Council of the European Union

Brussels, 26 June 2015
(OR. en)

10347/15

LIMITE

COPS 197
POLMIL 68
EUMC 25
CYBER 62
RELEX 522
JAI 509
TELECOM 154
CSC 160
CIS 9
COSI 85

NOTE

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

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (18.09.2015)

Delegations will find attached the Six-Month report on the Implementation of the Cyber Defence Policy Framework, as finalised by the Politico-Military Group on 26 June 2015.

Six-Month 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. EU Concept For Cyber Defence for EU-led Military Operations
G. Cyber Defence Capability Requirements Statement

1. Purpose

Aim: This document provides an overview of the state of play of the implementation of the EU Cyber Defence Policy Framework (CDPF) over the period of 15 December 2014 – 15 May 2015,

Objectives: The objectives of the report are to:

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

2. Context

Since the adoption of the EU Cybersecurity Strategy in February 2013, cyber defence has 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 more particularly 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.

However, the context has also been rapidly evolving. Cyber capabilities are now part of many conflicts, for example Ukraine in the context of hybrid warfare, or with the cyber attacks on TV5, Le Monde, Le Soir and other media. The risk of cyber-attacks, both by states and non-state actors, is growing. The need for international cooperation to improve transparency and reduce the risk of miscalculation has become clearer during the last few years. Useful first steps have been made by the international community to increase trust and confidence in cyberspace. The 2013 report of the UN Group of Governmental Experts agreed that existing international law, notably the UN Charter and the Law of Armed Conflict/International Humanitarian Law, applies to cyberspace. More effort should be made to reach a common understanding of how norms and rules should apply in cyberspace. Encouraging international discussion on the adoption of norms and principles for responsible behaviour in cyberspace and confidence-building measures will certainly contribute to a more stable cyberspace.

In the framework of the European Council of December 2013, cyber threats are recognised as a significant emerging threat and the (May 2015) FAC Conclusions called for bold action to implement the CDPF. A primary focus of the CDPF is the development of cyber defence capabilities made available by Member States for the purposes of the Common Security and Defence Policy. A key task for the CSDP thus remains the reinforcement of cyber defence capabilities and to increase the resilience of CSDP structures, missions and operations, which remain two of the main aims of the CDPF.

The EEAS, together with the Commission and the EDA, remain strongly committed to supporting the development of robust and resilient cyber defence capabilities, linked to CSDP structures, missions and operations.

3. Executive Summary

As laid out in the CDPF, the development of cyber defence 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 will continue. Ensuring the Member States' involvement alongside the EU institutions and defining their roles in the implementation process remains vital. It remains essential that, as the cyber threat develops, new cyber defence requirements are identified, and then included in the CDPF. During this reporting period, the EEAS, the Commission, notably DG CNECT, DG HOME, the CERT-EU, the EDA and ENISA have increased their cooperation in order to deliver the implementation of the CDPF. The procedure for constructing and promulgating a common understanding of the cyber defence implications for CSDP planning has been refined. Cyber awareness has been pursued among relevant services (Directorate K, Crisis Management and Planning Directorate, Civilian Planning and Conduct Capability, EU Intelligence Analysis Centre, EU Military Staff, EDA and the Commission) and some pilot training sessions have been delivered to personnel serving in selected CSDP operations. The integration of cyber defence into the EU-led missions and operations will be further improved by the CMPD and the CPCC.

Several successes can already be highlighted, notably the ongoing mainstreaming of cyber aspects into strategic CSDP threat assessments, the 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. This work is ongoing in specific CSDP cyber defence training modules. The enhancing of the cooperation between the CERT-EU (Computer Emergency Response Team for the EU institutions) and the NCIRC (NATO Computer incident response capability) has already begun. The EU has also expressed its continued support for global cyber norms discussions.

The process has started to improve the mainstreaming of cyber aspects into the planning for CSDP missions and operations. The EU Military Staff is reviewing the EU Concept for Cyber Defence in EU-led Military Operations. Looking to the future, the development of an EU concept for cyber defence in 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.

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

The resilience of networks supporting CSDP structures, missions and operations remains a key priority. In order to support the convergence between the capability developments planning of the Member States, the Capability Development Plan (CDP) 2015 has been revised by the EDA Steering Board in Ministerial Format in November 2014 and cyber defence remains one of twelve priority actions regarding capability shortfalls to be addressed through cooperation.

Cyber Defence has been added to the Collaboration Database (CoDaBa) and is fully integrated in the new CDP-tool by the EDA as a way for the Member States to inform each other about cooperative cyber training opportunities.

