Council of the European Union

Brussels, 19 November 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	19 November 2018
To:	Delegations
Subject:	EU Cyber Defence Policy Framework (2018 update)

Delegations will find in the Annex the EU Cyber Defence Policy Framework (2018 update), adopted by the Council at its 3652nd meeting held on 19 November 2018.

ANNEX

EU CYBER DEFENCE POLICY FRAMEWORK

(as updated in 2018)

Scope and Objectives

To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities.

The EU Cyber Defence Policy Framework (CDPF) supports the development of cyber defence capabilities of EU Member States as well as the strengthening of the cyber protection of the EU security and defence infrastructure, without prejudice to national legislation of Member States and EU legislation, including, when it is defined, the scope of cyber defence.

Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.

The objective of the updated CDPF is to further develop EU cyber defence policy by taking into account relevant developments in other relevant fora and policy areas and the implementation of the CDPF since 2014. The CDPF identifies priority areas for cyber defence and clarifies the roles of the different European actors, whilst fully respecting the responsibilities and competences of Union actors and the Member States as well as the institutional framework of the EU and its decision-making autonomy.

Context

The European Council Conclusions on CSDP of December 2013 together with the Council Conclusions on CSDP of November 2013 called for the development of an EU Cyber Defence Policy Framework, on the basis of a proposal by the High Representative, in cooperation with the European Commission and the European Defence Agency (EDA). The EU Cyber Defence Policy Framework was adopted by the Council on 18 November 2014[1] and since then, through its implementation, concrete outputs have contributed to significantly enhance Member States' cyber defence capabilities. As part of the 2017 Annual Report on the Implementation of the Cyber Defence Policy Framework[2], and taking into account EU initiatives in the area of security and defence, notably the Coordinated Annual Review on Defence (CARD), the Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF), and the Civilian CSDP Compact as well as the 2018 revision of the Capability Development Plan (CDP) and the Civilian Capability Development Plan (CCDP), Member States called for an update of the EU Cyber Defence Policy Framework.

Cyber security is a priority within the Global Strategy on the EU Foreign and Security Policy and within the EU Level of Ambition[3]. The Global Strategy emphasises the need to increase capacities to protect the EU and its citizens and respond to external crises. The Global Strategy underlines the need to strengthen the EU as a security community. In this context, Security and defence efforts should also enhance the EU's strategic role and its capacity to act autonomously when and where necessary and with partners wherever possible. These goals require more cooperation in capability development, promoting the effectiveness and interoperability of the resulting civilian and military capabilities.

---

1 Council document 15585/14, 18.11.2014.
2 Council document 15870/17, 19.12.2017
3 Council Conclusions on implementing the EU global strategy in the area of security and defence, 14.11.2016

The common set of proposals for the implementation of 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[4] include concrete actions to expand EU and NATO cooperation on cyber security and defence including in the context of missions and operations, as well as in relation to cyber defence capability development, research and technology, training, education, exercises and mainstreaming cyber into crisis management. This cooperation takes place in full respect of the principles of openness, transparency, inclusiveness, reciprocity, and decision-making autonomy of the EU. A Technical Arrangement between the Computer Emergency Response Team of the EU (CERT-EU) and the NATO Computer Incident Response Capability (NCIRC), signed in February 2016, is facilitating technical information sharing to improve cyber incident prevention, detection and response in both organisations.

It should be recalled that several EU policies contribute to the objectives of cyber defence policy as set out in this document, and this framework also takes into account relevant regulation, policy and technology support in the civilian domain. For example in July 2016, the European Parliament and the Council adopted the Network and Information Security Directive[5] (NIS), which will increase the overall preparedness of the Member States against cyber threats, and enhance EU-wide cooperation. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. The transposition deadline of the Directive was 9 May 2018.

