Council of the European Union

Brussels, 19 December 2017
(OR. en)

15870/17

LIMITE

COPS 404
POLMIL 169
EUMC 158
CYBER 221
RELEX 1130
JAI 1218
TELECOM 370
CSC 304
CIS 13
COSI 342

NOTE

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

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (06.03.2018)

Delegations will find attached the Annual Report on the Implementation of the Cyber Defence Policy Framework, as agreed by the Politico-Military Group on 19 December 2017.

ANNEX

ANNUAL REPORT ON THE IMPLEMENTATION OF THE

CYBER DEFENCE POLICY FRAMEWORK

REFERENCE DOCUMENTS

A. European Council conclusions (19 December 2013, EUCO 217/13)

B. Council conclusions on Common Security and Defence Policy (18 November 2014, 15532/2/14 REV 2)

C. EU Cyber Defence Policy Framework (18 November 2014, 15585/14)

D. EU Cybersecurity Strategy 2013 (7 February 2013, JOIN(2013) 1 final)

E. Council conclusions on CSDP (18 May 2015, 8971/15)

F. First report on the implementation of the Cyber Defence Policy Framework (26 June 2015, 10347/15)

G. Second report on the implementation of the Cyber Defence Policy Framework (10 November 2015, 13801/15)

H. Third report on the implementation of the Cyber Defence Policy Framework (1 June 2016, 9701/16)

I. Fourth report on the implementation of the Cyber Defence Policy Framework (25 November 2016, 14904/16)

J. EU Concept For Cyber Defence for EU-led Military Operations (22 November 2016, EEAS(2016) 1597)

K. Integrating cyber security in the planning and conduct of civilian CSDP missions (12 June 2017, EEAS(2017) 773)

L. Cyber Defence Capability Requirements Statement (March 2013)

M. Technical Arrangement between CERT-EU and the NATO Computer Incident Response Capability (February 2016)

N. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary general of the North Atlantic Treaty Organization (8 July 2016)

O. Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization (6 December 2016, 15283/16; 5 December 2017, 14802/17)

P. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox", 7 June 2017, 9916/17)

Q. Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (13 September 2017, JOIN(2017) 450 final)

R. Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (9 October 2017, 13007/17)

S. Council Conclusions on security and defence in the context of the EU Global Strategy (13 November 2017, 14190/17)

T. Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017, 14435/17)

1. Purpose

This document provides an overview of the implementation of the EU Cyber Defence Policy Framework (CDPF) for the period November 2016 - December 2017. The objectives of the report are to specify and further describe the relevant activities in the implementation of the EU CDPF, as well as outline the way ahead.

2. Executive Summary

In September 2017, the EU complemented its 2013 cybersecurity strategy, through a Joint Communication on building strong cybersecurity for the EU. The Council Conclusions related to this Joint Communication recognized the need for a renewed emphasis on the implementation of the 2014 EU Cyber Defence Policy Framework and to update it to further integrate cyber security and defence into Common Security and Defence Policy (CSDP) and to the wider security and defence agenda. Furthermore, it stressed the need to step up cooperation on cyber defence and to take full advantage of the proposed defence initiatives to accelerate the development of adequate cyber capabilities in Europe.

This report presents the objectives that have already been implemented, as well as the numerous priorities that require a renewed emphasis and ongoing engagement and cooperation by all.

The revised EU Concept for Cyber Defence in EU-led Military Operations and Missions was adopted on the 22 November 2016, and has been followed by the ongoing development of Cyber Defence Standard Operating Procedures.

The concept for integrating cyber security in the planning and conduct of civilian CSDP missions was also finalized in June 2017.

With the aim of supporting the development of Member States cyber defence capabilities, several projects are progressing under the EDA. For instance, the project arrangements for cyber ranges, which will put in place a cooperative mechanism to enable national cyber defence exercise and training facilities to coordinate efforts, were signed by the 11 contributing members and the project formally commenced the implementation phase in July 2017.

As a follow-up to the technical arrangement signed between the CERT-EU and NCIRC early 2016, the respective platforms on malware information sharing are now interconnected, allowing CERT-EU and NCIRC to share information on cyber-attacks in real time.

In November 2016, the importance to have a governance mechanism for cyber security policy at the EEAS/CSDP level was stressed by the PMG. An internal EEAS Cyber Governance Board, chaired by the EEAS Secretary General, is now in place, and met for the first time in June 2017.