In relation to the *Pooling & Sharing* projects, several projects have started so far:

a) Cyber Ranges: 10 Member States (AT, CZ, EE, EL, ES, FI, IE, LT, LV, NL) are currently participating in the Cyber Ranges P&S project. The preparation phase is being finalised and the EDA Steering Board will endorse the Common Staff Requirement, by the end of July 2015. The project arrangements will then be negotiated and the Leading Nations will be identified. The realisation phase will start during the first semester of 2016.

b) Deployable cyber situation awareness packages for Headquarters (CySAP): 4 Member States (DE, EL, ES, IT) are currently participating in the CySAP project. The preparation phase is being finalised and the EDA Steering Board will endorse the Common Staff Requirement, by the end of July 2015. The project arrangements will then be negotiated and the Leading Nations will be identified. The realisation phase will start in 2016.

c) Multi-Agent System for Advanced Persistent Threat detection (MASFAD): the results of this project will be delivered by September 2015 with a "Proof-of-Concept" prototype. The EDA then propose to launch a follow-on *ad hoc* project together with the Member States in order to further develop the prototype results into a full operational capability.

d) Pooling of Member States demand for private sector training: Based on the results of the Pilot Course for "Digital Forensics" of April 2014, the EDA will launch, during the 2nd semester of 2015, an initiative to establish an *ad hoc* project to develop a streamlined provision of training courses, provided by the private sector cyber security and cyber defence institutions, through the pooling of Member States demands.

In March 2013, the EUMS and the EDA joined the cyber defence workstrands of the Multinational Capability Development Campaign (MCDC). Through the participation of the EU in the MCDC 2013-2014 Campaign, supporting documents, such as a *Handbook and Guidelines for integrating cyber into operational planning* and a *Guide and Specifications for the analysis of the cyber domain,* for cyber defence planning for CSDP have been made available for supporting the planning of operations both in CSDP and national frameworks. The EUMS and EDA will participate in the current MCDC multinational cyber defence work strand to further develop their doctrine for including cyber in conduct of operations.

To facilitate exchanges between Member States regarding their national doctrines, training, exercises etc., several actions have been taken, including the organisation of the mini-away day on cyber of the EU Military Committee (EUMC). The conclusions from the mini-away day reinforced the importance of work that has already started among the EUMS following the adoption of the CDPF. After the away day a social media guide for military assigned to CSDP Operations and Missions was agreed and circulated to all military personnel serving in CSDP Missions and Operations.

With regard to certain actions under this work strand, more work still remains to be done (e.g. 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), as outlined in the Annex.

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

During the last six months, the EEAS, with the support of the Commission and the EDA, has improved the coordination and the synergies among the different EU actors and agencies in the implementation of the CDPF.

Cyber remains a dual-use sector from which many synergies can be developed. 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. In addition, in May 2015, the EDA has launched a study entitled: "*The Analysis of the EU industrial market for the prioritized action of Cyber Defence in the CDP*".

The Commission has also launched two other cyber-related Framework Programme 7 projects: *PANOPTESEC* (http://www.panoptesec.eu/) and *CyberROAD* (http://www.cyberroad-project.eu/) in addition to some others like CAMINO http://www.fp7-camino.eu/ and COURAGE https://www.courage-project.eu/. To explore potential dual-use opportunities, the EDA has also joined the External Advisory Boards of these cyber security projects.

On 28 April 2015, the Commission adopted the European Agenda for Security for the period 2015-2020. This establishes a shared agenda for all relevant EU and national actors with the goal of improving cooperation to address cross-border security threats. Cybercrime is a key priority in the strategy and further links will be sought between Justice and Home Affairs and CSDP. Synergies are likely to arise and should be exploited *inter alia* in the support of security-related actions through training, funding and the promotion of security research and innovation.

On 6 May 2015, the Commission adopted the EU's Digital Single Market Strategy, which proposes the establishment of a contractual public private partnership on cybersecurity in the first half of 2016. This is expected to stimulate the competitiveness and innovation capacities of the European industry in the area of technologies and solutions for online network security. This initiative should help in structuring and coordinating digital security industrial resources in Europe, ensuring that there will be a sustained supply of innovative cybersecurity products and services. Cybersecurity standardisation is another important element fostering resilience in digital infrastructures and is also addressed in the Digital Single Market Strategy.

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. The call for projects should begin in 2016.

The Commission is also working in cooperation with the EDA and Member States on the preparation of the 2016-2017 work programme of the "Secure societies" societal challenge of Horizon 2020. This will make substantial funding available to support Research and Innovation activities in this area. This is expected to provide a framework for addressing the interaction between cybercrime, terrorist use of the internet and cyber defence. It will also put a special focus on digital security to ensure cybersecurity, trust and privacy in the Digital Single Market.

4.4. Improving training, education and exercises opportunities

Education and training: As highlighted in the 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

FR and PT have launched a project as Lead Nations, with the support of EE 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 July 2015 with significant progress expected by 2016.

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

In parallel, during the Spring of 2015 EE introduced the concept of a Cyber Olympics in the EDA Cyber Defence Project Team to other Member States. The concept is currently under evaluation in view of national application of other Member States.