---

4 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)

5 Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

The proposal, in September 2017, for a EU Cybersecurity Act includes the new mandate for the EU's cybersecurity agency (ENISA) and the establishment of a EU-wide certification framework. Once in place, the certification framework should support high standards for ICT processes, products and services and be a source of competitive advantage and increase confidence on the side of consumers and procurers. As well, the Commission in September 2017 took another step to prepare the EU for the case of a large-scale cross-border cybersecurity incidents ("Blue Print"), and is now working with Member States and other institutions, agencies and bodies on the development of European Cybersecurity Crisis Cooperation, putting in place the practical operationalisation and documentation of all the relevant actors, processes and procedures within the context of existing EU crisis and disaster management mechanisms, in particular the Integrated Political Crisis Response arrangements.

The Council conclusions on strengthening Europe's Cyber Resilience of November 2016 outlined the common goal of contributing to the EU's strategic autonomy, as referred to in the Council conclusions of November 2016 on the Global Strategy on the European Union's Foreign and Security Policy, including in cyberspace. The European Council reaffirmed this message in June 2018 and also underlined the need to strengthen capabilities against cybersecurity threats from outside the EU.

In 2017 the Council adopted a Framework for a joint EU diplomatic response to malicious cyber activities (the "cyber diplomacy toolbox")[6]. The Framework is expected to encourage cooperation, facilitate mitigation of threats, and influence the behaviour of potential aggressors in the long term. The Framework makes use of CFSP measures, including restrictive measures, to prevent and respond to malicious cyber activities. Actors of malicious cyber activities need to be held accountable for their actions, and EU Member States are encouraged to further develop their ability to respond to malicious cyber activities, in a coordinated way in line with the cyber diplomacy toolbox. States should not conduct or knowingly support information and communication technology activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technology.

A Joint Communication[7] on cyber was presented by the Commission and the HR/VP in September 2017 to mitigate risks stemming from the new threat landscape. It includes cyber defence as one of the main areas of action, and the CDPF is one of the pillars of its concrete implementation[8].

The Council conclusions of November 2017 on cyber issues recognised the growing linkages between cyber security and defence and called to step up cooperation on cyber defence, including by encouraging cooperation between civilian and military incident response communities. It also stressed that a particularly serious cyber incident or crisis could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause and/or the Mutual Assistance Clause.

---

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

7 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)

8 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)

On 11 December 2017, Permanent Structured Cooperation (PESCO) was launched. This ambitious, binding and inclusive cooperation framework has been established between 25 Member States and includes a commitment to increase efforts in the cooperation on cyber defence, as well as related PESCO projects. The first set of PESCO projects identified by PESCO participating Member States in 2017 includes two projects related to cyber defence: “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security” and “Cyber Threats and Incident Response Information Sharing Platform”. Further sets of PESCO projects are foreseen. PESCO will develop cyber defence capabilities, and therefore strengthen cooperation among participating Member States and increase interoperability.

The updated EU Capability Development Plan (CDP) endorsed by the EDA Steering Board in June 2018 identifies cyber defence as a key element, recognising the need for defensive cyber operations in any operational context, based on sophisticated current and predictive cyberspace situational awareness, including the ability to combine large amounts of data and intelligence from numerous sources in support of rapid decision making and increased automation of the data gathering, analysis and decision-support process. The CDP 2018 identifies cyber defence capability priorities in the following areas: cooperation and synergies with relevant actors across cyber defence and cybersecurity areas; cyber defence research and technology activities; systems engineering frameworks for cyber operations; education, training, exercises and evaluation (ETEE); addressing cyber defence challenges in Air, Space, Maritime and Land.

Finally, over the last few years, the need for the international community to prevent conflict, cooperate and stabilise cyberspace has become clear. The EU is promoting, in close cooperation with other international organisations, in particular the UN, the OSCE and the ASEAN Regional Forum, a strategic framework for conflict prevention, cooperation and stability in cyberspace, which includes (i) the application of international law, and in particular the UN Charter in its entirety, in cyberspace; (ii) the respect of universal non-binding norms, rules and principles of responsible State behaviour; (iii) the development and implementation of regional confidence building measures (CBMs). The Cyber Defence Policy Framework should also support this endeavour.

