Cybersecurity in the EU Common Security and Defence Policy (CSDP)

Challenges and risks for the EU

STUDY

Science and Technology Options Assessment

EPRS | European Parliamentary Research Service
Scientific Foresight Unit (STOA)
PE 603.175

Cybersecurity in the EU Common Security and Defence Policy (CSDP)

Challenges and risks for the EU

Study

EPRS/STOA/SER/16/214N

Abstract

This report is the result of a study conducted by the European Union Agency for Network and Information Security (ENISA) for the European Parliament's Science and Technology Options Assessment (STOA) Panel with the aim of identifying risks, challenges and opportunities for cyber-defence in the context of the EU Common Security and Defence Policy (CSDP). Acceptance of cyber as an independent domain calls for the investigation of its integration with the EU's current and future policies and capabilities. ENISA analysed the related literature and work on cybersecurity, including its own publications, to form the basis for this study. In addition, a number of stakeholders, experts and practitioners, from academia, EU institutions and international organisations, were consulted in order to ensure the study is well-founded and comprehensive.

The study revolves around three thematic areas, namely: policies, capacity building, and the integration of cyber in the CSDP missions, with the last one being the main focus of the study. For each thematic area, we compile a set of policy options, covering different levels, starting from the EU's political/strategic level and progressing down to the operational and even tactical/technical levels of the CSDP's supporting mechanisms.

These policy options are summarised in a separate options briefing document accompanying this study.

PE 603.175

The STOA project 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) — Challenges and risks for the EU' was carried out by ENISA at the request of the Science and Technology Options Assessment Panel, and managed by the Scientific Foresight Unit (STOA) within the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament.

AUTHORS

Panagiotis Trimintzios, Georgios Chatzichristos, Silvia Portesi, Prokopios Drogkaris, Lauri Palkmets, Dimitra Liveri and Andrea Dufkova.

The authors acknowledge and would like to thank the following external experts for their contributions to this report: Prof. Paul Cornish, Dr Maria Bada (The Global Cyber Security Capacity Centre Oxford); Dr Jason C. R. Nurse, Dr Jassim Happa, Dr Ioannis Agrafiotis (University of Oxford); Mr Wolfgang Röhrig (European Defence Agency); Mr Hans-Peter Morbach, WCdr Rob Smeaton (NATO); Prof. Raffaele Marchetti, Dr Roberta Mulas, Ms Beatrice Valentina Ortalizio, Ms Valeria Tisalvi (LUISS School of Government); Dr Stefanie Frey, Melani, Ltc Franz Landenhammer, Maj Nikolaos Pissanidis, Dr Lauri Linström, Mr Henry Röigas, Maj Christian Tschida (NATO CCDCoE).

STOA ADMINISTRATOR RESPONSIBLE

Zsolt G. Pataki
Scientific Foresight Unit (STOA)
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services
European Parliament, Rue Wiertz 60, 1047 Brussels
Email: zolt.pataki@ep.europa.eu

LINGUISTIC VERSION

Original: EN

ABOUT THE PUBLISHER

To contact STOA or to subscribe to its newsletter please write to: STOA@ep.europa.eu
This document is available on the internet at: http://www.europarl.europa.eu/stoa/.

Manuscript completed in May 2017

PE 603.175
ISBN 978-92-846-1058-7
doi: 10.2861/853031
QA-04-17-454-EN-N

Contents

1. Introduction

Cyberattacks against Estonian public and private infrastructure in 2007 established a new dimension in the use of IT assets and networks. IT was used to cause a direct hit to a country's sovereignty and create harm to its people. This event has triggered a series of discussions, decisions, agreements and actions both at the EU and international levels on the use of IT and its operating domain, the cyberdomain, and its interaction with society, economic life, defence and other types of human activities (Herzog 2011).

In recent years, the cyberdomain has become the focal point of research, discussions and debates beyond the technical level. Concepts and terms like 'hybrid operations', 'active cyberdefence', 'cyberthreat vectors' and 'advanced persistent threats' have emerged in an attempt to describe the uses of the newly established domain by adversaries attempting to compromise core EU values like human dignity, democracy, the rule of law, equality and respect for human rights.

In February 2013, the European Union published its cybersecurity strategy (European Commission and High Representative of the EU for Foreign Affairs and Security Policy 2013). This strategy declared that 'The EU's core values apply as much in the digital as in the physical world. The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.' It gave five strategic priorities to address cyberthreats, including the development of cyberdefence policy and capabilities related to the common security and defence policy (CSDP).

One of the strategic priorities included the development of cyberdefence capabilities, policies and collaboration at EU level between civilian and military stakeholders as well as at the international level between the EU and other international partners like NATO, the UN, the Organization for Security and Co-operation in Europe (OSCE) and others, as well as centres of excellence, industry and academia (European Commission 2013, 11).

The year 2016 was a milestone towards a safer cyberspace for the EU. The joint declaration ([1]) between the EU and NATO paved the way for substantive future collaboration between the two organisations, with cybersecurity having a prominent role. The second important evolution has been the adoption by the European Parliament and the Council of the directive on security of network and information systems (the NIS Directive) (European Parliament and Council 2013). Though not directly connected to the CSDP, this is nevertheless the first piece of EU-wide legislation on cybersecurity ([2]) and will be the vehicle for shaping policies and cybercapacities at both the EU and the Member State level.

([1]) The EU–NATO joint declaration is accessible at http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/ (accessed: 17 January 2017).

([2]) https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive (accessed: 17 January 2017).

2. Methodology and study structure

This study has been conducted using a combination of desktop research and information gathered from interviews and discussions with relevant stakeholders from EU institutions, NATO and academia.

Although the aim of this study is to provide suggestions on what needs to be done in cybersecurity for the CSDP in the medium and long term, some short-term suggestions are also presented. Emphasis is put on coherence, by building on current progress in cybersecurity in the EU area. Scanning beyond the focus of the CSDP was necessary in order to identify best practices, challenges and policies for cybersecurity. ENISA's own work has also been used for this study.

A literature research was carried out between October and December 2016 on policies, doctrines, cyber-resilience, the cyberthreat landscape and cybercapacity building. The desktop research on all three thematic areas covered progress made in the last decade at a global and international organisational level, as well as country level, at least for countries that are featured in bibliographic references concerning cyberspace.

A number of experts were consulted during the course of this study. These experts came from the public, private and academic sectors, and had both civilian and military backgrounds. The experts gave input to ENISA on all three different areas covered by the study through both remote interviews and physical meetings. Input was received via questionnaires and interviews. ENISA utilised opinions and inputs received from external experts for the authoring of this report.

Key points for attention are framed in boxes like this one.

2.1. Study structure

This study is structured around the three research themes defined in the tender's specifications (STOA 2016). The first research theme revolves around policy challenges in cyberdefence for the EU Member States, the EU institutions, the international stakeholders and decision-makers. This section is not limited to the CSDP but rather provides a holistic approach on international and EU trends and processes and towards a safer cyberdomain. The second research theme focuses on capacity building. This section includes an analysis of the state of play on the global stage between nations, international organisations and the private sector. The third research theme focuses on the CSDP and analyses key factors for the successful protection of EU-led missions, civilian and military, against cyberthreats.

The study is supported by three annexes:

Annex A: The EU cyberdefence policy framework action items
Annex B: The ENISA cyberthreat taxonomy
Annex C: Policy options

The study also includes a summary of policy options in the form of separate options briefing documents.

3. Challenges for cyberdefence

Countries like China, Russia and the United States rely on their individual foreign and interior policies, their unified military structures and the legal and budgetary power of central governments for the development of coherent cybercapacities. In the EU, the individual Member States are responsible for their own cybercapacities, having widely varying levels of cybermaturity, different threats, priorities and capabilities (ENISA 2014). This fact, combined together with the borderless nature of cyberdomain, puts the EU into a much more challenging role in cybercapacity building.

In this chapter, we first identify policy challenges for building cybercapacities and then focus on new technological challenges and the need for regulation in cyberspace. The human factor and more specifically building of trust via confidence-building measures are also discussed in this chapter.

3.1. Policy challenges

Cyberdefence presents several policy challenges inside the EU; the main ones include the following:

1. the delicate balance between Member States' sovereignty and EU powers and responsibilities;
2. the complex set of mandates within EU institutions;
3. cyberspace as a domain of operations and the issue of the application of existing laws of armed conflicts to the cyberdomain;
4. hybrid technologies, including drones used in conflicts;
5. the issue of common agreed definitions and taxonomy;
6. the number and diversity of actors involved in cyberdefence;
7. military and civilian overlaps in cyberdefence — a blurry borderline;
8. the limited availability of data to support policy development.

The list above is not exhaustive: some new policy challenges might emerge, some extra complexity might be added and some challenges might be reshaped, for instance by a possible CSDP slowdown or 'acceleration', due to, for example, changes in the EU political landscape such as United Kingdom's decision to exit the EU ([3]).

These challenges are addressed below. In addressing them, Member State, EU and international perspectives are taken into account.

3.1.1. The delicate balance between sovereignty and central powers and responsibilities

While defence remains largely a field of Member States' sovereignty, the EU has power and responsibilities in common security and defence. Indeed, 'the common security and defence policy (CSDP) is an integral part of the Union's common foreign and security policy (CFSP)' ([4]). CSDP enables the Union to take a leading role in peace-keeping operations, conflict prevention and in the strengthening of the international security. 'It is an integral part of the EU's comprehensive approach towards crisis management, drawing on civilian and military assets' (EEAS 2016). In this framework 'the European Council meeting in Nice on 7-11 December 2000 reached agreement on the establishment of the Military Staff of the European Union, setting out its mission and functions' (Council of the European Union 2001).

([3]) Article 50 of the Lisbon Treaty (http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-6-final-provisions/137-article-50.html) (accessed: 17 January 2017).

([4]) http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_6.1.2.html (accessed: 20 January 2017).

The balance between the Member States' sovereignty and EU powers and responsibility in security and defence is delicate: 'Within the EU there is often a discussion between EU Member States and the institutions about what constitutes EU business, and what sovereign and therefore national business is' (Smeaton and Roehrig 2014).

As far as concerns cyberdefence in particular, Smeaton and Roehrig noted that 'An increasing number of countries in Europe have a National Cyber Security Strategy (NCSS) as a key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyber-space' (Smeaton and Roehrig 2014).

Some Member States 'have included a military perspective of cyber-defence in their national approaches' (Cîrlig 2014, 6) and some have NCSSs mentioning defence objectives (ENISA 2014, 14). Others cover 'military cyberdefence objectives … in separate strategic documents' (ENISA 2014, 14, Footnote 30).

In 2013, Bakowski noted that 'Cyber war and cyber-defence have … rarely been addressed at EU level, arguably due to limits of competence in common foreign and security policy (CFSP) ([5]) and that 'EU Member States tend to cooperate within NATO instead, to improve their cyber-defence capacities' (Bakowski 2013, 4). As highlighted by Pawlak in 2015, 'The need for closer engagement with key international partners, as a way towards promoting the EU's political, economic and strategic interests, was recognised in the EU Cyber security strategy of 2013, and the Council conclusions on Cyber Diplomacy adopted in February 2015' (Pawlak 2015, 1).

With a view to promoting the 'EU political, economic and strategic interests' (Council of the European Union 2015, 2), the EU launched cyberdialogues with China, India, Japan, South Korea and the United States. The Council of the European Union, in its conclusions on cyberdiplomacy, also encouraged 'the EU and its Member States to prepare cyberdialogues within the framework of effective policy coordination, avoiding duplication of efforts and taking into account the broader EU political and economic interests, collectively promoted by all EU actors' (Council of the European Union 2015).

It is important to note that the European External Action Service (EEAS) plays an important role in the cyberdialogues, being the EU 'coordinating body for these processes' (Pawlak 2015, 4).

Another aspect to be considered in the EU Member States' mutual defence within the CSDP is that the Lisbon Treaty introduced within the area of the CSDP ([6]) the mutual defence clause (Article 42(7) of the Treaty on European Union (EU 2016)), which provides that if 'a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter (UN 1945). This shall not prejudice the specific character of the security and defence policy of certain Member States.' It is important to note that this 'obligation of mutual defence is binding on all EU countries. However, it does not affect the neutrality of certain EU countries and is consistent with the commitments of EU countries, which are NATO members ([7]). This provision is supplemented by the

([5]) 'EU Member states have committed themselves to a common foreign security policy [CFSP] for the European Union. The European security and defence policy aims to strengthen the EU's external ability to act through the development of civilian and military capabilities in conflict prevention and crisis management' (EEAS 2016).

([6]) 'The common security and defence policy (CSDP) enables the Union to take a leading role in peace-keeping operations, conflict prevention and in the strengthening of the international security. It is an integral part of the EU's comprehensive approach towards crisis management, drawing on civilian and military assets' (EEAS 2016).

([7]) Article 5 of the NATO Treaty indeed states that 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they

solidarity clause (Article 222 of the Treaty on the Functioning of the EU) which provides that 'EU countries are obliged to act jointly where an EU country is the victim of a terrorist attack or a natural or man-made disaster' ([8]).

As noted by Troszczynska-Van Genderen, 'This clause implies the use of both civilian and military structures (including CSDP structures inside the EU that could be used in an internal operational context, among them the crisis management structures within the EEAS, including the military staff, and CSDP support structures such as the EU Satellite Centre in Torrejón (Spain), civil protection and counter-terrorism)' (Troszczynska-Van Genderen 2015, 14).

EU Member States need to continue joining efforts and assist each other to become stronger overall and to further enhance their cybercapability.

EU institutions and Member States should avoid duplication of efforts and act in line with the broader EU political and economic interests.

3.1.2. The complex set of mandates within EU institutions

In the EU, 'amongst relevant EU level organisations, we find a somewhat diverse picture with respect to cyber-defence. There is a complex operational setup regarding who undertakes cyber-defence activities (e.g. detection, reaction, response) between the EEAS, General Secretariat of the EU Council and European Commission' (Robinson, Walczak, et al. 2013, 6).

