Council of the European Union

Brussels, 10 November 2015
(OR. en)

13801/15

LIMITE

COPS 340
POLMIL 97
EUMC 41
CYBER 107
RELEX 895
JAI 833
TELECOM 205
CSC 262
CIS 13
COSI 136

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

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (11.05.2016)

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 9 November 2015.

ANNEX

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. EU Concept For Cyber Defence for EU-led Military Operations

H. 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 May 2015 – 15 October 2015. 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

As set out in the EU CDPF, the development of cyber defence and security capabilities and technologies should address all aspects of capability development, taking into account the responsibilities of all relevant actors. Several actions have already been taken, and the work is ongoing. Ensuring the Member States' involvement alongside the EU institutions and defining their roles in the implementation process is vital. It remains essential that, as the cyber threats develop, new cyber defence requirements are identified, and then included in the EU CDPF. During this reporting period, the EEAS, the Commission, notably DG CNECT and DG HOME, CERT-EU, the EDA and the European Network and Information Security Agency (ENISA) have increased their cooperation in order to deliver the implementation of the EU CDPF. The establishment of an internal EEAS cyber governance structure is being considered in order to mainstream both cyber defence and cyber security aspects in the crisis management structures daily work. The integration of cyber defence and security into the EU-led missions and operations still needs to be improved further.

Several successes can already be highlighted, notably the ongoing mainstreaming of cyber aspects into strategic CSDP threat assessments, 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 addition of a cyber-dimension to Multi-Layer (ML) and MILEX exercises.

The process has started to improve the mainstreaming of cyber into the planning for CSDP missions and operations, notably in operations EUFOR RCA and EUNAVFOR MED. The EU Military Staff is reviewing the EU Concept for Cyber Defence in EU-led Military Operations and adapting it to the EU CDPF. Looking to the future, the development of an EU concept for cyber defence in both CSDP missions and operations will maximise the synergies between the civil and military CSDP planning approaches to cyber defence. The EDA concluded a two-year foundational project to define elements for the integration of cyber defence into CSDP, notably in training needs analysis. The results of this analysis could be taken into account by the ESDC when developing its standard curricula.

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, the cyber domain has become a critical asset 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. A first progress report was presented by the European External Action Service (EEAS) in June 2015 and agreed by the Political and Security Committee in July 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. The threat of cyber-attacks, both by states and non-state actors, is growing. 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 and the Law of Armed Conflict, 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.

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 Investment Program (JIP) with interested EDA participating Member States (pMS). This program will primarily focus on R&T aspects of cyber defence. The EDA has planned a series of workshops in which pMS' experts will be invited to contribute to the different aspects of the Program Arrangements (PA) – general, administrative, legal, financial and technical. The first of these workshops took place on 21 October 2015 at the Belgian Royal Military Academy premises in Brussels. The scoping and establishment of the JIP will be supported with funding from the EDA Operational Budget (see below).

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

- The "Crypto Landscaping" project is intended to deliver its final results in the first quarter of 2016. A follow-on project for the development of a "Business Case for multi-crypto environment" is currently under preparation. The call for tenders for this project was launched at the end of October 2015.

- The final results of the "Multi-Agent System for Advanced Persistent Threat Detection (MASFAD)" project were delivered in September 2015 with a "Proof-of-Concept" prototype. The final results will be presented to pMS during the November 2015 meeting of the Project Team. The EDA will then propose to launch a follow-on *ad hoc* project together with the interested EDA pMS in order to further develop the prototype results into a full operational capability.

- The EDA commissioned and concluded a low-volume "Industrial Analysis for the Prioritised action of Cyber Defence of the Capability Development Plan (15.CPS.SC.028)". The results will be presented to pMS by RAND Europe at the November meeting of the Project Team Cyber Defence.

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 has proposed to pMS to provide *inter alia* funding in the EDA three-year planning framework for 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 for a Cyber Situational Awareness solution for HQs (see also CySAP); and Consultancy support for the scoping and the establishment of the Cyber Defence JIP.

After initial negotiations with pMS about the 2016 EDA budget line, the requested funding for 2016 cyber defence-related projects represents a volume of 555,000 euro (including some funding for projects which were already launched in 2015).