Priorities

Six priority areas have been identified in the updated CDPF. A primary focus of this policy framework is the development of cyber defence capabilities, as well as the protection of the EU CSDP communication and information networks. Other priority areas include: training and exercises, research and technology, civil-military cooperation and international cooperation. In the area of training, emphasis is given to the upscaling of Member States' cyber defence training and of cyber awareness training of the CSDP chain of command. It is also important that the cyber dimension is adequately addressed in exercises in order to improve the EU's ability to react to cyber and hybrid crises by improving decision-making procedures and availability of information. Cyberspace is a rapidly developing domain and new technological developments need to be supported, both in the civilian and military domains. Civil-military cooperation in cyber field is key to ensure a coherent response to cyber threats. Last, but not least, enhancing cooperation with international partners could help enhance cybersecurity within the EU and beyond, and to promote EU principles and values.

This framework outlines proposals and opportunities for coordination between relevant EU institutions, bodies and agencies. It also reflects the important role of the private sector for the development of technologies for cyber security and cyber defence.

Additionally, the CDPF further supports cyber defence integration within the Union's crisis management mechanisms where, to deal with the effects of a cyber crisis, relevant provisions of the Treaty of the EU and the Treaty on the Functioning of the EU[9] may be applicable.

1. Supporting the development of Member States' cyber defence capabilities

The development of cyber defence capabilities and technologies should address all aspects of capability development, including doctrine, leadership, organisation, personnel, training, industry, technology, infrastructure, logistics and interoperability. To this end, Member States should step up their efforts to deliver effective cyber defence capability. The EEAS, the Commission and EDA should work together and support these efforts.

A continuous assessment of the vulnerabilities of the information infrastructures that support CSDP missions and operations is required, along with a near real-time understanding of the effectiveness of the protection. From an operational point of view, one of the main areas of attention of cyber defence activities will be to maintain the availability, integrity and confidentiality of CSDP communication and information networks, unless specified otherwise within the mandate of the operations or missions. Furthermore, the EEAS, in cooperation with Member States, will further integrate cyber capabilities in CSDP missions and operations.

Actors of malicious cyber activities need to be held accountable for their actions. It is important that EU Member States, supported by the EEAS, foster mutual cooperation to respond to malicious cyber activities. The cyber diplomacy toolbox is developed to help achieve such a mutual response. The EEAS and EDA will organize regular exercises on the basis of the cyber diplomacy toolbox in which EU Member States can practice this.

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

Considering that in national legislation of Member States as well as EU legislation, the scope of cyber defence is broad and diversified, where and when it is defined, there is a need to develop a common aggregated understanding on the scope of cyber defence.

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

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

- Use the CDP and other instruments such as CARD that facilitate and support cooperation between Member States in order to improve the degree of convergence in the planning of cyber defence requirements of the Member States at the strategic level, notably on monitoring, situational awareness, prevention, detection and protection, information sharing, forensics and malware analysis capability, lessons learned, damage containment, dynamic recovery capabilities, distributed data storage and data back-ups.
- Support current and future cyber defence-related Pooling and Sharing projects for military operations (e.g. in forensics, interoperability development, standard setting).
- Develop a standard set of objectives and requirements defining the minimum level of cybersecurity and trust to be achieved by Member States, drawing on existing EU-wide experience.

The EEAS and the EDA will:

- Facilitate exchanges between Member States on national cyber defence doctrines as well as on cyber defence oriented recruitment, retention and reservists programs.

The EDA will:

- Study the different scopes of cyber defence military requirements in Member States national legislation and best practices. The main objective of the study will be to develop an enterprise architecture for cyber defence, to include scope, functionalities and requirements used in the domain by the Member States upon the national and EU legislation.

Member States will, on a voluntary basis:

- Improve cooperation between their military CERTs to improve the prevention and handling of incidents.
- Take advantage of the PESCO to further increase cooperation on cyber defence, including new projects.
- Take advantage of the European Defence Fund to jointly develop cyber defence capabilities.
- Develop a common understanding on the application of the mutual assistance clause in the cyber field, while preserving its flexibility.
- Develop baseline cyber defence requirements for information infrastructure.
- To the extent that the improvement of cyber defence capabilities depends upon civilian network and information security expertise, take advantage of the expertise from ENISA, the Member State authorities assembled in the NIS Cooperation Group, and other possible entities at EU level with expertise in civilian cybersecurity.