As stated in the EU cyberdefence policy framework adopted by the Council of the European Union on 18 November 2014, there is 'a need to streamline security rules for the information systems provided by different EU institutional actors during the conduct of CSDP operations and missions. In this context, a unified chain of command could be considered with the aim to improve the resilience of networks used for CSDP' (Council of the European Union 2014, 6).

Concerning defence capabilities, at EU level 'The EU Military Staff (EUMS) and the European Defence Agency (EDA) are working to improve EU cyber-defence capabilities' (Smeaton and Roehrig 2014, 24). The EUMS — 'working under the direction of the EU Military Committee (EUMC) and under the authority of the High Representative/Vice President (HR/VP) — is the source of collective (multi-disciplinary) military expertise within the European External Action Service' (EEAS 2016).

Since the mandates within EU institutions and bodies sometimes still largely reflect the old 'pillar system' (comprising the European Communities, the common foreign and security policy and police and judicial cooperation in criminal matters) cooperation between different actors is less easy. To enhance their cooperation, EU-level organisations — including the EDA, ENISA, Europol's European Cybercrime Centre (EC3) and CERT-EU — discuss ways to work together in the field of cybersecurity and defence (EDA 2016).

Concerning the strategic engagement of the EU with international organisations, the Council of the European Union, in its conclusions on cyberdiplomacy, has emphasised 'that many recent cyberspace

agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area'.

([8]) http://eur-lex.europa.eu/summary/glossary/mutual_defence.html (accessed 13 December 2016).

developments have taken place in different international organisations, in particular the UN, Council of Europe, OSCE, OECD, NATO, AU, OAS, ASEAN etc.' and has encouraged the EU and its Member States to prepare cyberdialogues within the framework of effective policy coordination' (Council of the European Union 2015, 11). In addition, the Council of the European Union has invited 'the Member States, the Commission and the High Representative to regularly report to the Council on the implementation of these conclusions' and has encouraged 'the regular collaboration between the competent Council preparatory bodies, in particular with the Friends of the Presidency Group on Cyber Issues, which should continue serving as a comprehensive cross-cutting forum for EU cyberpolicy coordination and cooperation' (Council of the European Union 2015, 13).

EU institutional actors should streamline security rules for the information systems used during the conduct of CSDP operations and missions.

EU institutions and bodies should act in line with their respective mandates in the field of cyberdefence and pursue closer cooperation.

EU-level organisations should coordinate efforts with international organisations.

3.1.3. Cyberspace as a separate domain of operation and application of existing law of armed conflicts

At the Wales Summit in September 2014, the Heads of State or Government participating in the meeting of the North Atlantic Council affirmed that 'cyber-defence is part of NATO's core task of collective defence'. Moreover, the Heads of State or Government participating in the meeting of the North Atlantic Council in Warsaw on 8 and 9 July 2016 clearly recognised cyberspace as a 'domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea' (NATO 2016).

While cyberspace is now fully recognised by the military as a domain of operations, the actual application of the existing law of armed conflict to the cyberdomain might raise some issues. As emphasised also by Pawlak, the 'issue of militarisation and expansion of cyber weapons is problematic given the lack of clarity on when a cyber-attack would constitute use of force under Article 2.4 of the UN Charter and the threshold for self-defence as stipulated in Article 51.3' (Pawlak 2015, 2). Sommario in his recent article about *jus in bello* in the cyberdomain, argued that 'When … threats [in cyber-space] may degenerate into an armed conflict, the exercise for international lawyers becomes that of assessing whether the existing legal framework — developed at a time when the cyber domain did not yet exist and was presumably not even thought of — offers adequate rules to protect states and individuals from the menaces of cyber warfare' (Sommario 2016).

Pawlak also observed that 'establishing in practice whether a cyber-attack constitutes an armed attack, whether it constitutes a legitimate use of force (*jus ad bellum*), and how force may be employed (*jus in bello*), remains contentious among international legal scholars and is one of many subjects being discussed by the Governmental Group of Experts working under UN auspices' (Pawlak 2015a, 6).

Indeed, some guidance on how to tackle the issue of the application of the existing law of armed conflicts to the cyberdomain can be found in the work of the UN Governmental Group of Experts as well as in the Tallinn Manual on the International Law Applicable to Cyberwarfare.

EU institutional actors together with international organisations, academia and the military and legal communities should work together to remove legal uncertainty when applying the current legal framework on armed conflicts to cyberspace, to implement such a framework and its interpretation and provide guidance thereto.

3.1.4. Hybrid technologies — drones used in conflicts

The evolution of hybrid technologies today offers interconnected information systems to physical systems (cyberphysical systems). Especially in recent years, these technologies have entered massively into our everyday lives and into the military domain. With the broad range of, for example, unmanned systems, smart devices and sensors, a broad range of physical objects can become cyberphysical and subsequently raise concerns in terms of cybersecurity. It is important to retain control of physical objects by safeguarding their cybersecurity features because of the obvious damage that such objects can inflict on third parties if control is lost, as well as the obvious loss of the asset that this might entail.

The issue of applicability of law of armed conflicts is also raised with reference to some remotely controlled technologies, such as drones, which are remotely piloted aircraft systems.

Drones are used in conflicts to enhance situational awareness but they can also be equipped and used with high-precision weapons. There is still some legal uncertainty on whether the law of armed conflict apply to drones.

At the EU level, the European Parliament, in its resolution of 27 February 2014 on the use of armed drones, expressed 'its grave concern over the use of armed drones outside the international legal framework' and urged 'the EU to develop an appropriate policy response at both European and global level which upholds human rights and international humanitarian law' (European Parliament 2014).

As noted in the report submitted to the UN Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'legal uncertainty in relation to the interpretation and application of the core principles of international law governing the use of deadly force in counter-terrorism operations leaves dangerous latitude for differences of practice by States' (UN Human Rights Council 2014, 18).

A common position should be sought at EU level on the use of hybrid technologies, including drones, in armed conflicts.

3.1.5. The issue of commonly agreed definitions and taxonomy

Despite the spread of usage of words related to cyberspace, we do not yet have unanimously agreed definitions and taxonomy at either the international or EU level.

As observed indeed by Cîrlig, terms such as cyber security, cyber-attack, cyber-crime, cyber war (or warfare) and cyber terrorism have entered the public discourse; however, there is no consensus on their definitions, making it difficult to create a conceptual framework in which relations and international agreements related to cyber-space can be developed.(Cîrlig 2014, 2).

With specific reference to cyberarmed conflict, interpretation issues might arise due to a lack of terminological clarity. 'Currently there is a limited clarity over what constitutes an act of cyber war and what the appropriate response might be' (Cîrlig 2014, 2). Indeed, as noted by Osula and Rõigas, 'non-lawyers tend to speak of "cyber war" in a generic sense as encompassing all forms of hostile cyber activities conducted by or against states and use the term "cyber-attacks" as referring to any harmful cyber operations. However these terms do not formally reside in international law' (Osula and Rõigas

2016, 27) and for 'international lawyers the term "cyber war" is better rendered as "cyber armed conflict'' (Osula and Rõigas 2016, 29).

EU institutions, Member States and international organisations should work together to reach, at EU and possibly at international level, a common definition and a common taxonomy of key terms, including war/conflict-related cyberterms.

3.1.6. The number and diversity of the actors involved in cyberdefence

Several very diverse actors play important roles in the formulation of cyberpolicies at Member State, EU and international level. While most of them are governmental actors, private actors — such as industry — play key roles too.

At national level, for instance, the ministries of defence, the interior and justice, law enforcement agencies and intelligence agencies, and also universities, including research centres specialising in defence and warfare studies, normally play a role but their 'weight' in the formulation of cyberpolicies differs from Member State to Member State. In general, the 'cyberdefence centre of gravity' varies from Member State to Member State, making a coherent approach at the EU level even more challenging. Clearly, the situation is exacerbated if account is taken of the already complex set-up of mandates within EU institutions described in Section 3.1.2 above.

At international level, as emphasised in the Council conclusions on cyberdiplomacy, 'recent cyberspace developments have taken place in different international organisations, in particular the UN, Council of Europe, OSCE, OECD, NATO, AU, OAS etc.' (Council of the European Union 2015, 11). The dialogue with international partners is very important and, as stated in the EU cybersecurity strategy, is one of the key activities for developing cyberdefence policy and capabilities related to the framework of the CSDP (European Commission and High Representative of the EU for Foreign Affairs and Security Policy 2013, 12). This is the reason why, in order to address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field' (European Commission and High Representative of the EU for Foreign Affairs and Security Policy 2013, 15).

A list of organisations that, among others, play a relevant role in the field of policy development for cyberdefence is presented in Table 1.

ORGANISATION	ROLE
United Nations ([9]), including the UN GGE (Group of Governmental Experts) on Developments in the Field of Information and Telecommunications in the Context of International Security ([10])	The report (UN 2015) of the UN GGE, published in July 2015, inter alia, recommends some confidence-building measures and provides comments on how international law applies.
Council of Europe ([11])	Which 'helps to protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime (Council of Europe 2011) and the technical cooperation programmes on cybercrime'.
Organisation for Security and Cooperation in Europe (OSCE) ([12])	Which in March 2016 adopted the decision on 'Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies' (OSCE 2016)
Organisation for Economic Cooperation and Development (OECD) ([13])	Supporting initiatives in privacy, security, digital identity and the e-market ([14])
North Atlantic Treaty Organisation (NATO) ([15])	Including the NATO Cooperative Cyber-Defence Centre of Excellence (CCDCoE) ([16]): 'Viewed very simply, NATO's cyberdefence role may be split into two broad themes … The first priority is the protection of its own networks, as agreed by Allies at the NATO Summit in Wales in 2014 (NATO 2014). NATO's second priority is to assist its members in developing their own cyberdefence capabilities and capacity (N. Robinson 2016). The European Union and NATO have signed a technical Arrangement between the NATO Computer Incident Response Capability (NCIRC) and the CERT-EU (NATO 2016)

([9]) UN website: http://www.un.org/en/index.html (accessed: 29 November 2016).

([10]) For more information on the UN GGE and on developments in the field of information and telecommunications in the context of international security see https://www.un.org/disarmament/topics/informationsecurity/ (accessed: 5 December 2016).

([11]) Council of Europe page related to action against cybercrime: https://www.coe.int/en/web/cybercrime (accessed: 18 January 2017).

([12]) OSCE website; http://www.osce.org/ (accessed: 18 January 2017).

([13]) OECD website: http://www.oecd.org/ (accessed: 9 January 2017).

([14]) http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm (accessed 20 January 2017).

([15]) NATO website: http://www.nato.int/nato-welcome/index.html (accessed 5 December 2016).

([16]) CCDCoE website: https://ccdcoe.org/index.html (accessed: 5 December 2016).

African Union (AU) ([17])	Adopting a cybersecurity and data protection framework ([18])
Organisation of American States (OAS) ([19])	Assisting American states to develop cybercapacities ([20])
Association of South-East Asian Nations (ASEAN) ([21])	Focusing on cybersecurity capacity and confidence-building actions ([22])

Table 1: Examples of international organisations with an active role in cybersecurity

In addition, cooperation with third countries is very important. For instance, cooperation with the United States is developing further, notably in the context of the EU–US Working Group on Cyber Security and Cyber Crime (European Commission and High Representative of the EU for Foreign Affairs and Security Policy 2013, 15). Due to the fact that criminal networks often operate in several jurisdictions, or receive support from third country governments, and that some cyber-attacks might pose a serious threat to a state's security — potentially resulting in a military conflict — a transatlantic discussion about secure and safe cyber-space necessarily involves both diplomats and military staff' (Pawlak 2016, 7).

Also 'the private sector is a key player in cyber-space. Technological innovations and expertise from the private sector are crucial [for instance] to enable NATO and Allied countries to mount an effective cyber-defence' (NATO 2016). Industry is the main supplier of hardware and software used by the military staff, also for operations. This is the reason why NATO launched the Industry Cyber Partnership (NATO 2014). In addition, as highlighted by McKay, Neutze, Nicholas and Sullivan, industry contributes to minimise 'the possibility and potential impacts of cyber conflict … by leveraging rigorous processes, tooling and training to securely develop, operate and maintain ICT products and services'; moreover, the private sector can also play a role in determining 'how it can best counter the proliferation of cyber weapons and limit their impact' (McKay, et al. 2015, 15).

Furthermore, cooperation between the military and industry and academia is essential for the development of cyberdefence technology to face new cyberthreats and 'information-sharing activities and exercises, education and training are just a few examples of areas in which NATO [and other military forces] and industry have been working together' (NATO 2016).

Finally, CSIRTs from the private sector also play an important role: information and expertise from national and governmental CSIRTs but also from other CSIRTs including those from the private sector are of undoubted value when responding to cyberattacks, including those that might be part of an armed conflict.

([17]) AU website: http://www.au.int/en/ (accessed 5 December 2016).

([18]) https://www.accessnow.org/african-union-adopts-framework-on-cybersecurity-and-data-protection/ (accessed 19 January 2017).

([19]) OAS website: http://www.oas.org/en/ (accessed 29 November 2016).

([20]) https://www.sites.oas.org/cyber/en/pages/default.aspx (accessed 18 January 2017).

([21]) ASEAN website: http://asean.org (accessed 29 November 2016).

([22]) https://ccdcoe.org/asean-focus-cybersecurity-capacity-and-confidence-building-2017.html (accessed 18 January 2017).

The presence of several diverse actors playing important roles in cyberdefence might lead to overlaps, duplication of work and a non-coherent approach, across different EU Member States and internationally, towards the way in which cyberpolicies are discussed, assigned and formulated.

EU and international partners should exploit synergies and work more closely in the field of cyberdefence.