Other successes of the CDPF, also highlighted in previous reports, include the implementation of a Technical Arrangement between CERT-EU and NCIRC, the current mainstreaming of cyber aspects in CSDP operations and missions, as well as first efforts to install a strategic cyber threat assessments for CSDP planning, the current development of several Pooling & Sharing (P&S) projects, and the development of cyber training requirements under way for headquarters of CSDP missions and operations.

In the third quarter of 2017, several exercises with a strong cyber defence dimension took place. In September, the Estonian Presidency organised, in close cooperation with the European Defence Agency and other EU stakeholders, a table top ministerial level cyber exercise EU CYBRID 2017, where the EU ministers of defence had an opportunity to test the EU crisis management procedures during a crisis with substantial cyber-attacks. The EU PACE2017 and NATO CMX-17 exercises also had many cyber aspects included to the exercise scenario, which provided an opportunity to test the decision-making in the EU and NATO during the crisis with multiple elements, including serious cyber-attacks. MILEX17, the annual military operational planning exercise was also conducted in November 2017 using the UK EU OHQ and an ES FHQ.

As the implementation of the EU Cyber Defence Policy Framework moves forward, the Member States' involvement alongside the EU institutions remains vital in all areas. Growing cyber threat calls for the regular identification of new cyber defence requirements.

3. Context

The cyber threat landscape has changed drastically since the adoption of the Cyber Defence Policy Framework in 2014. Cybercrime business models have evolved and new threats related to Internet-of-Things are emerging. The changed geopolitical environment has also affected the way we perceive cyber threats and, across the EU, we are now looking at cyber threats at a more strategic level to protect the well-being of our democracies, societies and economies.

A Joint Communication was presented by the Commission and the HR/VP in September 2017 to mitigate risks stemming from the new threat landscape. It also includes cyber defence as one of the main areas of action, and the CDPF is one of the pillars of its concrete implementation.

The EU CDPF was adopted in November 2014 by the Foreign Affairs Council, following the tasking by the European Council of December 2013. The same European Council also welcomed Cyber as one out of four key capability programmes of EDA.

Four progress reports have been presented by the European External Action Service (EEAS) to the Political and Security Committee in 2015 and 2016. This document embodies the fifth written progress report. An interim oral update on the implementation of the Cyber Defence Policy Framework was provided to the PMG in May 2017.

Over the last few years, the need for the international community to prevent conflict, cooperate and stabilize cyberspace has become clear. The EU is promoting, in close cooperation with other international organisations, in particular the UN and the OSCE, a strategic framework for conflict prevention, cooperation and stability in cyberspace, which include (i) the strict application of international law, and in particular the UN Charter in its entirety, in cyberspace; (ii) the full respect of universal non-binding norms, rules and principles of responsible State behaviour; (iii) the development and implementation of regional confidence building measures (CBMs). To the extent possible, the CDPF should also support this endeavour.

Cyber security and defence are also priorities within the EU Global Strategy. The Strategy emphasizes the need to increase capacities to protect Europe and respond to external crises. The commitment to mutual assistance and solidarity in Europe includes, among other issues, cyber security and defence aspects. The EU Global Strategy has a strong emphasis to the strengthening of the EU as a security community, which should be strategically autonomous. It requires solid European defence technology and industry. Deeper defence cooperation with more interoperability and effectiveness in defence capability development are also priorities.

Specifically on cyber security, the strategy calls for more technological capabilities aimed at mitigating threats and raising resilience of critical infrastructure, networks and services. It also stresses the reinforcement of the cyber elements in CSDP missions and operations as well as advancement of cooperation between the Member States and with core partners such as the US and NATO.

In particular, the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization in Warsaw on 8 July 2016 stresses the need to expand EU and NATO coordination on cyber security and defence including in the context of missions and operations, as well as in relation to training, education and exercises. Of the actions ('common set of proposals', including the 'common set of new proposals') endorsed by the two Councils for the implementation of the Joint Declaration, five are related to cyber security and defence. The Warsaw Summit has also declared cyberspace as a domain of operations. This cooperation takes place in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of the EU.

In July 2016, the EU adopted the Network and Information Security Directive, which will harmonise the overall preparedness of the Member States against cyber threats, and enhance EU wide cooperation. The NIS Directive should be transposed to the Member States legislation by May 2018. It addresses a set of common standards and rules for ensuring a high level of network and information security and resilience of civilian ICT across many sectors of the EU.