Member States, the EEAS/EU Military Staff, the ESDC and the EDA will:

- Consider developing cyber defence training in view of EU Battlegroup certification.

The Commission, in cooperation with the Member States, will:

- Consider cyber defence in the work programmes of the European Defence Industrial Development Programme and the European Defence Fund.

2. Enhancing the protection of CSDP communication and information systems used by EU entities

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

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

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

For better coordination and to enhance the protection and resilience of CSDP communication and information systems and networks, an internal EEAS Cyber Governance Board under the EEAS Secretary General was created in 2017.

The EEAS/BA will:

- Strengthen IT security capacity within the EEAS, based on existing technical capability and procedures, with a focus on prevention, detection, incident response, situational awareness, information exchange and early warning mechanism. A cooperation strategy with the CERT-EU and existing EU cyber security capabilities will be further enhanced.

The EEAS/BA will, together with the EUMS, MPCC, CMPD and CPCC:

- 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.

The EEAS/Single Intelligence Analysis Capacity (SIAC) will:

- Building upon existing structures, strengthen its cyber threat assessment and intelligence capability to identify new cyber risks and provide regular risk assessments based on the strategic threat assessment and near real-time incident information coordinated between relevant EU structures and made accessible at different classification levels.

The EEAS/ SIAC and CERT-EU will:

- Promote real-time cyber threat information sharing between Member States and relevant EU entities. For this purpose, information sharing mechanisms and trust-building measures will be developed between relevant national and European authorities, through a voluntary approach that builds on existing cooperation.

The EEAS/EUMS and MPCC will:

- Further develop and integrate into strategic level planning a cyber defence concept for CSDP military missions and operations.
- Develop, in cooperation with the operational headquarters, a generic operational level Cyber Standard Operation Procedure.

The EEAS/CPCC and CMPD will:

- Further develop and integrate into strategic planning a cyber defence concept for CSDP civilian missions.
- Strengthen CSDP civilian missions' cyber defence capabilities building upon existing infrastructure and promoting the standardisation and harmonisation of technologies used within CSDP missions and operations, taking advantage, where relevant, of the expertise of CERT-EU, ENISA and EDA.
- In the process of strengthening civilian CSDP, further investigate the possible support to host nations on cyber security by civilian CSDP missions.

The EEAS will:

- Further develop common requirements for CSDP military and civilian missions and operations.
- Enhance cyber defence coordination to implement objectives related to the protection of networks used by EU institutional actors supporting CSDP, drawing on existing EU-wide experiences.
- Review regularly resource requirements and other relevant policy decisions based on the changing threat environment, in consultation with the Member States and other EU institutions.

3. Promotion of civil-military cooperation

Cyberspace is a rapidly developing domain: technological developments need to be strengthened by security systems, both in the civil and military domain. To the extent possible, coordination should be foreseen between the civil and the military domain in the cases that similar technological developments bring solutions for civil and military applications. In other cases, military capabilities and weapon systems are so specific that there is no scope for sharing with civilian technologies. Without prejudice to Member States' internal organisation and legislation, civil-military cooperation in the cyber domain can be considered inter alia for exchange of best practices, information exchange and early warning mechanisms, incident response risk assessments and awareness raising, and for training and exercises.

Improving civil cyber security is an important factor which contributes to overall network and information security resilience. The NIS Directive increases preparedness at the national level, and strengthens cooperation at Union level between Member States both at strategic and operational level. This cooperation involves both national authorities overseeing cybersecurity policies as well as national CERTs and CERT-EU. Cooperation between civil and military CERTs should be reinforced taking due account of these developments. The new European Cybersecurity Act aims to improve European resilience to cyberattacks and provide a cybersecurity certification framework for products and services, thus increasing trust in the civilian digital sphere.