The public and private sectors alike should exploit synergies and work more closely to further develop cyberdefence technologies and enhance cyberdefence in general.

3.1.7. Military and civilian overlaps in cyberdefence — a blurry borderline

As observed by Lyngaas, there is a 'thin line between military and civilian cyber-defence' and cyberdefence has both military and civilian dimensions. This means that, because 'threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be further enhanced' and 'European military and civil cyber security stakeholders will have to work much closer together' (Lyngaas 2015, 57).

Cyberdefence policies should be shaped in the light of this dual nature, military and civilian, of cyberdefence. However, this might represent a challenge: on the one hand, closer military and civilian cooperation should be enhanced, on the other hand cyberdefence policies should clearly define roles and responsibilities of military and civilian actors.

EU civilian and military cyberauthorities should further identify and exploit synergies as well as seeking to promote cooperation.

3.1.8. The limited availability of updated and reliable data to support policy development

The success of policymaking relies greatly on the available data to support it. Indeed, as stated by Banks, 'Ideally, we need systems that are informed by evidence at each stage of policy development, from when an issue is first identified, to the development of the most appropriate response, and subsequent evaluation of its effectiveness. This is even more important when dealing with complex problems' (Banks 2009).

Unfortunately, we do not have much data currently in the field of cyberdefence and their quality, in particular, is not always high. This is due partially to the challenges mentioned above (e.g. clarity about definitions) but also to the fact that some data might be covered by military secrets and that the data that we have is not always collected in a scientific way (e.g. because of use of uncontrolled variables, lack of control experiment and no statistical checking).

EU institutions and Member States should make efforts to collect current and reliable data to support policy development in cyberdefence.

3.2. Cybernorms

A norm can be perceived as a standard, model or pattern and is based on high-level principles. It can carry a legally binding obligation, i.e. treaties, or can act as points of reference for expected behaviour. Over the last two decades a new domain has evolved — 'cyberspace' and 'cybernorms' or cyber 'norms of behaviour' are regarded as the most suitable vehicles for guiding states' behaviour in this new domain (Osula and Rõigas, 11). Currently the norm in cyberspace is moving towards an expectation of risk and a number of cyberattacks within the EU Member States and beyond. Governments, organisations and individuals accept that they will face a number of cyberattacks annually and decide to focus on enhancing their cybersecurity capacity and resilience in order to be able to defend against large-scale attacks. Within the EU, apart from the cybersecurity strategy 'An open, safe and secure cyberspace', the NIS directive is the first piece of EU legislation specifically aimed at improving cybersecurity and represents a very significant step in the approach of establishing regulatory baselines at Union level.

To understand modern cyberattacks, it is no longer possible to consider only the technological level. It is also essential to consider all aspects of cyberspace and the threats generated within it. This model is underpinned by three assumptions, namely the need to do the following.

1. Consider cyberattacks holistically. Attacks are no longer only technical, and must be treated as such. Some properties will be measurable, but other aspects will be close to impossible to establish (such as attribution or motives).

2. Involve a broad spectrum of stakeholders when considering a cyberattack. Attacks are best understood when stakeholders are able to communicate effectively amongst each other and make a decision collectively. While this may not always be the case, it is nevertheless important to involve all parties.

3. Establish a shared understanding. As attacks will consist of properties that relate to a variety of different fields (not just technical), it is important to establish a common perspective about what has happened. It is important to identify the knowledge gaps between each expert in order that they can be removed and thus enable better decision-making (Happa and Fairclough 2017).

What seems to be missing currently when it comes to norms in cyberspace is a uniform approach to what is a norm, what are the principal aspects influencing the emergence of norms and what is their source of authority. States and international organisations play a key role in developing norms. The role of the states is prominent also in implementing and enforcing cybernorms. Especially for norms in relation to cyberdefence and the security domain, the states have an important role to play.

Of course, we need to emphasise the different types of cybernorms. Often we speak about positive norms, which tend to guide a desirable or appropriate behaviour online ([23]), and negative norms, which control undesirable behaviour. Equally, offensive norms guide the conduct of offensive operations in cyberspace while defensive norms encourage defensive behaviour ([24]).

3.2.1. Technological innovation and the need for cybernorms

There have been numerous technology innovations accompanying cyberspace, particularly in the form of devices, applications and services. The Internet of Things, for instance, has already started to make

([23]) Microsoft, 'International cybersecurity norms: Reducing conflict in an internet-dependent world', 2015 (https://blogs.microsoft.com/microsoftsecure/2014/12/03/proposed-Cyber security-norms/).

([24]) Microsoft, 'From articulation to implementation: Enabling progress on cybersecurity norms', 2016 (https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cyber security-Norms_vFinal.pdf).

its mark and is predicted by many to herald the next significant paradigm shift in technology. In addition, omnipresent social media, especially media-sharing platforms, chat sites, web forums and blogs, is radically changing the way current societies operate. Through these innovations, there is a wealth of online crowdsourced (un-)structured information. Through the use of credibility and trustworthiness metrics, this information could be appropriately analysed and used for insight and intelligence.

There have been multiple attempts to characterise quality, credibility and trustworthiness metrics within social media (Nurse, et al. 2014). Some of these focus on the data itself and engage in assessments of the data's characteristics (e.g. provenance, timeliness, source, reputation, corroboration). A part of this would involve the calibration of metrics to cyberdefence and further exploration of how such metrics could be best applied. Other issues to consider at this stage, in particular, relate to the ethics of data gathering and how use of the data is such that it does not impinge on the General Data Protection Regulation or any other EU regulations.

In closing, we as a European society are presented with a great deal of opportunities through the right use of crowdsourced intelligence and metrics that allow its quality and trustworthiness to be judged. It is critical that we make use of current and future technological innovations in these areas to benefit society. However, we should also ensure that appropriate mechanisms (policy, industrial and academic) are set up to make the best use of the opportunities presented and also to avoid the potential perils that accompany their use. This touches in particular, on the spaces of emergency response (and, for example, integrating crowd-sourced intelligence) and defence in the cyber-realm.

The EU should work with a densely instantiated and structured policy-driven method to incorporate information and intelligence from crowd-sourced information.

3.2.2. International efforts on cybernorms and the role of the European Union

The 2015 GGE report ([25]) listed four positive norms:

- protection of Critical National Infrastructure (CNI);
- prevention of cyberweapon proliferation (using the Wassenaar regime ([26]));
- management of critical ICT vulnerabilities;
- assistance to victim states when attacked.

It has to be mentioned though that all of these are 'attribution agnostic'. 'Attribution agnostic' 'refers to the development of security mechanisms that do not rely on attribution to levy deterrent effects, increase threat-actor risk or deliver punitive measures. It follows that the anonymous nature of the internet implies that cyberdefenders must stop attempting to achieve attribution and instead focus on gaining a thorough understanding of the organisations they are trying to defend; only then can they engage and counter nefarious tactics that are likely to be used against the defenders' (Rivera and Hare, 101).

([25]) http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

([26]) The Wassenaar Arrangement has been established between several states in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists. More information: http://www.wassenaar.org/

There are also a number of norms relating to the relationship between the private sector and states. Generally, the private sector is seen as having the responsibility for the so-called 'security by design' methodology to ensure usable and secure products. This responsibility however brings up aspects of liability caused by malfunctioning of the aforementioned products. Even if the objective should be conformity with description or quality/fitness for purpose, the transition towards 'attribution agnostic' security mechanisms introduces limitations on obtaining coverage and increases their exposure.

The principle of security by design should be adopted in CSDP procurement equipment, while also addressing liability and supply chain integrity provisions.

Moreover, critical national infrastructure has often been the responsibility of industry or/and the state and that can cause confusion over who is leading the protection of the infrastructure. There are many norm proposals from governments, the private sector, academia and civil society addressing a range of challenges caused by exploitation of information and communications technology systems. Most norm proposals from governments and international organisations describe the need for states to prevent malicious cyberactivity emanating from their territory and that critical infrastructures should not be targeted by cyberattacks in times of peace. However, the need for public–private sector collaboration is not recognised as a norm.

States benefit from cooperating with non-state actors when it comes to governing the normative processes. Norms in cyberspace require cooperation between all state and non-state actors, such as governments, industry, academia and civil society. The level and quality of intervention of each of those stakeholders can certainly influence the norms in cyberspace. Until now, that kind of cooperation has usually been agreed informally in the form of PPPs.

Even though many governments have acknowledged that international law applies to the internet, such laws are static and binding and do not necessarily address new cyberspace scenarios. Stakeholders in cyberspace advocate for the development and implementation of norms. A UN report (2013) ([27]) further underlines that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'. Member States should cooperate in implementing the mentioned norms and principles of responsible behaviour.

As already pointed out and suggested (Drent, Homan and Zandee, 9), the European Union should play an important role in setting and discussing norms in cyberspace: it should actively contribute to the efforts of international organisations and invest resources to identify and promote examples of norms in cyberspace.

([27]) UN General Assembly, Resolution A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013 (http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98) (accessed: 20 January 2017).

3.2.3. Confidence-building measures

Confidence-building measures (CBMs) aim to prevent or reduce risks of conflict by reducing or eliminating causes of mistrust, misunderstanding and miscalculation between states ([28]). The primary focus of CBMs is that exchange of information about military doctrines and resources contributes to stability by enhancing situational awareness and building common understanding. CBMs are one of the key mechanisms in the international community's toolbox aimed at preventing or reducing the risk of an incident by eliminating the causes of mistrust and miscalculation between states. Such measures serve as tools for ensuring that states have the same understanding of the normative commitments they make and that they respect them. Consequently, CBMs in cyberspace quickly became an element in the debates at the global and regional levels. The international strategy for cyberspace of the White House (2011) ([29]) also stated that cyberspace cooperation needs to be promoted, 'particularly on norms of behaviour for states and cyber security, bilaterally and in a range of multilateral organisations and multinational partnerships'.

However, where attribution is important, yet still difficult, we need an arrangement of confidence-building measures. The OSCE has adopted a set of CBMs ([30]) to reduce the risks of conflict stemming from the use of ICT in 2013. The CBMs are practical, risk-reduction measures designed to enhance transparency and reduce misperception and escalation between states. They include provisions for communication- and information-sharing at the government and expert level and for the use of the OSCE as a platform for exchanging best practices, with the aim of increasing inter-state cooperation and stability. CBMs are extremely valuable in order to create an environment in which norms that are more ambitious can take hold; they are the first step towards normative development. When it comes to CBM implementation though, it becomes necessary also to think about capacity building. In order to implement CBMs we first need a systematic capacity-building programme. Capacity Building (CB) also provides the opportunity to bring about effective PPPs ([31]), which should make policy, practice and the normative framework all more coherent and durable. So, all three are essential: CBM, CB and norms.

The EU should invest in a systematic cybercapacity-building programme for technological innovation to support the confidence-building measures.

UN suggests the development of voluntary confidence-building measures to increase transparency, predictability and cooperation in the ICT environment (UN General Assembly 2013). These measures include:

- exchanging views and information on national strategies and policies, best practices, etc.;
- creating bilateral, regional and multilateral consultative frameworks for confidence building;
- enhancing sharing of information among states on ICT security incidents;

([28]) http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI%282015%29571302_EN.pdf (accessed: 20 January 2017).

([29]) 'International Strategy for Cyber-space, Prosperity, Security, and Openness in a Networked World', The White House, Washington, 2011 (https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber-space.pdf) (accessed: 20 January 2017).

([30]) http://www.osce.org/pc/109168?download=true (accessed: 17 March 2017).

([31]) https://www.enisa.europa.eu/topics/national-cyber security-strategies/ppps/public-private-partnership (accessed: 17 March 2017).

- exchanging information and communication between national computer emergency response teams;
- increasing cooperation to address incidents that could affect ICT or critical infrastructure that relies upon ICT-enabled industrial control systems;
- enhancing mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile state actions, thereby improving international security.

4. Capacity building

Building cybersecurity capacity is complex and challenging. It requires substantial efforts, including building policies, strategies, skills, legal frameworks, awareness and cooperation in both the public and the private sectors. In addition, the international cooperation and synergies are a very important factor in capacity building. The bonding element is trust and a clear view at all levels that the security of the cyberdomain is a common good.

In general terms, capacity consists of an entity's ([32]) ability to achieve its objectives and solve any problems that occur. Capacity also aims to strengthen an entity's ability to collaborate with other entities for their mutual benefit by exchanging skills and tools needed. Capacity building, therefore, can be defined as the planned development of or increase in knowledge, output, awareness, skills and other capabilities of an entity through acquisition, incentives, technology, standards, policies, training and cooperation.

4.1. Models for measuring cybercapacity

In order to be able to facilitate capacity building one has to be in position to measure it. The use of a cybersecurity capacity monitoring tool is essential; such monitoring tools are based on cybersecurity capacity models.

Cybersecurity capacity models allow for the coherent development and monitoring of cybercapacities and their maturity across different dimensions of interest. A few models have been developed for this purpose and are currently being applied internationally to monitor the capacity building of companies, organisations and even whole countries. For example, the United States NIST's cybersecurity framework is an open and coordinated process that attempts to coherently improve the country's critical infrastructure cybersecurity.

One of the most widely used general cybersecurity capacity models is the Cybersecurity Capability Maturity Model (CMM) ([33]) (GCSCC, University of Oxford 2016), developed by the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford. The model covers cybersecurity capacity building holistically. It considers the cybersecurity capacity over five dimensions:

1. devising cyberpolicy and strategy;
2. encouraging responsible cyberculture within society;
3. building cyberskills into the workforce and leadership;
4. creating effective legal and regulatory frameworks;
5. controlling risks through organisation, standards and technology.