On 11 December 2017, Permanent Structured Cooperation (PESCO) has been launched. This ambitious, binding and inclusive European framework established between Member States also includes a commitment to increase efforts in the cooperation on cyber defence, as well as related projects.

4. Progress regarding the implementation of the Cyber Defence Policy Framework

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

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. In that respect a revised Cyber Defence Strategic Context Case (SCC) was endorsed by the EDA Steering Board in March 2017. This SCC will govern the EDA Cyber Defence Activities with a mid-term time horizon. The EDA Project Team (PT) Cyber Defence continues to meet 3 times a year with a strong participation of Member States. The last meeting took place in October 2017 in Tallinn in combination with the 1st EDA Cyber Innovation Day. Next meetings of the PT are planned for February and May 2018.

The mainstreaming of cyber remains a priority, and EDA will for instance ensure that cyber related aspects are appropriately reflected in its current and future projects/activities in the Air Domain (such as SESAR and RPAS) as well as an emergent area for the maritime and space domains.

On 30 June 2015 the EDA Steering Board in R&T Directors composition tasked the EDA to start the negotiations for the establishment of a holistic Cyber Defence Joint Program with interested EDA participating Member States (pMS). Consultations lead to the establishment of an Ad-Hoc Working Group (AHWG) on Cyber Defence R&T for a trial period of 18 months by the EDA Steering Board on 19 October 2016. The AHWG shall develop a Cyber Defence Strategic Research Agenda (CD SRA) and propose the way ahead for enduring support for Cyber Defence related collaborative R&T thereafter. The first Cyber Defence R&T AHWG meeting took place at the end of November 2016 and met 4 times since then. The CD SRA and the recommendations for the way ahead are expected by the first half of 2018. To explore synergies with the civilian cyber security research activities, the AHWG invited the European Cyber Security Organisation (ECSO) to participate in two of the AHWG meetings.

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

- The project for the establishment of a web-based "Cyber Defence Training and Exercise, Coordination and Support Platform" (CD TEXP) is progressing as scheduled and the IT platform is expected to be technically ready for operational usage by end 2017. The platform will reference inter alia the cyber ranges federation, DePoCyTE, cyber training by MS opened to other MS attendance, and courses from EU institutions. It will be hosted and operated by the Portuguese Armed Forces.

- Other projects include, inter alia: (1) the development of a Deployable Cyber Evidence Collection and Evaluation Capability (DCEC2), in which two technology demonstrators will be tested in operational environments in 2018; (2) preparation of a Cyber Defence Pilot Exercise for Cyber Operations Planning at OHQ/FHQ level including a Cyber Defence Pilot Seminar for non-Cyber Defence Staff Officers (J1-J9 and special advisors), which will be executed in June 2018 in Salzburg, AT; (3) Comprehensive Cyber Strategic Decision Making Exercises, to be executed in 2017 and 2018; (4) and in cooperation with ESDC the preparation of the delivery of a Senior Decision Maker Cyber Operation Planning Seminar, which will take place in January 2018 at the DE Defence Academy in Hamburg; (5) the continuation of the Target Architecture and System Requirements study for an enhanced Cyber Situation Awareness;

- Currently projects for Research on Cyber Defence Career Models for Armed Forces as well as to update the EU Cyber Defence Landscape overview are under preparation for execution in 2018.

In relation to the *Pooling & Sharing* agenda, the development of several projects continues apace:

a) Cyber Ranges: The project arrangements have been signed by all eleven contributing members before May 2017. The project is co-lead by EL, FI and NL, with AT, BE, DE, EE, IE, LV, PT and SE as contributors. The project implementation phase has commenced with the 1st Project Arrangements Management Committee meeting 13 July 2017. This Project will put in place a collaborative mechanism to enable national cyber defence exercise and training facilities to coordinate efforts, exchange information and, ultimately, to interconnect for ambitious multinational cyber exercises and other training events. An exchange of letters between the EDA and the European Space Agency (ESA) has been signed recently facilitating negotiations between the project contributing members and ESA about future cooperation on Cyber Ranges with ESA.

b) Deployable cyber situation awareness packages for Headquarters (CySAP): Ad Hoc R&T Cat B project was accepted by EDA Steering Board decision in August 2017 with DE, ES and IT as contributing Member States. Project Arrangements development on a Rapid Research Prototype will progress simultaneously with the results of the OB study on Target Architecture and System Requirements. The Project Arrangement together with a Research Technical Proposal from the Industry Consortium shall be ready by 2018 Q2. In that case, CySAP shall deliver its results by end 2019.