The EDA, the European Network and Information Security Agency (ENISA), the European Cybercrime Centre (EC3) and CERT-EU, together with other relevant EU bodies and agencies, within their respective mandates and without overlapping with Member States' competences, as well as the Member States, are encouraged to further enhance their cooperation in the following areas:

- Develop common cyber security and defence competence profiles based on international best practises and certification used by EU institutions, bodies and agencies, taking also into account private sector certification standards.
- Contribute to develop further and adapt public sector cyber security and defence organisational and technical standards for use in the defence and security sector. Where necessary, build on the ongoing work of ENISA and EDA.
- Establish or further develop working mechanisms and arrangements to exchange best practice notably on education, training and exercises as well as on research and technology and other areas providing for civil-military synergies.
- Draw on existing EU experiences in cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyber defence capabilities.

The Member States will, on a voluntary basis:

- Strengthen cooperation between civil and military CERTs between the Member States.

The EEAS, the Commission and Member States will:

- Include cyber defence in EU crisis and disaster management procedures (through the blueprint process).

4. Research and technology

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

Cyber defence capability development has an important R&T dimension. Within the framework of the Cyber Defence Research Agenda (CDRA), the EDA has provided a sound basis for the prioritisation of future R&T funding within the intergovernmental framework. The subsequent Strategic Research Agenda developed within the relevant EDA Ad Hoc Working Group provides informed prioritisation on cyber-related technologies necessary for the military while identifying opportunities for dual-use efforts and investments, be it in national, multinational or EU-funded contexts.

The development of technological capacities in Europe to mitigate threats and vulnerabilities is essential. Industry will remain the primary driver for cyber defence-related technology and innovation. Cryptography, secure embedded systems, malware detection, simulation and visualisation techniques, network and communication systems protection, identification and authentication technology are some of the areas that need to be addressed. It is also important to foster a competitive European industrial cyber security supply chain by supporting the involvement with small and medium-sized enterprises (SMEs).

Ensuring that Europe is able to keep up with international competitors on cyber technological capabilities also depends on our ability to boost breakthrough innovation, through national as well as EU instruments, such as the European Innovation Council.

To facilitate civil-military cooperation in cyber defence capability development, to strengthen the European Defence Technological and Industrial Base[10], and to contribute to the EU's strategic autonomy also in the area of cyberspace, when and where necessary and with partners wherever possible**,**

The EDA, the Commission and Member States will:

- Seek synergies of R&T efforts in the military sector with civil Research & Development programmes, in particular those regarding breakthrough innovations, and consider the cyber security and defence dimension when implementing the Preparatory Action on Defence Research.
- Share cybersecurity research agendas (e.g. European Defence Agency Strategic Research Agenda on cybersecurity), as well as resultant roadmaps and actions; to this end, a cross-sectoral cyber defence research agenda will be developed, in close cooperation with the Commission and the Member States.
- Contribute to improve the integration of cybersecurity and cyber defence dimensions in the programmes that have a dual-use security and defence dimension, e.g. Single European Sky Air Traffic Management Research (SESAR) programme.

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

The Commission will:

- Consider the creation of a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres to support cybersecurity technological and industrial capacities and to increase the competitiveness of the Union's cybersecurity industry, ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres and with other EU agencies. The Centre should, inter alia, enhance cooperation between civilian and defence technologies and applications, working closely and in full complementarity with the European Defence Agency in the area of cyber defence.
- 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.

The Commission, in cooperation with the Member States, will:

- Consider cyber defence issues in the calls of the Preparatory Action on Defence Research.
- Consider cyber defence in the topics called for in the European Defence Fund.
- Support EU policy coherence to ensure that policy and technical aspects of EU cyber protection remain at the forefront of technology innovation and are harmonised across the EU (cyber threat analysis and assessment capability, "security by design" initiatives, dependency management for technology access, etc.).

5. Improve education, training and exercises opportunities

To increase preparedness to address cyber threats and to develop a common cyber defence culture across the EU, also benefiting EU missions and operations, there is a need to improve and upscale cyber defence training opportunities. It is crucial that education and training budgets are used efficiently while delivering the best possible quality. Pooling and sharing cyber defence education and training at the European level will be of key importance.

The European Security and Defence College (ESDC), the EEAS, the EDA, the Commission and Member States will:

- 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, which should also address skilled personnel retention issues in the short, medium and longer term.
- 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.
- Engage with European private sector training providers, as well as academic institutions, to raise the competencies and skills of personnel engaged in CSDP missions and operations.