In each of the model's dimensions there exist multiple factors, which characterise what it means to possess cybersecurity capacity; countries, regions and organisations will have varying degrees of capacity in each factor and consequently across each and every dimension. Indeed, it is possible to identify a range of levels of capacity capability that might be attained. The main objective is to identify these levels in a cybersecurity capacity maturity model — whereby the lowest level would imply a non-existent or limited level of capacity, and the highest level both a strategic approach and an ability to optimise against environmental considerations (operational, threat, socio-technical and political). At the time of writing this report, the CMM had already been applied to more than 45 countries across the globe.

([32]) Where an 'entity' can be an individual, a company, an organisation, a country or a coalition.

([33]) CMM resource site at: https://www.sbs.ox.ac.uk/cyber security-capacity/content/front (accessed: 17 March 2017).

The CMM model is used further in this study in Chapter 5 in order to facilitate cybercapacity-building proposals in the context of the CSDP.

A capacity maturity model, such as the CMM, should be considered for developing and monitoring cybersecurity capacities in the context of the CSDP.

4.2. Capacity building in the European Union

The increase in cyberthreats and the perception of cyber insecurity is causing a growing mistrust among citizens, potentially holding back the European economy as it increasingly becomes digital. Recognising its key importance to the growth of the EU's digital economy, cybersecurity forms a key component in the digital single market (DSM) strategy for Europe (European Commission 2015).

The DSM strategy recognises the need to protect the EU's communication networks and critical infrastructure and respond effectively to cyberthreats, and the need to build on existing national and EU-level cybersecurity strategies and regulation. The DSM strategy reiterated the EU's 2013 cybersecurity strategy (European Commission 2013).

The aim of the EU's cybersecurity strategy is to establish common minimum requirements for network and information security among the Member States; to set up coordinated prevention, detection, mitigation and response mechanisms; and to improve the preparedness and engagement of the private sector. The strategy seeks to stimulate demand for effective NIS ICT products and to certify these products by establishing a platform to identify good cybersecurity and by developing security standards for cloud computing.

In particular, the DSM strategy also highlighted one of the key priorities of the cybersecurity strategy, which is to develop industrial and technological resources for cybersecurity, acknowledging that gaps exist between the rapid development of technologies and solutions for online network security. It calls for 'a more joined-up approach … to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities and citizens'.

The directive on security of network and information systems ('NIS directive') ([34]) represents the first EU-wide rules on cybersecurity. The objective of the directive is to achieve a high common level of security of network and information systems within the EU, by means of:

- improved cybersecurity capabilities at national level;
- increased EU-level cooperation;
- risk management, baseline security measures and incident reporting obligations for operators of essential services and digital service providers.

The NIS directive applies to organisations that provide elements of a country's critical national infrastructure — i.e. operators in energy, transport, health and banking — requiring them to report cybersecurity breaches promptly. The new directive and the GDPR are both elements of compliance rules, which will come into full effect in May 2018.

([34]) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (accessed : 17 March 2017).

4.2.1. Capacity building and cybersecurity strategies

To meet current and emerging cybersecurity threats, it is essential to develop and constantly improve a cybersecurity strategy (CSS). A CSS includes the strategic principles, guidelines and objectives and in some cases specific measures to mitigate risk associated with cybersecurity. Following a high-level top-down approach, national-level cybersecurity strategies set the main directions for subsequent actions to enhance cybersecurity within a country.

Currently 25 of the 28 EU Member States either already have in place or are in the process of drafting a national cybersecurity strategy. Therefore, the cybersecurity maturity varies in the EU. Also in some cases the focus and the objectives vary from country to country; for example, some countries focus more on fostering economic growth and business prosperity whereas other countries put the emphasis on fighting cybercrime and building strong cyberdefence programmes.

Some of the most common objectives included in a national cybersecurity strategy include the following:

- develop national cybercontingency plans;
- protect critical information infrastructure;
- organise cybersecurity exercises;
- establish baseline security measures;
- establish incident reporting mechanisms;
- raise user awareness;
- foster research and development;
- strengthen training and educational programmes;
- establish an incident response capability;
- address cybercrime;
- engage in international cooperation;
- establish a public–private partnership;
- balance security with privacy;
- institutionalise cooperation between public agencies;
- provide incentives for the private sector to invest in security measures.

Figure 1: National cybersecurity strategies in the EU

Source: ENISA ([35]).

At the national level, the United Kingdom recently published its national cybersecurity strategy for 2016-2021 (HM Government, UK 2016) to promote cooperation between states and claims that good cybersecurity practice is also in the interest of the United Kingdom's collective security. The implementation plan of the strategy defines capacity building under five pillars:

- **defend**: aims to ensure that national networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyberattacks;
- **deter**: aims to build and enhance the available tools and instruments in order to increase the country's deterrence capability;
- **develop**: sets out the rules for acquiring tools and capabilities for the country to protect itself from cyberattacks;
- **international cooperation**: sets out the importance of the United Kingdom's cooperation with international partners;
- **metrics**: points out the importance of cybersecurity metrics, measurements and calibrated data that would help to assess the level of success of the strategy.

In another national effort, the E-Governance Academy in Estonia is in the process of creating the National Cyber Security Index (NCSI) ([36]). The NCSI is a global index that measures countries' NCSI preparedness to prevent the realisation of fundamental cyberthreats and their readiness to manage cyberincidents, crimes and large-scale cybercrises. It focuses on the aspects of national cybersecurity that are clearly measurable such as:

- legislation in force (input);
- established units (input);

([35]) National cybersecurity strategies map, ENISA (https://www.enisa.europa.eu/topics/national-cyber security-strategies/ncss-map) (accessed: 15 March 2017).

([36]) http://ncsi.ega.ee/methodology/ (accessed: 15 March 2017).

- cooperation (input);
- outcomes of units or processes (output), such as:
  - policies,
  - exercises,
  - portals,
  - programmes,
  - technologies, etc.

The Software Alliance (BSA) has created the EU cybersecurity dashboard ([37]) illustrating the cybersecurity landscape and based on a set of criteria highlighting the key cybersecurity legislation and policy, as well as the main entities currently operating within each jurisdiction. In particular, the dashboard covers:

- legal foundations for cybersecurity;
- operational capabilities;
- public–private partnerships;
- sector-specific cybersecurity plans;
- education.

Designing and implementing a national cybersecurity strategy is not an easy task. From inception until the official publication, the governing body and relative stakeholders have achieved some important milestones in different areas (ENISA 2016).

In the next sections, we will highlight the most important areas, which are important prerequisites for developing an effective national strategy and consequently helping capacity building.

4.2.2. Cooperation between public stakeholders

Establishing effective cooperation between stakeholders is one of the major challenges the countries are facing during the implementation of their national cybersecurity strategies. In many cases, cooperation in the area of cybersecurity is new for some public-sector stakeholders and requires a behavioural change. Major challenges for cooperation are different interests and competencies among the relevant public stakeholders. In addition, the problem is often caused or compounded by the lack of a clear governance structure.

The EU Council has recognised cyberdefence as a priority for capability development. Moreover, cyberspace is now widely recognised by the military as the fifth operational domain besides land, sea, air and space. The EU cybersecurity strategy also identifies as one of its important aspects the promotion of civil–military cooperation and dialogue at all levels. This cooperation is of primary importance in order to build national cybersecurity capacity.

Now more than ever before it is recognised that in the rapidly evolving cyberthreat landscape, it may not be possible to establish, maintain and use a cyberdefence capability effectively without cooperation. Cooperation, and sharing development costs, is essential.

The cooperation between public-sector stakeholders, in particular between the civilian and military, should be encouraged and promoted.

([37]) http://Cyber security.bsa.org/countries.html (accessed: 15 March 2017).

4.2.3. Trust building

A prerequisite for cooperation, and therefore for effective capacity building, is the existence of trust. Trust building between the different stakeholders, from both public and private sectors, is therefore essential for efficient capacity building.

Trust can be one of the biggest obstacles to enhanced and effective communication between different stakeholders. Trust issues between public and private stakeholders have been identified by many countries as one of the main obstacles in the implementation of core objectives of a cybersecurity strategy, such as the establishment of baseline security requirements, incident reporting or establishing public–private partnerships.

Lack of trust between stakeholders can even lead to lack of sharing of security incident information. This can lead to a vicious circle: if no one reports cybersecurity incidents, then it is impossible to know the current cyberthreat situation. Such lack of knowledge would make it impossible to increase cybersecurity. This component is of vital importance for both cooperation and information sharing.

Trust-building measures should be organised continuously, as trust is a process and not a state.

The building of trust requires extensive dialogue as well as considerable time and effort. Trust-building activities, such as workshops, informal meetings and common projects, are essential for capacity building.

Trust can also be achieved through public–private partnerships, which can play a very significant role. They can help to enhance trust through the high frequency of contact between counterpart individuals and the identification and sharing of common intentions and objectives or credibility between the technical staff.

The Information Sharing Framework (ISF) from the Multi-national Alliance for Collaborative Cyber Situational Awareness (MACSSA 2013) indicates that trust depends on an AAA model: authentication (are you who you claim you are?), authorisation (do you have permission to undertake the activities?) and accountability (can you evidence compliance in any court of law?).

The EU should invest in activities that promote the establishment of trust between all stakeholders involved in cybersecurity.

4.2.4. Resourcing

One of the most important factors in building cybercapacities across Europe is the availability of the needed resources, ranging from the limited numbers of competent cyberprofessionals up to the lack of appropriate infrastructures.

The lack of resources varies and depends on the priorities set in the national strategy, most importantly on the actual economic strength. Cybersecurity public authorities in the EU have identified the lack of

funding and financial resources as a problem for the implementation of measures despite the fact that public spending for cybercapacities is trending upwards at the EU level ([38]).

Regarding human resources, the problem mainly relies on the availability of skilled personnel and the unequal benefits that skilled personnel receive when employed in the private sector ([39]) versus the public sector. The latter needs to consider alternative offerings in order to attract cyberprofessionals. Therefore, widening the cybersecurity focus in higher education, as well as offering continuous professional development through training and exercises, is vital. The knowledge and expertise of people in this domain is a fundamental requirement for cybersecurity capacity.

The EU should ensure appropriate resources for cybersecurity capacity building and continue investing in cybersecurity, while at the same time supporting education, training and career path development.

4.2.5. Common approach for cybersecurity and privacy

The lack of a common approach to security and privacy has been identified as a major obstacle by countries whose strategy is focused around the growth of the digital market. A joint approach regarding the flow of data inside the EU and the confidentiality of communication of citizens and business is essential.

Gaining awareness about information security proves difficult in many cases, in which the public perceives security as intrusive surveillance and an unwanted intrusion into personal rights and liberties. This can lead to a lack of understanding of the crosscutting nature of digital services and the pervasiveness of cybersecurity, resulting in insufficient cooperation and coordination between the national data protection and information security authorities.

The private sector should be engaged in capacity-building activities such as training, education and awareness as well as operational capacities such as intelligence, analysis and response.

4.2.6. Risk analysis

The implementation of vulnerability, threat and general risk analysis is a very important prerequisite for capacity building. One needs first to understand the threat landscape and the risks for which the appropriate strategic priorities, and consequently capacities, need to be developed.

Classical risk analysis methods can be challenging though, both resource- and finance-wise, due to the complexity and the volume of information that needs to be analysed. Therefore, risk analysis has to be a focused approach and the scope needs to be chosen carefully; otherwise, the design could be too comprehensive and cover too many risk areas. An example of how to achieve this is by going for scenario-driven risk assessments instead of a full-scale integral risk analysis (ENISA 2013).

Good practices and guidelines should be adopted for the development of coherent vulnerability and threat assessment and risk analysis.

([38]) http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber security-strategy/ (accessed: 17 March 2017).

([39]) http://work.chron.com/Cyber security-jobs-public-vs-private-sector-30284.html (accessed: 17 March 2017).

4.2.7. Contribution from the private sector

The role of the private sector can generally be divided into two categories:

- **capacity building** through training and awareness raising with policymakers and other stakeholders;
- **operational collaboration** through developing highly secure technology, sharing best practices and facilitating a multiple stakeholder response to assist in preventing, identifying and responding to cyberthreats.

The private sector can provide technical expertise on a wide range of cybersecurity challenges. For example, private companies can help to measure and reduce cybersecurity risks, protect critical infrastructures, provide forensic support and cyberthreat intelligence, offer incident response and work with policy experts to amend and revise effective national strategies and regulations. In addition, the private sector delivers, in whole or in part, many of the critical services on which society depends. Accordingly, discussions on protecting the most sensitive and vital functions from offensive cyberactivities must necessarily involve the private sector to determine the infrastructure that supports those functions. In addition, the ICT industry can actively help in tracking, recording and responsibly disclosing vulnerabilities.

The private sector should share information in order to help counter the proliferation of cyberattacks and limit their impact. This can be accomplished through the exchange of information between affected entities. For example, to help protect their customers, software vendors can share information on new and suspected attacks. This collaboration should begin when an event is detected and continue until the associated risk has been appropriately managed. Similarly, software providers, security researchers, law enforcement, internet service providers (ISPs) and CSIRTs can engage in coordinated efforts to eradicate specific strains of malware by combining legal and technical measures.

The private sector should be engaged in capacity-building activities such as training, education and awareness as well as operational capacities such as intelligence, analysis and response.

4.2.8. Public–private partnerships

One important element to promote the active contribution of the private sector to national and EU cybersecurity is through cooperation with the public authorities in the form of PPPs. PPPs are considered an effective tool to ensure close cooperation between public and private stakeholders across different issues.

Around 12 EU Member States are currently using this instrument to incentivise the private sector to contribute to the protection of critical infrastructures. A good example is the UP KRITIS PPP in Germany ([40]), a national initiative between the state and local carriers for the protection of critical information infrastructures in Germany. The latter are the organisational and physical structures and facilities that are of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

At the EU level, the European Commission also considered PPPs as important tools in its 'Communication on strengthening Europe's cyber-resilience system and fostering a competitive and

([40]) http://www.kritis.bund.de/EN/Topics/CriticalInfrastructureProtection/GeneralInformation/generalinformation_node.html (accessed: 17 March 2017).

innovative cybersecurity industry' (European Commission 2016). An EU PPP is seen as one of the key activities for protecting the EU against cyberattacks covering multiple aspects, such as supporting EU NIS research, developments and innovation for increased competitiveness, prompting European cooperation for sectoral information sharing and analysis centres (sectoral ISACs) and removing barriers that prevent market participants from sharing event information.