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. It plays a pivotal role in providing the institutional framework for curricula development on cyber security, including cyber defence. So far, the ESDC has conducted six cyber awareness courses since the academic year 2010-2011. The mainstreaming of a cyber defence, as an horizontal subject, is foreseen in several standard courses and more courses dedicated to cyber defence, including through the ESDC's e-learning platform, are planned for the coming academic years. Cyber security will also be included as one of the potential topics for an essay during the bi-annual CSDP Olympiad.

The EU still lacks legal training in relation to cyber defence in its operations and missions. Therefore, possibilities for further cooperation have been discussed between the ESDC and the Cooperative Cyber Defence Centre of Excellence located (CCD CoE) in Tallinn.

Several pilot courses have also been developed with the support of the EDA. A senior decision maker course on operational planning aspects took place in September 2014 in Brussels. The curriculum was finalised together with the ESDC and is expected to be adopted in the 2015 ESDC course programme.

In May 2014 the EDA, together with EE and PT, organised a pilot course on "*Comprehensive Strategic Cyber Decision Making"*, with a table-top exercise for PT. This exercise was also observed by several Member States and NATO. Two more exercises will be organised with the support of CZ and AT as a "proof-of-concept" in June and September 2015.

With the support from CCD CoE, with which the EDA has a liaison, the EDA has completed 3 cyber-awareness seminars for the CSDP Operation Headquarters in Larissa, in the framework of the EUFOR RCA. The curriculum is ready to be replicated for other operations as required.

The EDA will present the results of a feasibility study to the EDA Cyber Defence Project Team on the possibility of setting up a CSDP cyber defence training facility during the second semester of 2015.

As mentioned above, a P&S project is being set up by the EDA to facilitate training by the private sector.

Further synergies will be sought with the European Cybercrime Centre within Europol (EC3) and ENISA regarding the development of common civ-mil training standards and curricula. The European Cybercrime Training and Education Group (ECTEG), funded by the Internal Security Fund and composed of participants from EU Member States and candidate countries law enforcement agencies, international bodies, academia and private industry, has developed training material for law enforcement agencies in Europe and is ready to exchange best practice with CSDP community.

Exercises: Based on the PMG lessons learned, exercise ML 16 should tackle cyber threats beyond a simple information security incident. This will 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. It will 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 also benefited from early inclusion of a cyber narrative. The aim during 2015 will be to achieve consideration of the cyber dimension during strategic planning, rather than as a more tactical level issue, and to generate lessons-learned to improve the preparedness of EU CSDP planners.

Although it remains a major objective of the EU, at this stage the EEAS lacks the resources to develop a dedicated cyber defence exercise. This highlights the need to better streamline cyber defence 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 CCD COE in Tallinn) in order to develop their competences in that domain.

DELETED

5. Management and governance

DELETED

6. Recommendations

It is recommended that the PSC notes the progress and achievements in the implementation of the CDPF and that the intended plan of work for the next 6 months is endorsed, with a view to presenting an updated progress report before the FAC in November 2015.

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

ANNEX

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	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);	Cyber Ranges Common Staff requirement (CSR) presented at the end of the 1st semester 2015 Cyber Situational Awareness packages presented at the end of the 1st semester 2015	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	2016	EDA, MS, COM (DG CNECT, ENISA)

	experience;		
	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 (PMG), IntCen, EEAS (MDR) 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, K3), 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. A cooperation strategy with the CERT-EU and existing EU cyber security	2015-2016	EEAS (MDR), CERT-EU

	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 (MDR, 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 Threat and Intelligence Assessments include contributions from CERT-EU drawing on their cyber risk	Ongoing	IntCen, MS, EUMS (SIAC)

	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;	2015/2016	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;	2015	EEAS
	g. Review regularly resource requirements and other relevant policy decisions based on the changing threat environment, in consultation with the	Ongoing	EEAS, MS

	relevant Council working groups and other EU institutions;		
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 practises 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	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;	2015	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;	2015	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.	Ongoing	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.	To be determined	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;	2015-2016	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/K3, 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 in the EU institutions, based on existing standards and knowledge.	2016	ESDC, MS, EEAS

	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 EU CSDP cyber defence exercise and explore possible coordination with pan-European cyber exercises such as *CyberEurope*, organised by ENISA;	2016	EEAS (CMPD, EUMS, CPCC, CROC),

			ENISA
	k. Consider participating in other multinational cyber defence exercises;	2015	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 (K3, 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;	To be determined	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;	To be determined	MS, EDA, EEAS (EUMS, CMPD)
	c. Enhance cooperation on concepts for cyber defence training and education as well as exercises;	To be determined	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	2015	CERT-EU,

	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.		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.	Negotiations in 2015 of a 2nd set of CBMs; UN GGE report to be expected in June 2015	EEAS, MS