eLearning courses on cybersecurity.

Based on the Cyber Awareness Seminars provided to the OHQ Larissa for EUFOR RCA in 2014, three similar seminars were delivered to the OHQ Rome for EUNAVFOR MED in December 2015. The preparation and delivery of the seminars was supported by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE). The Operation Commander has requested for such training seminars to be followed up at least twice a year along the rotation of the OHQ staff. The suggestion was also made to use EU common funding for such seminars.

*Feasibility study*

The EDA Cyber Defence Project Team concluded in September 2015 a feasibility assessment for the establishment of an EU Cyber Defence Centre/training facility, according to the 2011 tasking from the revised Capability Development Plan (CDP). The assessment was forwarded by the EDA Chief Executive to the relevant Council Working Groups (PMG and EUMC) for further consideration in a wider cyber defence context.

Both the PMG and the EUMC were briefed on the various models and options by the EDA in April and May 2016. The PMG underlined the importance of a step-by-step and needs-based approach in view of enhancing the coherence and availability of policies and structures within the framework of the CDPF. There was an overall preference at this stage to focus on improved coordination of education, training and exercises in the area of EU cyber defence by better using available structures and linking up ongoing initiatives, while also stressing the importance of coordination with and non-duplication of existing structures. The need to integrate civilian missions' aspects and to link to the work on countering hybrid threats was emphasised as well. Whilst focussing on better using existing structures and taking into account relevant work on education and training, reflections should continue on this basis, keeping both PMG and the EUMC involved in the next steps.

The call for tender for an EU-wide "Cyber defence training & exercise, coordination and support platform (financed by the EDA operational budget) was concluded in December 2015. The implementation of the project started in January 2016. The platform is expected to be fully operational in the second semester of 2017. In a letter from its Armaments Director from 19 June 2015 Portugal indicated its interest to host and operate the platform once it will be delivered. The platform will inter alia also serve as the major coordination and management platform for the cyber ranges federation as well as for DePoCyTE.

Negotiations started on the possible establishment of a cooperation roadmap between EDA and ENISA on various subjects such as training and exercises. Negotiations should be finalized in the first of half of 2016.

Exercises: Although developing a dedicated CSDP cyber defence exercise remains a major objective of the EU, at this stage the EEAS lacks the resources to do so. This highlights the need to better streamline cyber defence and security in the existing exercises organised by the Member States.

Based on the lessons learned from the crisis management exercise Multi-layer 14 (ML 14), exercise Multi-layer 16 (ML 16) will tackle cyber threats beyond a simple information security incident. This would aim to raise awareness and understanding of the cyber defence considerations at the civil and military strategic and operational levels during the planning phase of an envisaged mission and operation. This would also help to define the requirements for cyber threat risk management techniques to be included in the EU Crisis Response planning procedures. To this end, a subgroup (syndicate) with the participation of ENISA has been established within the ML16 planning team with the objective to work out a credible and exercisable cyber event.

MILEX 2015 was provided with a comprehensive cyber-narrative to improve the preparedness of CSDP planners on strategic level. In practice, the exercise was primarily used by UK and EL to prepare EU Battlegroups activities, with cyber effects and their possible consequences considered but only playing a minor role. Lessons-learned will be used for the planning of MILEX 2016, where again a comprehensive cyber narrative will be included.

Several pilot exercises are planned to take place in 2016 and 2017 funded by the EDA Operational Budget as a bridging effort. Enduring support for such type of exercises has been introduced in the DePoCyTE initiative (see 4.1.). The EDA 2016 and 2017 budget foresees support for an OHQ level cyber defence pilot exercise. Discussions are currently ongoing with ENISA and NATO CCD CoE to develop such an exercise as a joint effort.

Also in this reporting period, the EU has been invited as an observer in multinational cyber defence exercises such as NATO's *CyberCoalition* 2015, CMX 2016, and has taken this opportunity in order to develop more competences in this domain.

### 4.5. Enhancing cooperation with relevant international partners

Regarding cooperation between CERT-EU and the NATO Computer Incident Response Capability (NCIRC), a Technical Arrangement was agreed in February 2016. The agreement facilitates technical information sharing between NCIRC and CERT-EU to improve cyber incident prevention, detection and response in both organisations, in line with their decision making autonomy and procedures.

The next high level staff-to-staff consultations between the EU and NATO will be held in Autumn 2016. Meanwhile, EUMS maintains informal contacts on working level with NATO's International Military Staff, including a Cyber Defence work strand which aims to raise the mutual understanding of Cyber Defence issues and relevant ongoing work in this area.