Recently the European Commission announced (European Commission 2016) a plan to establish a public–private partnership on cybersecurity (cPPP) in the area of technologies and solutions for online network security, which was launched in July 2016 ([41]).

The EU should sponsor the development of private–public partnerships for cybersecurity.

4.3. Efforts in capacity building beyond the EU

The EU is closely engaged in international cooperation for cybersecurity. There are a number of multilateral initiatives addressing cybersecurity, such as the work of the Council of Europe, the UN, the Organisation for Economic Cooperation and Development (OECD), the Organisation for Security and Cooperation in Europe (OSCE) and NATO ([42]). These organisations have recognised the breadth and complexity of the cybersecurity challenge and that their response to the cybersecurity challenge can be but one part of the whole.

The EU is active in an EU–US Working Group on Cybersecurity and Cybercrime, as well as in other multilateral fora, such as the OECD, the United Nations General Assembly (UNGA), the International Telecommunication Union (ITU), the OSCE, the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF).

4.3.1. Council of Europe

The Council of Europe (CoE) has launched the 'Action against Cybercrime' ([43]). This helps to protect societies worldwide from the threat of cybercrime through related acts like the agreement on a Convention on Cybercrime (Council of Europe 2011). Within the CoE, the Cybercrime Convention Committee (T-CY) represents the State Parties to the Budapest Convention on Cybercrime, aiming at facilitating the effective use and implementation of the convention, the exchange of information and consideration of any future amendments. The high-level approach of the CoE is illustrated in Figure 2.

([41]) http://europa.eu/rapid/press-release_IP-16-2321_en.htm (accessed: 17 January 2017).

([42]) NATO is covered in Section 5.

([43]) https://www.coe.int/en/web/cybercrime (accessed: 23 March 2017).

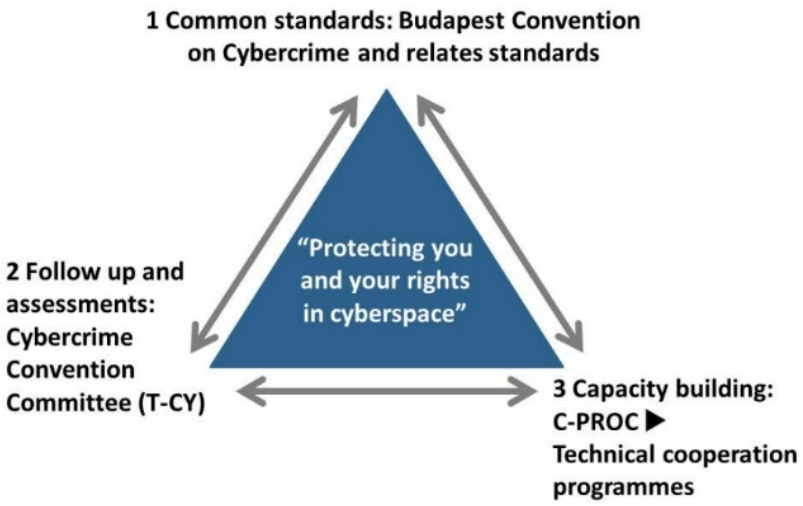

Figure 2: Council of Europe approach to protection in cyberspace

Source: CoE ([44])

The approach is based on three pillars: common standards, to close follow-up and regular assessment of them and capacity building. The Cybercrime Programme Office of the Council of Europe (C-PROC) is the capacity-building function that complements the work of the Cybercrime Convention Committee (T-CY). C-PROC is responsible for assisting countries worldwide in strengthening their legal systems' capacity to respond to the challenges posed by cybercrime and electronic evidence based on standards. In particular, it supports:

- strengthening legislation on cybercrime and electronic evidence in line with rule of law and human rights (including data protection) standards;
- training judges, prosecutors and law enforcement officers;
- establishing specialised cybercrime and forensic units and improving interagency cooperation;
- promoting public–private cooperation;
- protecting children against sexual violence online;
- enhancing the effectiveness of international cooperation.

4.3.2. Other international cybercapacity-building initiatives

Cybersecurity maturity is dependent on many factors, such as necessary skills, support by government, funding, use of information communication technologies, etc. Today, an increasing number of countries develop national cybersecurity strategies with the assistance of specific initiatives of large organisations (OECD, ITU, ISACA, etc.). A list of the countries across the world having developed a national cybersecurity strategy is presented by the ITU ([45]).

([44]) https://www.coe.int/en/web/cybercrime (accessed: 23 March 2017).

([45]) http://www.itu.int/en/ITU-D/Cyber security/Pages/National-Strategies-repository.aspx__(accessed: 17 January 2017).

The ITU has worked on the Global Cybersecurity Index ([46]), an initiative that measures the commitment of countries to cybersecurity. It includes legal measures, technical measures, organisational measures and capacity building and cooperation. Within the scope of supporting the Nations on cybersecurity and within the framework of the global cybersecurity agenda, the ITU has already created an inventory of cyberwellness profiles per country ([47]). The cyberwellness profiles provide an overview of the countries' levels of cybersecurity development based on the five pillars of the global cybersecurity agenda — namely, legal measures, technical measures, organisation measures, capacity building and cooperation.

The OECD conducted a survey among its members that resulted in a report (OECD, Working Party on Information Security and Privacy 2005) whose main findings include the importance of international cooperation for fostering a culture of security and the role of regional facilitating interactions and exchanges. International cooperation is consolidated in the area of cybercrime and CSIRTs.

The World Economic Forum (WEF) has published the 'Global Information Technology Report 2016', which assesses the state of networked readiness of 139 economies using the Networked Readiness Index (NRI) and, as part of the theme 'Innovating in the digital economy', examines the role of ICT in driving innovation. It presents the detailed performance of each economy in the NRI, and rankings for each of the 53 individual indicators included within it ([48]). Cybersecurity is considered to be heavily dependent on the underlying infrastructure and on countries' capabilities in general; therefore when assessing capabilities, this report can give a good overview when other sources are lacking.

([46]) http://www.itu.int/en/ITU-D/Cyber security/Pages/GCI.aspx (accessed: 17 January 2017).

([47]) http://www.itu.int/en/ITU-D/Cyber security/Pages/Country_Profiles.aspx (accessed: 17 January 2017).

([48]) http://reports.weforum.org/global-information-technology-report-2016/executive-summary/ (accessed: 17 January 2017).

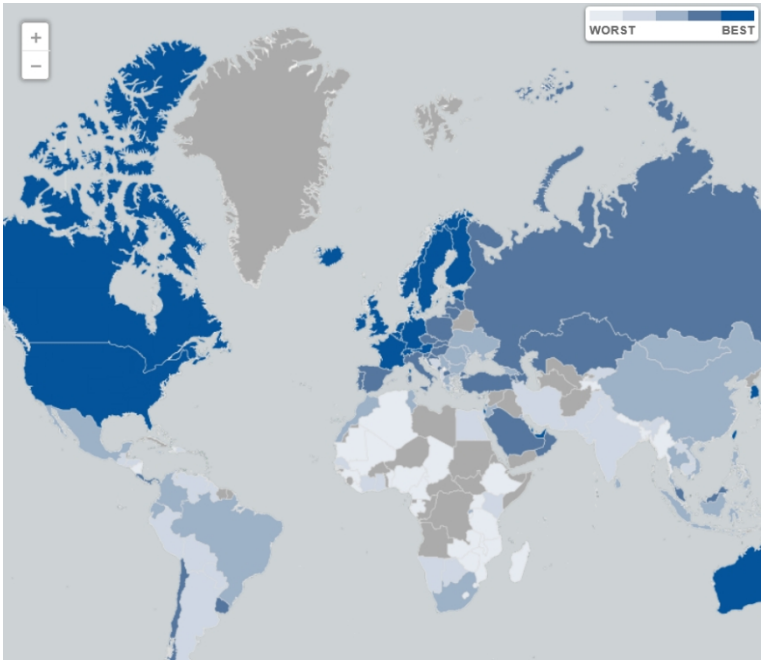

Figure 3: Networked Readiness Index 2016 ([49])

The GFCE, the Organisation of American States (OAS) and the governments of Argentina, Chile and Estonia have launched an ongoing initiative called 'Cyber Security in OAS Member States'. The project aims to build an integrated approach to cyberthreats, and includes seven work streams, covering topics such as the adoption of technical standards, crisis management exercises and best practice in e-government. One of the work streams looks at 'Access to cybersecurity expertise' ([50]) and provides assistance in the formulation, implementation and technical review of national cybersecurity policies with partners from private sector companies, public sector authorities, academia and non-profit institutions. This diverse partnership has enabled the 35 governments of the Americas to access relevant expertise through formal reports, as well as on-demand joint initiatives such as training activities, workshops and round tables. Through these activities, governments gain access to practical training in implementing the best practice presented.

Moving onto the world map, the World Bank's 'West Africa regional communications infrastructure program' (WARCIP) seeks to bridge connectivity gaps between 16 west African countries and the rest of the world, while the ASEAN broadband corridor project aims to establish areas in each ASEAN member state with high-speed internet connectivity.

4.4. Attribution of cyberattacks

Having an incident management capability is an important component in an effective response to cyberattacks. Equally important for such a capability is to be able to identify the source of the attacks, namely the perpetrators. Information obtained by national intelligence services that has a specific 'cyber' interest and an impact on CSDP missions should be analysed, evaluated and correlated with national and/or EU cybersecurity agencies in order to identify perpetrators.

([49]) http://reports.weforum.org/global-information-technology-report-2016/report-highlights/ (accessed: 6 March 2017).

([50]) https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/access-cybersecurity-expertise (accessed: 23 March 2017).

Communication of information to EU-level mechanisms like the EU-INTCEN and the CSDP OHQs/MHQs should be further developed for a safer operational environment of CSDP missions.

Regarding the analysis of actors and the threat environment, national intelligence services are usually the institutions that provide information and assessments to the analysis and reporting centres for information assurance that, together with the national intelligence services, constitute a coherent mechanism for threat awareness.

Every effort needs to be made to not only enhance this capacity but also to promote the sharing of information related to CSDP missions at the EU level.

4.4.1. Policy issues

Cyberattacks linked to cyberespionage, cybersabotage or even cyberterrorism are nowadays a common occurrence and pose a particular challenge as they are mostly conducted by states or are state sponsored. In these scenarios, the capabilities of the intelligence services have proven to be more effective than the means used by law enforcement or the military as there is no international consensus on whether these actions are considered violations of international law or an act of war.

On critical infrastructure, there is also an exponential increase of cyberattacks, especially cyberespionage and cybersabotage. The biggest policy challenges are that most of the time, perpetrators cannot be identified beyond any reasonable doubt, which in turn makes it hard to take corresponding counter-measures. Many countries, though, are increasingly adopting a more aggressive cyberstrategy against perpetrators even though evidence might not be beyond any doubt.

Most countries maintain trustworthy international partners and a solid network of cooperation, which leads to an exchange of information that in turn facilitates the evaluation and analysis of cyber incidents.

Cooperation between international intelligence services should be enhanced further as they are imperative in all efforts to attribute a cyberattack related to terrorist activities but also in the CSDP context.

4.4.2. Existing tools and methods

There are various techniques for performing attribution of computer attackers who are exploiting data networks. These techniques are constantly trying to counteract the rapid evolution of malicious techniques, tools and services like anonymisers. Attribution can be defined as 'determining the identity or location of an attacker or an attacker's intermediary'. In the public literature, 'trace back' or 'source tracking' are often used as terms instead of 'attribution'.

A large number of different attribution techniques exist. Each technique has its strengths and weaknesses; no single technique replaces all others.

Examples of attribution techniques (Wheeler and Larsen 2003) are:

- store logs and trace back queries;
- perform input debugging;
- modify transmitted messages;
- transmit separate messages (e.g. iTrace);
- reconfigure and observe network;
- query hosts;

- insert host monitor functions (e.g. 'Hack Back');
- match streams (via headers, content and/or timing);
- exploit/force attacker self-identification (e.g. beacons, web bugs, cookies, watermarking);
- observe honeypot/honeynet;
- employ forward-deployed intrusion detection systems (IDSs)
- perform filtering (e.g. Network Ingress Filtering);
- implement spoof prevention;
- secure hosts/routers;
- surveillance attacker;
- employ reverse flow;
- combined techniques.

As with any traditional investigation, the attribution attempts start with a post-mortem analysis of a cybersecurity incident. If the incident has been caused by malware, the analysis becomes the focal point of the investigation. Whenever a malware is found, the investigative process follows a similar path to the traditional crime investigation. The content and the behaviour of the malware are analysed. Indicators extracted from this kind of analysis consist of network connections established with a certain server, or the creation, deletion or modification of a specific file.

From the indicators extracted from both static and behavioural analyses, network indicators represent an important kind of evidence used by cyberinvestigators, especially the ones related to the malware Command and Control (CnC) server since the analysis of these can lead to further findings about the attacker. CnC are servers controlled by the attacker where the malware is instructed to send the stolen data and receive further instructions. Whenever network indicators are found, the analysts' interest is shifted toward uncovering further details of the CnC server. If the extracted network indicator consists of a domain name, analysts normally proceed to query the WHOIS ([51]) lookup-database in order to retrieve information about the registrant, or the individual who registered the domain name. Starting from the registrant's personal information found in the WHOIS database, the investigation could continue through open source intelligence techniques (OSINT) in order to pinpoint the registrant's real identity and location. In order to make the CnC communication effective, domain names have to resolve to an active IP address, which might be an additional pivot point for the analyst's investigation.