In relation to the *Pooling & Sharing* agenda, several projects continue to develop:

a) Cyber Ranges: The EDA Steering Board endorsed the Common Staff Requirement in June 2015. The project arrangements are currently under negotiation with the pMS interested to contribute to the project. The signature of the arrangements is envisaged for March 2016. The realisation phase will start immediately after the signature of the arrangements in the first quarter of 2016.

b) Deployable cyber situation awareness packages for Headquarters (CySAP): The finalisation of the preparation phase of this *ad hoc* project has been slightly delayed. The endorsement of the Common Staff Requirement by the EDA Steering Board is envisaged for the end of October 2015. The start of the realisation phase remains planned for 2016.

c) Pooling of Member States demand for private sector training: The preparation of the initiative by the EDA is being finalised. This initiative will be integrated in the negotiations on the Cyber Defence JIP.

The Executive Steering Group (ESG) of the Multinational Capability Development Campaign (MCDC)[1] agreed the campaign plan for 2015-2016, including the cyber defence work strands, which are US-led and which will focus on the integration of defensive cyber operations in the planning of multinational military operations. The final results of the workshops will be presented to the MCDC 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 and Member States.

The EU Military Staff is currently preparing the review of the EU Concept for Cyber Defence in EU-led Military Operations and adapting it to the EU CDPF, aiming to provide guidelines to EU Member States for the development of military capability requirements for their own use but especially for CSDP-related operations. This work shall be finalised by the third quarter of 2016.

Building on the revised EU Concept for Cyber Defence in CSDP Military Operations, a process will be started on preparing an overarching policy paper or concept for both civilian and military missions and operations.

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, as outlined in the Annex.

4.2. **DELETED**

[1] **DELETED**.

DELETED

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 opportunities to develop many synergies. These potential synergies cover several aspects of cyber, from competence profiles to research. Several projects were launched in 2014 and 2015. The Commission has launched a study into the "*Synergies between the civilian and the defence cybersecurity markets*" in which both the EEAS and the EDA are participating. The draft interim report of the project was delivered on 19 October 2015, followed by an inception report discussion on 27 October 2015. Moreover, a workshop on the project will be organised on 1 December 2015.

The Commission has also launched two other cyber-related Framework Programme 7 projects: *PANOPTESEC* (http://www.panoptesec.eu/), whose third technical review is scheduled for mid-December 2015, and *CyberROAD* (http://www.cyberroad-project.eu/). To explore potential dual-use opportunities, the EDA is a member of the External Advisory Boards of these cyber security projects.

The Preparatory Action for CSDP-related research is under preparation by the Commission in cooperation with the EDA and the EEAS. The Consultations are ongoing in order to define the governing model, as well as modalities and priorities for the Preparatory Action. Many Member States have already highlighted that cyber defence should be considered as one of the main priorities of the Preparatory Action.

With regard to certain actions under this work strand, more work still remains to be done, notably on improving the integration of cyber security and cyber defence dimensions in the programmes that have a dual-use security and defence dimension, such as Galileo.

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 Estonia and the EUMS, and building on the existing EDA Training-Needs-Analysis, to identify the CSDP Military Training Requirements for cyber defence. The next stage of this work is scheduled for December 2015 with significant progress expected by the end of 2016.

In the framework of the Military Erasmus initiative, an "EU module on cyber defence" will be conducted as a pilot activity by France in November 2015, with the support of Portugal and Belgium.

CSDP training provided by the EU

The ESDC network is 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. Moreover, the ESDC will organise a meeting to identify further synergies with the European Cybercrime Centre within Europol (EC3) and ENISA and other relevant entities regarding the development of common civ-mil training standards and curricula.

Several pilot courses have also been developed with the support of the EDA. In May 2014 the EDA, together with Estonia and Portugal, organised a pilot course on "*Comprehensive Strategic Cyber Decision Making*", with a table-top exercise for Portugal. This exercise was also observed by several Member States and NATO. Two more exercises were organised with the support of the Czech Republic and Austria as a "proof-of-concept" in June and September 2015.