c) Pooling of Member States demand for private sector training and exercise (DePoCyTE): the initiative for the "Demand Pooling for the Cyber Defence Training and Exercise support by the private sector" (DePoCyTE) was launched in January 2016. An *ad hoc* working group to develop the necessary documentation for the pre-project phase was established in April 2016 and the Common Staff Target (CST) has been endorsed by the EDA Steering Board in December 2016. Works for the development of the Common Staff Requirement (CSR) are ongoing including the development of a related business case with the objective to have the CSR ready for EDA Steering Board Endorsement by early 2018. Starting the negotiation of the Project Arrangement is expected for the 1st semester 2018.

d) Advanced Persistent Threat Detection (APT-D): Ad Hoc R&T Cat B project was approved by EDA SB in April 2017. Project Arrangement negotiations are underway with a revised research technical proposal with three contributing Member States BE, DE and NL.

In the EDA Steering Board meeting at 13 November 2017 Defence Ministers received an update on the EDA efforts on cyber defence and welcomed the Agency's achievements on cyber defence capability development and called on the Agency's continuing efforts to fully implement the Strategic Context Case (SCC) agreed in March 2017.

To highlight the importance assigns to Cyber Defence, the EDA Annual Conference of 2017 was dedicated to Cyber.

In December 2017, a first set of PESCO projects have been identified by PESCO participating Member States. Among others it includes a Lithuanian-led project "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" and a Greece-led project "Cyber Threats and Incident Response Information Sharing Platform".

Facilitating exchanges between Member States on cyber defence issues is a continuous task for both EU institutions and Member States themselves. The 2017 Cyber Defence Smart Defence & Pooling and Sharing conference organised by the Portuguese Armed Forces in April 2017is an example of such platform for networking and sharing knowledge, to encourage new opportunities for cooperation.

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.

The work to update the Requirements Catalogue from 2005, RC(05) over the past few months identified the military capability requirements against 5 illustrative scenarios. The need for appropriate cyber defence capabilities was clearly articulated.

In the framework of the Connecting Europe Facility (CEF) Telecom Programme a Cyber Digital Service Infrastructure (DSI) is under development, aiming to establish and deploy cooperation mechanisms between national Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs) to enhance the EU-wide capability for preparedness, information sharing, coordination and response to cyber threats. Following the implementation process of the Network and Information Security (NIS) Directive, the EU CSIRT Network has been established, which may be used as additional mechanism for enhanced information exchange on Cyber Security.

DELETED

DELETED

DELETED

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

A key objective of the European Defence Action Plan is to examine ways of using Commission programmes to support European military capability priorities as identified by Member States. The Action Plan also strengthens the EU's strategic autonomy as well as the defence industry innovation and competitiveness in the global markets. Cyber security and defence is one of the critical sectors for maintaining European technological and operational superiority in the next decade and where an EU approach could add value.

More broadly, the promotion of civil-military cooperation was further promoted in 2017, as showcased by the strong emphasis on cyber defence in the Joint Communication on building strong cybersecurity for the EU.

In addition, two sets of Council conclusions in November 2017 highlighted the need to encourage synergies between civilian and military cyber communities, including in response to cyber incidents.

4.4. Improving training, education and exercises opportunities

Cyber defence training and education platform

Following the presentation by the Commission and the High Representative of the Union of the cyber package in September 2017, the work conducted by EDA since 2014 and the results of its update study on cyber training and education, and the relevant Council Conclusions, a cyber defence training and education platform is currently under establishment within the European Security and Defence College (ESDC). To ensure training and education opportunities within the Member States are upscaled to the appropriate level, the Commission should support this endeavour.

The implementation of the proposed solution within ESDC is currently under preparation with relevant stakeholders with a view of achieving Initial Operational Capability by Mid-2018.

EU Military Training Group

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. Four workshops were organised in February, March, June and October 2016 to set up the framework associated with the development of a Cyber Defence Curriculum. During 2017, the two cyber discipline co-leaders organized two Workshops. The latest, taking place in Paris in September 2017 was the occasion to:

– ensure the coherence of EU and NATO efforts in the domain, in line with the 2016 Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization;

– reinforce the dual-use relevance, taking into account the new cyber package;

– remind the importance of the use of a common vocabulary within EU, as well as with NATO;

– make progresses on the finalisation of an overview on the curricula associated to any category of employment at several levels of competencies;

– agree on sending, before the end of 2017, a renewed questionnaire to identify the updated capabilities that Member states need and provide an analysis of prioritized needs in the domain of cyber military education and training in 2018.