Although the WHOIS database can be also used for querying IP addresses, it only reveals the company that owns the IP range where the CnC address belongs. An IP range might consist of several dozens, hundreds or even thousands of different IP addresses, hence knowing which company owns a specific IP range only gives the investigator a vague piece of evidence since the company is likely to be unaware of the activity related to each of its IP addresses (Riccardi 2016). The main challenges in this area include the following.

- In most cases only the last known IP addresses can be resolved.
- Botnets are globally distributed and it is a great technical challenge to identify and analyse their command and control servers.
- Highly complex cyberespionage Trojans have been developed in order to avoid attribution.

([51]) WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912. Source: http://www.abbreviations.com/WHOIS (accessed: 17 March 2017.)

4.4.3. Improving attribution through capacity building

An important obstacle to improving attribution is the lack of financial and personal resources, as well as skilled personnel that can assist in detection, identification and defence against cyberincidents. Although a country may have the specialists mentioned below, stocking up on personnel in the following areas would greatly improve cyberattribution:

- operational forensic experts;
- technical forensic experts;
- specialists in actor analysis;
- specialists in situational cyberawareness;
- language specialists.

Cooperation between countries is another important aspect that needs attention. Information exchange and cyberthreat intelligence regarding the attribution of malicious actors threatening EU cyberspace, and CSDP missions as an extension, should be enhanced and further developed, with coordination by EU bodies and institutions.

The EU should invest in building the capacity to improve the attribution of cyberattacks and incidents.

5. Cyberdefence and the EU common security and defence policy

The cyberdomain is increasingly being recognised in the global community as a new operational domain along with air, land, sea and space. The European Commission pioneered this approach in 2013 by accepting that 'The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyberdomain' (European Commission and High Representative of the EU for Foreign Affairs and Security Policy 2013). Subsequent 'policies and actions like Directive 2013/40/EU (European Parliament and Council 2013) and the EU cyberdefence policy framework (Council of the European Union 2014) have been aligning the EU to this new reality. The CSDP is no exception, with the 'Military concept for cyberdefence' released in December 2016 by the European External Action Service (EEAS 2016).

For CSDP missions, the operationalisation of cyber should be considered as a trifold task:

- to establish a good understanding of the cyberthreat landscape for the CSDP;
- to mitigate threats to the CSDP by taking measures at the EU and Member State levels;
- to build alliances with non-EU actors that share the same moral values.

5.1. Understanding cyberthreats to the CSDP

'Peace and stability are the cornerstones upon [which] the European Union has been built. The need for a common security and defence policy is becoming more and more obvious as these two core values are attacked. The CSDP is the prerequisite to achieve peace and stability as no country alone can tackle the immense challenge we are facing today' ([52]).

The increasing use of cyberspace in the European Union and Member State realms applies naturally in CSDP missions ([53]). Command and control systems, information exchange, support and logistics rely on classified and unclassified IT infrastructures that run through the cyberdomain. The cyberdomain is a prime candidate for malicious actors aiming to cause harm to CSDP missions, as it is a cheap, hard-to-attribute and sometimes very efficient way to achieve their goals. Its use as a threat vector has expanded in recent years to include attacks on critical infrastructure and data privacy. The complexity of cyberattacks has also increased to include multi-threat vector attacks and even hybrid warfare ([54]), a blend of cyber and traditional operations, in order to achieve geopolitical goals. Moreover, these threats come on top of all other types of cyberthreats, like common cybercrime, 'hacktivism' or 'challenging' cyberdefences for fun or as a hobby.

Another characteristic of this cyberthreat landscape is that threat actors do not only target the technical or tactical layers. The cyberthreat extends all the way down from the political/strategic layer of CSDP administration to the technical/tactical layer, in a coherent (organised campaign) or non-coherent fashion (spontaneous attacks). Objectives therefore can also be geopolitical, economic and cultural.

Cyberthreats may or may not originate from the cyberdomain itself. Other domains could pose threats to the cyberdomain or the cyberdomain itself could be the threat vector against other domains. Figure 4

([52]) 'Handbook on CSDP missions and operations', foreword by the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission Federica Mogherini, ESDC, 2015.

([53]) An overview of civilian and military CSDP missions is presented at Source: http://www.iss.europa.eu/uploads/media/CSDPbasics.pdf (accessed 15 November 2016).

([54]) The term 'hybrid warfare' appeared at least as early as 2005 and was subsequently used to describe the strategy used by Hezbollah in the 2006 Lebanon War. Since then, the term 'hybrid' has dominated much of the discussion about modern and future warfare, to the point where it has been adopted by senior military leaders and promoted as a basis for modern military strategies. (Source: http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ (accessed 15 November 2016)).

presents this relationship, which has already been mentioned for the CSDP (Roehrig 2015, 193), where the 'virtual world' and its threats are associated with CSDP crisis management for the following reasons.

- Crises can be initiated or exacerbated through cyberspace.
- Crises or disasters in the physical domains can affect the regional availability of cyberspace.
- Vital and critical crisis management assets can be affected through cyberattacks.

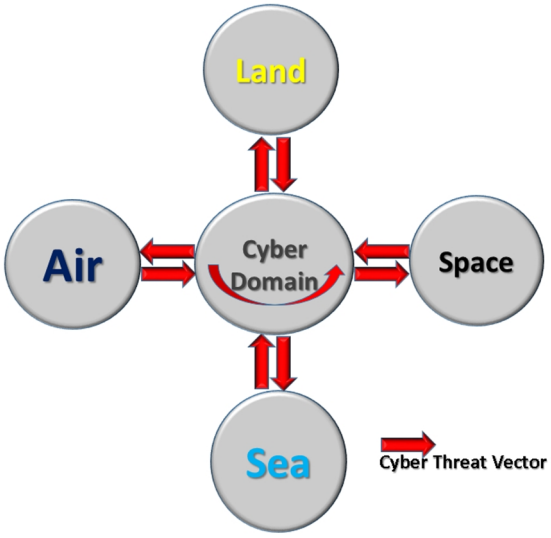

Figure 4: Cyberthreat vectors

In addition, depending on the decision layer in which the cyberthreat is examined/analysed (political, strategic, operational or tactical/technical), these threat vectors change forms. Different layers have different morphs of the threats and of the threat actors.

5.1.1. Political/strategic threat assessment

An interesting approach to cyberthreat taxonomy is presented in US Defence Science Boards work (Defence Science Board 2013). Cyberthreats are categorised in three levels, with two tiers per level as shown in Table 2. This taxonomy focuses on threat actors acting within the cyberdomain and their intentions and capabilities and applies to CSDP missions at the political, strategic and operational levels, where decision makers, generals and operational commanders need to conduct higher-level assessments of CSDP mission threats.

THREAT ORIGIN	THREAT LEVEL	CHARACTERISTIC	TIER	DEFINITION
CYBERDOMAIN	A	Exploits pre-existing known vulnerabilities	1	**Practitioners** who rely on others to develop the malicious code, delivery mechanisms and execution strategy (use known exploits).
			2	**Practitioners** with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
	B	Discovers unknown vulnerabilities	3	**Practitioners** who focus on the discovery and use of unknown malicious code are adept at installing user and kernel mode root kits ([55]), frequently use data mining tools and target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
			4	**Criminal** or **state actors** who are organised, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
	C	Creates vulnerabilities using full spectrum	5	**State actors** who create vulnerabilities through an active programme to 'influence' commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
			6	**States** with the ability to successfully execute full spectrum (cybercapabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic etc. domains and apply at scale.

Table 2: Cyberthreat taxonomy (US DoD Defence Science Board Report, 2013)

These three threat levels are directly connected to the financial capabilities of the threat actors, varying from the Euros range (Level A) to the multimillions of Euros range (Level C).

([55]) User mode toolkits involve system hooking in the user or application space. Whenever an application makes a system call, the execution of that system call follows a predetermined path and a Windows rootkit can hijack the system call at many points along that path. Kernel mode rootkits involve system hooking or modification in kernel space. Kernel space is generally off-limits to standard authorised (or unauthorised) users. One must have the appropriate rights in order to view or modify kernel memory. The kernel is an ideal place for system hooking because it is at the lowest level and thus, is the most reliable and robust method of system hooking.

5.1.2. Technical/tactical threat assessment

A complementary approach is given by ENISA (ENISA 2016). This threat taxonomy focuses on the operational and tactical/technical layers. Targeted cyberattacks may be initiated either within the cyberdomain (Categories 6, 7) or in other domains (Categories 1, 3, 8). Other (not deliberately caused) cyberthreats concern traditional Infosec (Categories 2, 4, 5). ENISA's threat taxonomy (ENISA 2016) categorises these cyberthreats into eight groups and three tiers per group, with increasing granularity. These categories are summarised in Table 3 and further explained in Annex B.

Although analysing the non-cyberdomain-originated threats is not the purpose of this section, categories (1, 2, 3, 4, 5, 8) that concern other domains and typical IT mission planning should be an integrated part of the total cybersecurity strategy and the operational planning of a CSDP mission.

	CATEGORIES	DOMAIN
1	Physical attacks (deliberate/intentional)	**Sea-land-air-space**
2	Unintentional damage/loss of information or IT assets	**Infosec**
3	Disaster (natural, environmental)	**Sea-land-air-space**
4	Failures/malfunction	**Infosec**
5	Outages	**All**
6	Eavesdropping/interception/hijacking	**Cyber**
7	Nefarious activity/abuse	**Cyber**
8	Legal	**All**

Table 3: ENISA threat taxonomy

As mentioned earlier, this approach focuses on the operational and tactical/technical layer. It describes in detail all those factors that pose a threat to the cyberdefence operations area ([56]) of a CSDP mission including threats originating from other domains. This taxonomy also includes non-human actors/factors such as environmental and physical threats where security measures might already have been taken into account in traditional Infosec policies/directives, operational contingency plans and operational directives.

5.1.3. Operating spaces

Another aspect that needs to be examined concerns the 'proximity' of a cyberthreat to CSDP mission commanders/directors. This property of cyberspace can be extremely useful for CSDP mission commanders/directors when trying to assess the importance of the threat, attribute the threat to a threat vector/actor or exercise mitigation measures. Table 4 describes operating spaces in terms of near, mid and far, based on the United Kingdom Ministry of Defence Cyber Primer threat taxonomy

([56]) A cyber defence operations area is the aggregate of communication and information networks and systems that affect the operation, regardless of their position in EU territory or federated environment or as part of the force deployment in operations abroad, as well as the portion of the cyberdomain of military and civilian interest — including its physical, logical and social dimensions — needed to guarantee unrestricted access to this domain and the adequate anticipation and response to threats or aggressions through the cyberdomain that can affect the operation. Definition provided by EEAS in its document 'EU concept on cyber defence for EU-led military operations and missions'.

(Development, Concepts and Doctrine Centre 2016). As the title of this paragraph reveals, the operating spaces classification is meant to be used (and actually makes sense) at the operational layer.

NO	PROXIMITY	CONCERNS
1	NEAR	Local networks and systems, civilian and military, controlled and assured by the CSDP mission commander/chief and considered vital for the operational objectives of the CSDP mission.
2	MID	Networks and systems, civilian and military, considered vital for the operational objectives of a CSDP mission, but not under the control and assurance of the CSDP mission commander/chief. Control and assurance relies on another EU institutional or Member State public or private authority involved in the CSDP mission.
3	FAR	Networks and systems, civilian and military, which if influenced will have an impact that will prove critical to CSDP mission objectives. Control and assurance of these networks and systems lies beyond EU institutional or Member State public or private authorities involved in the CSDP mission.

Table 4: Classification of cyberthreats per proximity

5.1.4. The importance of the operational layer

It is suggested that analysis of the cyberthreat landscape in CSDP missions use the aforementioned approach for each administration layer.

For the political and strategic layer, classification of cyberthreats should follow the process presented in Table 2 that classifies a cyberthreat to a threat category (A, B or C) and to a tier (1 to 6).

At the tactical/technical layer, the threat assessment focuses on the criteria explained in Table 3. ENISA's threat landscape and cybertaxonomy are the suggested tools for the CSDP staff at this layer to conduct threat assessments and risk analysis during planning of CSDP missions.

The operational layer faces a double challenge. Being the middle layer of CSDP administration, and the layer having direct control over CSDP missions, risk analysis needs to use both approaches explained earlier in Tables 2 and 3 in order to produce operational threat assessments, operational advice geared towards the political/strategic layer and guidance geared towards the tactical/technical layer. Operational headquarters need also to determine the distance of cyberthreats from the theatre of operations as described in paragraph 5.1.3. Fusion of all this information and the production of advice and guidance is a very challenging task for the operational layer, which needs to have sufficient skills, organisation and capabilities.

Cyberskills and capabilities at the operational layer should be further enhanced because they are essential in order to assess cyberthreats in CSDP missions.