Based on the Cyber Awareness Seminars provided to the OHQ Larissa for EUFOR RCA in 2014, three similar seminars are scheduled to be delivered to the OHQ Rome for EUNAVFOR MED in December 2015. Preparations for these seminars are ongoing with support of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE).

The EDA Project Team Cyber Defence concluded in September 2015 the assessment of the feasibility for the establishment of an EU Cyber Defence Centre/training facility according to the tasking from the revised Capability Development Plan (CDP). The outcome of this assessment will be addressed by EDA Steering Board in order to provide further guidance to the Agency on the way ahead.

The call for tender for an EU-wide "Cyber defence training & exercise, coordination and support platform (financed by the EDA operational budget) has been published in the Open Journal on 13 October 2015. The project will be implemented from the first quarter of 2016 until the second quarter of 2017. In a letter from its Armaments Director from 19 June 2015 Portugal indicated its interest to operate the platform once it will be delivered.

Exercises: Based on the PMG lessons learned from the crisis management exercise Multi-layer 14 (ML 14), exercise Multi-layer 16 (ML 16) should 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.

The MILEX 2015 scenario has benefited from early inclusion of a cyber-narrative. During the Operational Headquarters planning cycle, non-technical cyber effects and their possible consequences will be considered. Lessons-learned will be used for the planning of MILEX 2016, where again a comprehensive cyber narrative will be included to further improve the preparedness of CSDP planners.

The EDA supported by the Estonian Ministry of Defence and ENISA, and in cooperation with the Czech and Austrian governments, has delivered two Comprehensive Cyber Strategic Decision Making exercises in Prague and Vienna in June and September 2015. Whilst it is intended that ongoing support for such type of exercises will be delivered in the future via an *ad hoc* project under the Cyber Defence JIP, a framework contract will not be in force before 2017. In order to keep the momentum on the initiative, the funding of three additional bridging exercises in 2016 is currently under scrutiny.

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 existing exercises organised by the Member States. However, EU representatives have been invited as observers in other multinational cyber defence exercises such as NATO's *CyberCoalition* 2014 and *Locked Shields* 2015 (held by the NATO CCD COE in Tallinn) in order to develop their competences in that domain.

4.5. **DELETED**

5. Management and governance

DELETED

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 April 2016.

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

Priorities	Actions	Deadline	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;	2015 (and will continue afterwards)	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);	2015 (and will continue afterwards)	EDA 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, 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: • national cyber defence doctrines, • training programmes • and exercises • 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.	2015-2016	EEAS (BA.IBS), CERT-EU

	A cooperation strategy with the CERT-EU and existing EU cyber security capabilities shall also be developed or, where available, further enhanced;		
	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;	2015-2016	EEAS (BA.IBS, CMPD, CPCC, EUMS)
	c. Building on existing structures, strengthen cyber threat analysis at strategic (SIAC) and operational levels to: • identify and analyse current and new cyber threats • 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) • continue the production of strategic Intelligence Assessments on cyber-related issues • ensure that the above mentioned	Ongoing	IntCen, MS, EUMS (SIAC), CERT-EU

	Threat and Intelligence Assessments include contributions from CERT-EU drawing on their cyber risk analyses • together with CERT-EU create the capabilities responsible for the elaboration of operational cyber threat analysis aiming at strengthening cyber security and network protection.		
	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;	2015-2016	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	2015	EEAS

	experiences;		
	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;	2015-2016	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	EDA, ENISA
	c. Develop a working mechanism to exchange best practice on exercises, training and other areas of possible civilian-military synergy;	2015-2016	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	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 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 2015	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) ESDC
	e. Follow the established ESDC certification mechanisms for the training programmes in close cooperation with the relevant services	2015-2016	ESDC, MS, EEAS

	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;		
	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, CROC), MS (PMG)
	j. Develop, as appropriate, a dedicated	2016-2017	EEAS (CMPD,

	EU CSDP cyber defence exercise and explore possible coordination with pan-European cyber exercises such as *CyberEurope*, organised by ENISA;		EUMS, CPCC, CROC), ENISA
	k. Consider participating in other multinational cyber defence exercises;	Ongoing	EEAS (EUMS, CROC), 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	2016	EDA, EEAS

	defence projects, based on appropriate assessments;		
	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.	2015	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