Finally, the EU has continuously supported the development of confidence building measures, as well as of norms of behaviour, through the Organisation for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF) and the United Nations Group of Governmental Experts (UN GGE) processes in order to increase transparency and reduce the risk of misperception in State behaviour.

## 5. MANAGEMENT AND GOVERNANCE

Following the presentation of the first two six-month implementation reports of the EU CDPF, the further mainstreaming of cyber issues into the CSDP daily management and decision-making has taken place. Cooperation with the Commission services and the relevant agencies, such as the EDA, the ESDC and ENISA, has been increasingly constructive over the last six months.

The PMG will continue to monitor and provide guidance on the implementation of the policy framework, including regularly in the format reinforced with cyber defence experts.

The EUMC and other relevant Council working bodies, such as the CIVCOM, should be further involved in the implementation of the relevant issues listed in the annex.

## 6. RECOMMENDATIONS

It is recommended that the PSC notes the progress and achievements in the implementation of the EU CDPF and that the intended plan of work for the next months is endorsed, with a view to presenting an updated progress report in October-November 2016.

It is also recommended that the PSC takes note of the EU CDPF management considerations.

| Priorities | Actions | Timeline | Lead/Actors |
|---|---|---|---|
| 1. Supporting the development of Member States cyber defence capabilities related to CSDP | a. 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; | Ongoing | EDA, MS |
| | b. Support current and future cyber defence related Pooling and Sharing projects for military operations (e.g. in forensics, interoperability development, standard setting); | Ongoing | EDA<br>MS |
| | c. 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; | 2016 | EDA,<br>MS, COM (DG CNECT, ENISA) |

| | | | |
|---|---|---|---|
| | d. Improve cooperation between military CERTs of the Member States on a voluntary basis, to improve the prevention and handling of incidents; | 2016-2017 | MS, IntCen, EEAS (BA.IBS) COM (DG CNECT) |
| | e. Facilitate exchanges between Member States on:<br>• national cyber defence doctrines,<br>• training programmes<br>• and exercises<br>• As well as on cyber defence oriented recruitment, retention, and reservists programs; | 2016 | EDA, EEAS (EUMS, SecPol 3), MS; COM |
| | f. Consider developing cyber defence training, in view of EU Battlegroup certification; | 2016 | MS, EEAS (EUMS), ESDC, EDA |
| | g. 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. | Ongoing | MS, ENISA |

| | | | |
|---|---|---|---|
| 2. Enhancing the protection of CSDP communication networks used by EU entities | a. 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.<br>A cooperation strategy with the CERT-EU and existing EU cyber security capabilities shall also be developed or, where available, further enhanced; | 2016 | EEAS (BA.IBS), CERT-EU |
| | b. 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; | 2016 | EEAS (BA.IBS, CMPD, CPCC, EUMS) |

| | | | |
|---|---|---|---|
| | c. Building on existing structures, strengthen cyber threat analysis at strategic (SIAC) and operational levels to:<br>• identify and analyse current and new cyber threats<br>• integrate cyber threat analysis in the production of the regular comprehensive Threat Assessments foreseen ahead of and during CSDP operations and missions (elaborated by SIAC)<br>• continue the production of strategic Intelligence Assessments on cyber-related issues<br>• ensure that the above mentioned Threat and Intelligence Assessments include contributions from CERT-EU drawing on their cyber risk analyses<br>• together with CERT-EU create the capabilities responsible for the elaboration of operational cyber threat analysis aiming at strengthening cyber security and network protection. | Ongoing | IntCen, MS, EUMS (SIAC), CERT-EU |

| | | | |
|---|---|---|---|
| | d. 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; | Ongoing | MS, EEAS (SIAC), CERT-EU |
| | e. Develop and integrate into strategic level planning, a unified cyber defence concept for CSDP military operations and civilian missions; | 2016 | EEAS (CPCC, CMPD, EUMS), MS |
| | f. 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; | 2016 | EEAS |
| | g. 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; | Ongoing | EEAS, MS |

| | | | |
|---|---|---|---|
| 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 | a. Develop common cyber security and defence competence profiles based on international best practices and certification used by EU Institutions, taking also into account private sector certification standards; | 2016 | EEAS, EDA, ENISA |
| | b. 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; | 2016-2017 | EDA, ENISA |
| | c. Develop a working mechanism to exchange best practice on exercises, training and other areas of possible civilian-military synergy; | 2016-2017 | ESDC, EEAS, EDA |
| | d. Leverage existing EU cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyber defence capabilities; | Ongoing | EDA, COM (DG HOME) |