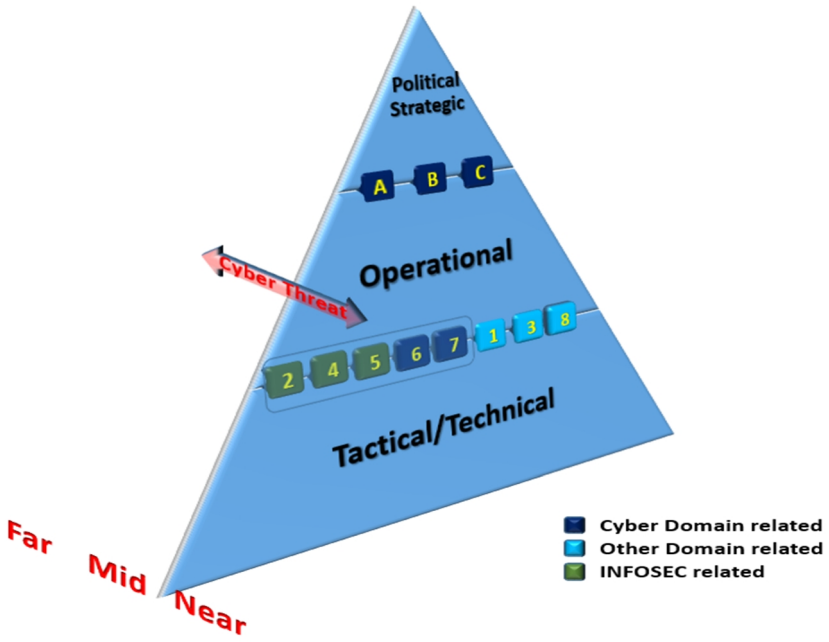

Figure 5: Cyberthreat taxonomy for the CSDP

5.1.5. Case studies

To better understand the impact that different types of cyberthreats can have on civilian and military CSDP missions, we present three different case studies of cyberattacks. Attackers and victims vary greatly in each case, but the common factor in all three attacks is geopolitical destabilisation. In the CSDP context, this is a major concern, a threat affecting directly or indirectly not only EU policies but also the EU personnel operating in military or civilian missions beyond the EU's borders. Although disclosure of details regarding cyberattacks against military or civilian operations remain classified most of the time, the events presented here are open sourced but nevertheless indicative of cyberthreats against all layers of administration.

Case study 1: Cyberattacks against Ukrainian critical infrastructure ([57])

This is a classic case (of an alleged state-sponsored cyberattack) at a theatre of military operations — a series of unscheduled electric power outages that occurred on 23 December 2015, leaving thousands of customers without electricity. After entering a SCADA (supervisory control and data acquisition) via a phishing email, the hackers took 30 electricity substations offline, damaged two power distribution platforms and removed two or three back-up power supplies to ensure the maximum duration of damage. Drives were wiped permanently with KillDisk to cover up the tracks, and passwords were changed to prevent operators from accessing control functions.

([57]) https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed 28 February 2017).

Potential risks for CSDP missions

There are several goals of this campaign:

1. Psychological operations. At the political/strategic level, this is a projection of power in an attempt to 'warn' of the attacker's capabilities, preoccupy public opinion and spread fear and a sense of insecurity among citizens.
2. Hybrid operations. At the operational level, this campaign could be a part of wider military operations to reduce the victim's military capabilities by attacking critical infrastructures ahead of kinetic attacks, or even create diversion.

In a CSDP mission context, EU personnel in a foreign country could be subject to similar threats, either against the CSDP infrastructure in the context of hybrid operations, or indirectly by being a target of psychological operations by the adversary against the country itself.

Target(s)	Three regional electric power distribution companies in Ukraine (Kyivoblenergo, Prykarpattyao-blenergo, Chernivtsioblenergo)
Type	Hybrid warfare – Denial of service – Attack against critical infrastructures
How	1. Infection of computer networks with a customised malware (Black Energy3). 2. A series of synchronised cyberattacks against circuit breakers with the use of remote administration tools (on either operating systems or industrial control systems) via remote virtual private network connections (VPN). 3. Sabotage of electrical substations by physically placing malicious devices in the network infrastructure. 4. Attacks against the uninterruptible power supplies of network servers.
Why	Military conflict between the Ukrainian and Russian armies following the annexation of Crimea by Russia.
Impact	Political – Military – Civilian: 225 000 customers (public–private sector) in Ukraine were left without electricity.

Figure 6: Case study 1 threat assessment for a fictitious CSDP mission in the region

Case study 2: Attacks against a country's political system ([58])

This is a different type of cyberattack that lasted for almost 9 years (2005-2014). Targets and victims were the political systems and politicians in many Latin American countries. The case concerns attempts by an individual attacker and its criminal group, motivated by financial profit, to influence political developments by targeting presidential campaigns in various Latin American countries, affecting election results, using blackmail and offering 'protection' through a variety of tools like website defacement, misinformation campaigns and exfiltration of personal data.

Potential risks for CSDP missions

Similar types of cybercampaigns can affect CSDP missions, especially civilian ones. In this case, we are talking about common cybercrime targeting the operational and political/strategic levels. Cybercriminals in cases such as this may harm the public profile of the mission itself, exfiltrate confidential information or sabotage the mission's goals. Motivation can be either political or financial. It is therefore essential that cybercrime considerations and mitigation procedures be taken into account in CSDP mission planning.

Target(s)	Presidential candidates and elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala and Venezuela.
Type	Attacks against availability, confidentiality and integrity – Psychological operations – propaganda – Blackmail.
How	1. Systematic defacement of presidential campaigns. 5. Smartphone hacking 6. Interception of conversations (man-in-the-middle attacks) 7. Phishing emails 8. Decryption of encrypted information 9. Malvertisement campaigns 10. Infection of computer systems 11. Cyberespionage, etc.
Why	Financial profit. Cyberoperations were conducted for money. Different packages and levels of service were available for customers.
Impact	The political impact cannot be estimated because of the duration and varieties of targets.

Figure 7: Case study 2 threat assessment for a fictitious CSDP mission in the region

([58]) https://www.bloomberg.com/features/2016-how-to-hack-an-election/ (accessed: 28 February 2017).

Case study 3: Cybermeans in the service of military operations ([59])

The last case study is an example of cyberactors directly threatening military operations. On 6 September 2007, the Syrian Air Defence failed to identify incoming hostile aircraft. Syrian long-range radars ceased to transmit, allowing the successful Israeli penetration of Syrian air space and bombing of the Dayr-as Zawr nuclear facility. This is one of the first known attacks using a blended mix of cyberassets and electronic warfare to deny services of military systems.

Potential risks for CSDP missions

This case study concerns possible direct cyberattacks against military CSDP missions. In this case, the target was military infrastructure, surveillance, command and control, communication and defence systems. As the offensive use of cyberspace is being integrated into national cyberstrategies and capabilities of an increasing number of countries worldwide (Cîrlig 2014, 4,5,6), CSDP military missions need to be able to self-defend their military assets against threats that originate from the cyberdomain. Since these capabilities work at the service of conventional warfare operations, the consequences beyond being only military, political or economic may also include the loss of human lives.

Target	Syrian air defence system.
Type	Hybrid warfare — Denial of situational awareness of Syrian air space.
How	Blended use of cyber and electronic warfare. Alleged use of the 'Suter' ([60]) airborne network attack system to invade communication networks and take ownership as system administrator.
Why	Controversy between Syria and Israel over Syria's nuclear programme.
Impact	Military — Political — Economic — Human lives. The alleged Syrian nuclear development programme was brought to a halt.

Figure 8: Case study 3 threat assessment for a fictitious CSDP mission in the region

5.2. Mitigation of cyberthreats

The mitigation of cyberthreats has to be viewed holistically and through the prism of a top-down approach. Mitigation measures taken at the political/strategic level need to be followed up and specified/explained further when moving towards the operational and the tactical/technical level. It is

([59]) (Development, Concepts and Doctrine Centre 2016) Case Study 2.

([60]) http://www.1913intel.com/2007/10/05/what-is-suter/ (accessed 28 February 2017).

of great importance to maintain this coherence of context and maturity across the whole command chain for the effectiveness and optimisation of efforts and resources.

Cyberthreat mitigation is achieved in two ways:

1. in the short term: by minimising the cyberfootprint and attack surfaces of CSDP missions;
2. in the mid to long term: by developing cybercapacities.

5.2.1. Cyberfootprint and attack surfaces for CSDP missions (short term)

Assessment of the optimal cyberfootprint ([61]) (Julish 2013) and attack surface ([62]) (Howard and Pincus 2003) for a CSDP mission is of great importance as it prevents unnecessary exposure to cyberthreats. CSDP missions, civilian or military, should maintain the necessary cybercapabilities and presence in the cyberdomain in order to conduct their missions efficiently and resiliently. Excess capabilities/ presence in the cyberdomain does not mean better mission outcomes: quite the contrary. This optimal 'size' should be estimated/specified during the early planning phases of the missions and in the context of standard planning processes like CMC ([63]), IMD ([64]), CONOPS and SOR ([65]), OPLAN ([66]), etc. The estimate of the required cyberfootprint and attack surface should be flexible enough to be adjusted if needed when the threat landscape conditions change and/or mission objectives justify an increase in or reduction of capabilities.

5.2.2. Developing cybercapacities (mid to long term)

The development of cybercapacities for the CSDP is a mid- to long-term process that improves cyber-resilience and the effective and safer use of cyberspace. Building cybercapacity is a coordinated and multivectored effort to increase cybersecurity from both the human and the technological aspect. The use of suitable cybercapacity maturity modelling is highly recommended for this goal. The use of cybercapacity-building models has already been discussed in the past in the CSDP context (Robinson, Walczak, et al. 2013).

As stated in Section 4.1, we consider that the best approach is to use such a model in order to measure and improve the maturity of cybercapacities in the CSDP in a coherent fashion.

Building cybercapacity for the CSDP should operate across five directions ([67]):

1. devising cyberpolicy and strategy;
2. promoting responsible cyberculture;
3. building cyberskills;

([61]) The definition of 'cyberfootprint' is given in (Julish 2013) as 'the security-relevant information they unknowingly give away to potential hackers via job postings, press releases, employees' public profiles and other venues'.

([62]) Attack surfaces against IT systems are the attack opportunities of hackers on three dimensions: (a) Targets and enablers; (b) channels and protocols; and (c) access rights (Howard and Pincus 2003).

([63]) Crisis management concept (CMC): adopted by the EU Council and serves as basis for the development of different strategic options for the Political and Security Committee (PSC) to consider and decide upon.

([64]) Initial military directive (IMD): a high-level EUMS document based on PSC decisions and constituting the basis for further planning of the CSDP mission by the operational/mission commander.

([65]) Concept of operations (CONOPS): a high-level planning document developed at the operational level to describe the goals, organisation and implementation structure of a CSDP mission. CONOPS is accompanied by a provisional statement of requirements (SOR) of means and resources needed for a CSDP mission.

([66]) Operational plan (OPLAN): a detailed operational document describing how the mission will be carried out based on CONOPS and SOR.

([67]) Inspired by the Cyber Security Capability Maturity Model (CMM) V1.2, Global cybercapacity Centre, University of Oxford.

4. creating effective legal and regulatory frameworks;
5. managing risk through organisation, standards and capabilities.

These five directions or 'dimensions' as presented in CMM (GCSCC, University of Oxford 2016) are 'linearly independent', meaning that there is no conceptual overlap and that, at the same time, they cover the whole spectrum of activities within the cyberdomain.

Mitigation measures at the political/strategic level for the CSDP

A lot of work has already been done in the EU with the adoption of the EU cyberdefence policy framework (Council of the European Union 2014). This political document set five main priorities for the CSDP, at the highest level, with specific action items under each one of them, assigned to EU bodies, agencies and institutions. Progress on these action items is monitored by way of biannual progress reports. This study's suggestion on using a capability maturity model for the development of cybercapacities requires the EU cyberdefence policy framework action items to be mapped over the five dimensions of the CMM. This mapping is presented in Table 5.

		DIMENSION				
CSDP — POLITICAL/STRATEGIC LAYER		I	II	III	IV	V
		Policy and strategy	**Cyberculture**	**Skills**	**Legal and regulatory**	**Standards, organisation and capabilities**
EU CYBERDEFENCE POLICY FRAMEWORK ([68])	Support the development of Member States' cyberdefence capabilities related to the CSDP	Item d	Item c	Items e,f		Items a, b, g
	Enhance the protection of CSDP communication networks used by EU entities	Items b, e, g	Items d, f			Items a, c
	Promote civil–military cooperation and synergies with wider EU cyberpolicies, relevant EU institutions and agencies, as well as with the private sector	Items g,h,i	Item f	Items a, c	Item j	Items b, d, e
	Improve training, education and exercises opportunities			All Items		
	Enhance cooperation with relevant international partners	Items a,b,d	Items e, f, g, h	Item c		

Table 5: Mitigation measures undertaken within the EU cyberdefence policy framework

An observation that has to be noted is the gap identified under dimension IV, that is to create applicable legal and regulatory frameworks for cyberdefence. Although the EU accepts that international and EU laws apply in the cyberdomain (European Commission and High Representative of the EU for Foreign

([68]) Item descriptions for the EU cyberdefence policy framework can be found in Annex A.

Affairs and Security Policy 2013) there is still a lack of consensus internationally, rendering the applicability of international and EU laws problematic in the CSDP context. In addition, the legal aspect of cybersecurity is currently the subject of much discussion, debate and research. What is cyberdefence, what is 'active' cyberdefence, *jus in bello* ([69]) and the legality of offensive cyberoperations, the lack of cybernorms, attribution issues and the question of jurisdiction are all issues under formulation (Klimburg and Tirmaa-Klaar 2011). Nevertheless, what CSDP cybersecurity requires is a coherent voice across EU institutions, bodies and Member States. A coordinated effort between CSDP stakeholders needs to address issues like the adoption of an EU-wide cybertaxonomy, rules of engagement (RoEs) for cybermeasures, collaboration on cyberthreat attribution, cybercrime law enforcement and legal protection of personnel against cyberthreats in areas of operation of CSDP missions. In addition, Memorandums of Understanding and legal agreements with non-EU countries hosting CSDP missions or with relevant international organisations are required for the effective handling of cyberthreats under dimension IV.

Further streamlining of CSDP capacity-building efforts with CMM dimensions requires additional measures to be taken. Table 6 presents the domains where additional measures are proposed at the political/strategic level. These measures are further explained in Annex C.