The ESDC will:

- Further develop the cyber education, training, evaluation and exercises platform established in ESDC (cyber ETEE platform).
- Create synergies with the training programmes of other stakeholders such as the ENISA, Europol, the European Police College (CEPOL) and the NATO Cooperative Cyber Defence Centre of Excellence.
- Explore the possibility of joint ESDC-NATO cyber defence training programmes, open to all EU Member States, in order to foster a shared cyber defence culture.

The Commission will:

- Assess options to upscale the training and education opportunities within the Member States identified by the cyber ETEE platform.

The EDA will:

- Develop further EDA courses in collaboration with ESDC to meet the Member States' cyber defence education, training and exercises requirements.
- Support the cyber ETEE platform inter alia through progressively integrating cyber education, training, evaluation and exercises modules developed in the frame of EDA.

The EEAS and Members States will:

- Follow the established ESDC certification mechanisms for the training programmes in close cooperation with the relevant services in the EU institutions, bodies and agencies, based on existing standards and knowledge. Consider the possibility of setting up cyber specific modules in the framework of the Military Erasmus initiative.

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

The EEAS, the EDA, CERT-EU and the Member States will focus on promoting cyber defence elements in CSDP and other exercises:

- Integrate a cyber defence dimension into existing exercise scenarios for *MILEX* and *MULTILAYER*.
- Regularly organize strategic/political exercises such as *CYBRID 2017* in coordination with the EU-led Parallel and Coordinated Exercise (PACE), and technical-operational exercises such as *DEFNET*.
- 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.
- Continue to participate in other multinational cyber defence exercises, such as *Locked Shields*.
- Invite relevant international partners to the exercises, such as NATO, in accordance with the EU exercise policy framework.
- Organise regular exercises on the basis of the cyber diplomacy toolbox in which EU Member States can practice responding to malicious cyber activities.

6. Enhancing cooperation with relevant international partners

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

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

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

- Step up ongoing activities in the framework of 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.
- Exchange best practice in crisis management as well as in cyber defence of military and civilian missions and operations.
- Work on coherence of output in the development of cyber defence capability requirements where they overlap, especially in long-term cyber defence capability development.
- Utilise further the EDA cooperation framework with the NATO Cooperative Cyber Defence Centre of Excellence as an initial platform for enhanced collaboration in multinational cyber defence projects, based on appropriate assessments.

The ESDC, the EEAS and the EDA will:

- Enhance cooperation on concepts for cyber defence training and education as well as exercises.
- Ensure reciprocal staff participation in exercises in line with the agreed framework.

CERT-EU will:

- Further exploit the technical arrangement between the CERT-EU and the NCIRC (NATO Computer Incident Response Capability) in order to improve situational awareness, information sharing and early warning mechanisms, and anticipate threats that could affect both organisations.

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

- Follow strategic developments and hold consultations in cyber defence issues with international partners (international organisations and third countries).
- Explore possibilities for cooperation on cyber defence issues, including with third countries participating in CSDP missions and operations.
- Promote in relevant international organisations, in particular the UN, the OSCE and the ASEAN Regional Forum, the application of existing international law, in particular the UN Charter in its entirety, in cyberspace, the development and implementation of universal non-binding norms of responsible state behaviour, and regional confidence building measures (CBMs) between States to increase transparency and reduce the risk of misperceptions in State behaviour.

The Commission and the EEAS will:

- Where relevant, support the building of cyber capabilities for EU partners through the amended Instrument contributing to Stability and Peace (IcSP).

Follow-up

Upon EEAS coordination of the implementation of the CDPF, an annual progress report that includes the six areas outlined above should be presented to the Politico-Military Group, with the participation of the members of the Horizontal Working Party on Cyber Issues, and to the Political and Security Committee, by EEAS / EDA / Commission, in order to assess the implementation of the CDPF. A six-monthly oral presentation will also be provided.

It is essential that, as the cyber threat develops, new cyber defence requirements are identified, and then included in the Cyber Defence Policy Framework. The next revision of the CDPF should be presented no later than by mid-2022, in close consultations with Member States.