EU Military Erasmus (coordinated by the ESDC)

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 was 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".

Cyber Training of Member States under the auspices of the ESDC

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 dedicated cyber awareness courses and mainstreamed cyber defence and security as a horizontal subject. Two standard curricula have been developed, the newest being a three-modular-course on cyber security. In addition, several cyber related articles were published in the ESDC handbook series.

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. 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.

Operational cyber defence training

Based on the Cyber Awareness Seminars provided to the OHQ Larissa for EUFOR RCA in 2014, and the OHQ Rome for EUNAVFOR MED in 2015 and 2016, EDA continues to lead training on 21-22 March and 3-4 October 2017 in OHQ EU NAVFOR MED/SOPHIA. The preparation and delivery of the seminars continues to be supported by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE) and by SYMANTEC on Cyber Threat Assessment. If the budget provisions allow, the seminar will continue organising up to 3 trainings per year along the rotation of staff as long as the OHQ is activated for EU NAVFOR MED/SOPHIA.

Exercises

Based on the lessons learned from the crisis management exercises Multi-layer 14 (ML 14) and Multi-layer 16 (ML 16), the EU tested its crisis response tools and mechanisms to counter cyber and hybrid threats this year. The EU-NATO Parallel and Coordinated Exercise PACE17 focused on four key areas, namely situational awareness, effectiveness of our instruments to counter cyber threats at EU level, speed of reaction and appropriate reactivity of our crisis response mechanisms, as well as our capacity to communicate fast and in a coordinated way. The exercise was followed by an evaluation phase, to identify lessons learned and improve our response mechanisms. These aspects will inform the planning for MILEX18 and EU PACE18.

A separate crisis management exercise was conducted by NATO from 4 to 11 October 2017. NATO's CMX17 exercise and PACE were conducted independently, but in a parallel and coordinated manner, ensured by EU – NATO staff-to-staff coordination and participation throughout both exercises. The aim was to improve the synchronisation of crisis response activities between the two organisations.

In September 2017, the Estonian presidency has organised a ministerial level table top exercise EU CYBRID 2017 in the margins of the EU informal Defence Ministers meeting. It has addressed strategic decision-making during the crisis with cyber aspects affecting CSDP command and control function. The exercise served as an awareness raising occasion for the Ministers of Defence of 28 Member States, in the presence of the NATO Secretary General.

Two Comprehensive Cyber Strategic Decision Making Exercises were conducted with the Greek government (May 2017) and the Latvian government (November 2017) facilitated by EDA. Two more exercises are envisaged for execution in 2018.

Also in this reporting period, EU bodies have been invited to attend, either in an observer or participant capacity, various multinational cyber defence exercises such as NATO's CMX, CYBER COALITION, TIDE SPRINT and LOCKED SHIELDS, providing an excellent opportunity to develop more competences in this domain. In 2018 for the first time an EU Team under the lead of CERT-EU will actively participate in the LOCKED SHIELDS exercise. Discussions on reciprocal arrangements for NATO to observe or participate in EU exercises, such as CYBER EUROPE, are ongoing.

Negotiations on the establishment of a cooperation roadmap between EDA and ENISA on various subjects such as training and exercises were finalized in spring 2017. Currently, negotiations between ENISA, EC3, CERT-EU and EDA continue in order to identify areas for quadrilateral cooperation.

DELETED

DELETED

6. Recommendations

It is recommended that the PSC:

– welcomes the progress and achievements in the implementation of the EU Cyber Defence Policy Framework, and encourages all stakeholders to further implement it;

– welcomes the work conducted so far on enhancing operational cyber protection of the EEAS and CSDP communications networks and encourages the EEAS to continue its efforts to that end;

– stresses the need to address the lessons learned within EU exercises, including those with other partners (e.g. NATO), in order to improve the understanding and actions needed and to identify possible synergies between them;

– invites the EEAS and the EDA to present proposals, in cooperation with the European Commission and based on Member States' input, for the update of the EU Cyber Defence Policy Framework by mid-2018;

– calls for the presentation of an updated progress report in December 2018, which would cover the year 2018. An interim oral update on the implementation of the Cyber Defence Policy Framework should be provided by EEAS, in cooperation with the European Commission and the European Defence Agency (EDA), to the PMG in May-June 2018.