| | | | |
|---|---|---|---|
| | e. Seek synergies in 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; | Ongoing | COM (DG HOME, DG CNECT), EDA |
| | f. 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; | Ongoing | EDA, COM |
| | g. 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; | Ongoing | COM (DG CNECT, DG HOME) |
| | h. Support EU policy coherence to ensure that policy and technical aspects of EU cyber protection remain at the fore front 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.); | 2016-2017 | COM (DG CNECT, GROW, HOME), MS |

| | | | |
|---|---|---|---|
| | i. Contribute to improving the integration of cybersecurity and cyber defence dimensions in the programmes that have a dual-use security and defence dimension, e.g. SESAR. | 2016-2017 | COM, EDA, MS |
| | j. Support synergies with the civilian cybersecurity industrial policy development undertaken at national level by the Member States and at European level by the Commission. | Ongoing | COM, EDA, MS, EEAS |

| | | | |
|---|---|---|---|
| 4. Improve training, education and exercises opportunities | a. 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; | Ongoing | EDA, ESDC, EUMS<br>COM, MS (FR/PT), Private Sector |
| | b. 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; | 2016 | MS, EEAS, EDA, ESDC |
| | c. Based on the EDA feasibility assessment, explore the possibility and rationale of setting up a cyber security/cyber defence training facility for CSDP possibly as an integral part of the ESDC, making use of their training experience and expertise; | End of 2016 | EDA, ESDC, MS, EEAS/SecPol3, EEAS/EUMS |
| | d. Develop further EDA courses to meet the CSDP cyber defence training requirements in cooperation with the ESDC; | Ongoing | EDA (lead) EEAS (EUMS)<br>ESDC |

| | | | |
|---|---|---|---|
| | e. 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. Cyber specific modules in the framework of the Military Erasmus initiative are planned as a pilot activity in November 2015, following the above mentioned mechanisms; | 2015-2016 | ESDC, MS, EEAS |
| | f. Create synergies with the training programmes of other stakeholders such as ENISA, Europol, ECTEG and the European Police College (CEPOL); | 2016-2017 | ENISA, Europol, ECTEG, CEPOL |
| | g. Explore the possibility of joint ESDC-NATO Defence College cyber defence training programmes, open to all EU Member States, in order to foster a shared cyber defence culture; | 2016 | ESDC, EEAS |
| | h. Engage with European private sector training providers, as well as academic institutions, to raise the cyber competencies and skills of personnel engaged in CSDP operations and missions. | 2015-2017 | EDA, EEAS, ESDC |
| | i. Integrate a cyber defence dimension into existing exercise scenarios' for MILEX and MULTILAYER; | 2015-2016 | EEAS (CMPD, EUMS, CPCC, CSDP.1), MS (PMG) |

| | | | |
|---|---|---|---|
| | j. 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; | 2016-2017 | EEAS (CMPD, EUMS, CPCC, CSDP.1), ENISA |
| | k. Consider participating in other multinational cyber defence exercises; | Ongoing | EEAS (EUMS, CSDP.1), MS |
| | l. 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. | Non applicable | EEAS (SecPol3, CMPD, EUMS, CPCC |
| 5. Enhancing cooperation with relevant international partners | a. Exchange of best practice in crisis management as well as military operations and civilian missions; | Ongoing | EEAS (EUMS, CMPD, CPCC) |
| | b. Work on coherence in the development of cyber defence capability requirements where they overlap, especially in long-term cyber defence capability development; | Ongoing | MS, EDA, EEAS (EUMS, CMPD) |
| | c. Enhance cooperation on concepts for cyber defence training and education as well as exercises; | Ongoing | EEAS (CMPD, EUMS), ESDC, EDA |

| | | | |
|---|---|---|---|
| | d. Further utilise the EDA liaison agreement with NATO's Cooperative Cyber Defence Centre of Excellence as an initial platform for enhanced collaboration in multinational cyber defence projects, based on appropriate assessments; | 2016 | EDA, EEAS |
| | e. Reinforce cooperation between the CERT-EU and relevant EU cyber defence bodies and the NCIRC (NATO Cyber Incident Response Capability) to improve situational awareness, information sharing, early warning mechanisms and anticipate threats that could affect both organisations. | 2016 (conclusion of the Technical Arrangement between CERT-EU and NCIRC in February 2016) | CERT-EU, EEAS, MS |
| | f. Follow strategic developments and hold consultations on cyber defence issues with international partners (international organisations and third countries); | Ongoing | EEAS (CMPD), MS |
| | g. Explore possibilities for cooperation on cyber defence issues, including with third countries participating in CSDP missions and operations; | 2016-2017 | EEAS (CMPD), MS |

| | | | |
|---|---|---|---|
| | h. 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. | Ongoing | EEAS, MS |