	DIMENSION				
CSDP — POLITICAL/STRATEGIC LAYER	**I**	**II**	**III**	**IV**	**V**
	Policy and strategy	**Cyberculture**	**Skills**	**Legal and regulatory**	**Standards, organisation and capabilities**
Enhance cyberincident response for the CSDP	**√**				
Protect critical infrastructures used by CSDP structures	**√**				
Enhance EU crisis management	**√**				
Improve cyberdefences	**√**				
Improve cyber-resilience of CSDP systems and processes	**√**				
Promote a cybersecurity mind-set for the CSDP		**√**			
Build trust and confidence		**√**			

([69]) *Jus in bello* is a Latin term, which means 'the law in waging war.' It is an aspect of the international law of war, which addresses the practices forbidden to belligerents during a war. *Jus in bello* defines standards by which a country can conduct war and the actions during the war should be just and fair. It is a group of principles intended as guidelines for the just prosecution of war. *Jus in bello* includes two principles of discrimination and proportionality. Discrimination defines legitimate targets and proportionality defines how much force could be used. http://definitions.uslegal.com/j/jus-in-bello/ (accessed 15 December 2016).

Protect the identity and privacy of CSDP staff.		√			
Consider the uses of social media for the CSDP		√			
Further develop cybercompetencies			√		
Introduce cyber into exercises and operations			√		
Enhance cybersecurity legislation				√	
Coordinate law enforcement for cybercrime				√	
Develop cybernorms and confidence-building measures				√	
Promote international cooperation on legal issues				√	
Promote public–private sector cooperation				√	
Develop/adopt common standards					√
Improve cyberdefence organisation in the CSDP					√

Table 6: Additional mitigation measures proposed for the political/strategic layer

Mitigation measures at the operational layer of CSDP missions

Moving down to the operational layer of the CSDP, measures and action items planned and taken (part of the EU cyberdefence policy framework but also beyond this) should be in coherence with the five dimensions mentioned earlier in Section 5.2.2. Table 7 suggests a list of mitigation measures at the operational layer of CSDP administration.

	DIMENSION				
CSDP — OPERATIONAL LAYER	I	II	III	IV	V
	Policy and strategy	**Cyber culture**	**Skills**	**Legal and regulatory**	**Standards, organisation and capabilities**
Develop cyber SOPs ensuring compatibility between civil and military incident response ([70])	√				
Develop policies for critical infrastructure cyber-risk assessment for CSDP HQs and missions	√				
Develop policies for coordination of efforts between civilian and military structures during cybercrises	√				
Consider cyberdefence as an operational task for CSDP missions and include cyberdefence considerations within CSDP operational planning processes	√				
Develop further the collaboration between CSDP OHQs, EU cyber stakeholders (e.g. ENISA,EC3) and strategic allies (e.g. NATO) at the operational layer	√				
Promote cooperation between EU agencies, bodies and institutions on information sharing		√			
Develop/promote cyberawareness campaigns targeting CSDP command structures		√			
Develop measures to safeguard the privacy of CSDP staff according to the general data protection regulation (GDPR)		√			
Develop measures to protect the identity of CSDP staff during missions		√			

([70]) More information on ENISA's related work can be found at: https://www.enisa.europa.eu/news/enisa-news/standard-operational-procedures-to-manage-multinational-cyber crises-finalised-by-eu-efta-member-states-and-enisa

Develop policies on social media usage for CSDP staff		√			
Utilise social media as a source of OSINT for CSDP missions		√			
Develop training paths/requirements for cyberduties for CSDP HQs			√		
Explore NATO's cyberdefence education and training opportunities and synergies for CSDP operational planners			√		
Integrate cyber into existing operational exercises (planning, execution, evaluation, lessons learned)			√		
Consider the involvement of CSDP OHQs in future pan-European cybersecurity exercises (e.g. Cyber Europe)			√		
Provide legal support for cyberdefence options to the CSDP operational commanders/directors				√	
Stimulate the awareness of CSDP staff on cybercrime threats in general as well as in the context of CSDP missions				√	
Enhance the regulatory frameworks for the cooperation between the private sector and CSDP HQs for the delivery of cybersecurity services				√	
Produce/adopt specific cybersecurity requirements/standards for military systems (C4ISR) used in CSDP missions					√
Develop standing cyberdefence duties in the CSDP operational structure					√
Consider a cyberthreat assessment capability					√
Consider a cyber-resilience assessment capability for CSDP HQs					√

Integrate cyber within CSDP missions' common operational picture					√
Integrate technical cyber intelligence into operational intelligence					√

Table 7: Mitigation measures at the operational level, civilian and military

Mitigation measures at the tactical and technical layer of CSDP missions

Mitigation measures at the tactical and technical layer are closely connected to corresponding measures implemented at the operational layer. Tactical/technical layer is on the fringes of the CSDP organisation but at the same time at the front line of cyberoperations areas. Often this layer lacks resources, human-wise and capability-wise, and/or operates under adverse conditions beyond the EU borders. It is therefore of great importance to be able to build a mature cybercapacity that is flexible, scalable and, most important, cyberworthy. It is also important that this capacity be able to transmit reliable information, reliably, to the operational layer regarding the cyberthreat landscape of the cyberoperations area.

	DIMENSION				
CSDP TACTICAL/ TECHNICAL LAYER	**I**	**II**	**III**	**IV**	**V**
	Policy and strategy	**Cyber-culture**	**Skills**	**Legal and regulatory**	**Standards, organisation and capabilities**
Enhance cooperation regarding information exchange and best practices between EU Member States' military and civilian CSIRTs	√				
Conduct cyberawareness campaigns (general and mission-specific) targeting tactical/technical personnel		√			
Develop awareness campaigns for CSDP staff on privacy, data and identity protection		√			
Utilise technical opportunities offered by EU agencies and institutions (e.g. ENISA,CERT-EU)			√		

Introduce cyberdefence injects in tactical/technical exercises			√		
Consider the development of cybercells at the technical/tactical layer (FHQs, MHQs)					√
Develop a technical cyberintelligence capability					√
Develop well-defined cyberdefence perimeters for classified and unclassified networks (centrally managed, monitored and protected)					√
Develop a collaboration capability between military CSIRTs and the CSIRT network					√

Table 8: Mitigation measures at the tactical/technical civilian and military level

5.3. The EU and NATO

A good example of building alliances with international organisations that share the same moral values as the EU is the EU–NATO strategic partnership. This partnership dates back to 2001, when there was an exchange of letters between the EU Presidency and NATO Secretary General on the definition of the scope of cooperation between the two organisations. This was followed by the NATO–EU Declaration on European security and defence policy (ESDP) in December 2002 and the Berlin Plus arrangements signed in March 2003, which set the basis for EU–NATO cooperation. With these arrangements, and after approval by the North Atlantic Council, the EU has been granted access to NATO's collective assets and capabilities for carrying out EU-led missions where NATO itself has no interest in conducting those missions. This agreement includes also common Council and committee meetings at both the political and military levels. In 2005 and 2006 respectively, the two organisations exchanged liaison teams at the EU Military Staff and at the Supreme Headquarters Allied Powers Europe (SHAPE), NATO's Strategic Command headquarters. However, up to that stage, cyberdefence had not been a major concern of either organisation and was more an element of information security. The Lisbon Summit in 2010 marked a new milestone for cooperation between the two organisations as the European Union has been mentioned multiple times as NATO's strategic partner and crucial to NATO's call for a comprehensive crisis management call. 'NATO and the European Union (EU) share common values and strategic interests, and are working side by side in crisis management operations. We are therefore determined to improve the NATO–EU strategic partnership, as agreed by our two organisations' being the exact wording ([71]). The EU White Paper published in 2016 (European Parliament-Directorate General

([71]) Lisbon Summit Declaration issued on 20 November 2010. Source: http://www.nato.int/cps/en/natolive/official_texts_68828.htm (accessed: 28 February 2017).

for External Policies 2016) mentions that the first attempts to include cyberdefence within the EU–NATO discussions date back to that same year.

5.3.1. Integrating cyber into operations: the NATO case

With the Warsaw Summit, NATO reaffirmed its defensive mandate and officially recognised cyberspace as a domain of operations ([72]). This is a very important evolution as cyber is becoming an integral part of all aspects of NATO's crisis response planning for Article 5 ([73]) and non-Article 5 crisis response operations.

Following this decision, mission-related activities of planning and execution need to take cyber into consideration in the same way as with the other operational domains — sea, land, air and space.

The approach of 'integrating' into current structures and processes rather than creating new structures and processes to deal with cyberthreats offers multiple advantages like coherence, resource optimisation and rapid integration within operations.

5.3.2. Human resources

Human resources (HR) is a key pinch point but no different to other emerging capabilities. Cyber inherently has a strong technical dimension and requires a high degree of specialisation. Understanding the implications of cyber requires additional skills to 'translate' cyberthreats and their impact on the different layers of administration and on other domains (e.g. legal, social, financial). People who possess these skills, if and when found, seldom have the necessary military experience to integrate their knowledge into military operations. Where such personnel exist within a nation, they also tend to be fully occupied developing the national approaches to cyberdefence. Such challenges though, do not apply only for NATO, as already stated in Section 4.2.4. This is a global issue ([74]) and therefore, naturally, applies in the EU area and in the CSDP cybercapacities in particular (Roehrig 2015, 137).

5.3.3. Education and training

As a consequence of the deficiency/shortfalls of trained personnel, cyberdefence E & T has been a priority within NATO and NATO nations. The process is not rapid, and developing training, at both national and multinational levels, suffers from the same HR challenges as the rest of the cyberdefence community. NATO is making progress with TNA work, and is engaged with the MNCD E & T that is bringing both NATO and the EU CD E & T communities together.

Common synergies in multinational projects between bodies, institutions, agencies of the EU and NATO should be reinforced.

([72]) CCDCoE Press Release: NATO Recognises Cyber-space as a 'Domain of Operations' at Warsaw Summit, 21 July 2016. https://ccdcoe.org/nato-recognises-cyber-space-domain-operations-warsaw-summit.html (accessed: 14 December 2016).

([73]) The principle of collective defence. An attack against one Ally is considered as an attack against all Allies. Source: http://www.nato.int/cps/en/natohq/topics_110496.htm (accessed: 14 December 2016).

([74]) https://newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cyber security-talent/ (accessed: 14 December 2016).

5.3.4. Revising policies

The rapidly evolving cyberthreat landscape creates unique challenges, particularly when combined with the wider HR challenges mentioned in Section 5.3.2. The necessity to develop cyberdefence policies and enable them to evolve, as our understanding of the threat evolves and develops, creates an increasing workload for the policy staff within NATO. This burden is increased by the immature and technical nature of cyber that places a heavy burden on the military staff to justify, explain and illustrate the implications and impact of the policy options presented to the policymakers.

Nevertheless, NATO is making solid progress on revising its policies to include cyber across all levels of the command pyramid by providing a clear doctrinal framework that 'elevates the contribution of cyber-defence to operations led by NATO from a supporting to a more standalone role' ([75]).

5.3.5. Building capacities at the operational layer

In many respects, building the capabilities at the operational layer is the most challenging. The 'Enhanced NATO Policy for Cyber-defence', an operational 'bridging' document for cyberdefence, led NATO to put cyberdefence measures in place and ensure cyberdefence linkage across the NCS ([76]) and NFS ([77]).

However, were NATO to undertake a defensive military operation in response to an attack by a near peer, technically capable advisory and the existing fixed processes would not extend to the deployed force. The deployed force would be responsible for its own cyberforce protection. The NATO forces would expect to be able to enable mission-related activity using the internet and exploit critical infrastructure provided within the host nation. In a cybercontested environment/conflict, effective advisory cyberoperations would have an impact on the NATO force. A key tool that NATO uses to help forces prepare for such an eventuality is the NATO exercise programme.

Developing a credible cyberadversary for the crisis planning and execution phases of CPX events has proved challenging, partly because of the issues identified above. Additionally, and significantly, the inertia found in large organisations and the fact that understanding cyber in the context of military operations is challenging for military officers versed in the delivery of kinetic effects has ensured a challenging adoption of cyber within the complex works of NATO major joint exercises. The intangibility of cyber has added to the challenge of transforming NATO forces to operate effectively in a cybercontested future.

5.3.6. Current status of EU–NATO cooperation

The latest agreement between NATO and the EU on cyberdefence is the technical arrangement between NCIRC and CERT-EU ([78]), which allows both organisations to exchange cyberdefence-related information.EU staff members are also granted access to observe the NATO exercise 'Cyber Coalition', which provides insight into NATO's procedures as well as 'Locked Shields', a technical cyberdefence exercise. Up to now though, NATO has not been invited to observe EU cyberdefence exercises.

([75]) http://www.nato.int/docu/Review/2016/Also-in-2016/cyber defence-nato-security-role/EN/index.htm (accessed : 14 December 2016).

([76]) NCS: NATO Command Structure. More information can be found at http://www.nato.int/cps/en/natohq/structure.htm (accessed: 14 December 2016).

([77]) NFS: NATO Force Structure. More info can be found at http://www.nato.int/cps/en/natohq/topics_69718.htm (accessed: 14 December 2016).

([78]) 'EU and NATO increase information sharing on cyber incidents'. Source: https://eeas.europa.eu/headquarters/headquarters-homepage/5254_en (accessed: 14 Dec 2016).

NATO and the EU also cooperated by contributing to the 'Multinational Capability Development Campaign', which was projected in the years 2015/2016 to propose multinational defensive cyberoperations capabilities. On 8 and 9 July 2016, the President of the European Council Donald Tusk and the President of the European Commission Jean-Claude Juncker travelled to Warsaw, Poland, to represent the EU at the NATO summit, at the highest level, and to sign the EU–NATO joint declaration together with NATO's Secretary General Jens Stoltenberg. The joint declaration boosts cooperation, among other things, on cybercrisis management in the context of missions and operations, cyber-resilience building, capacity building including education and training and cooperation on cyberexercises between the EU and NATO.

Both organisations are currently working on the implementation roadmap for this joint declaration

5.3.7. Extension of future cooperation

While the general impression is that the overall security environment is challenged more and more, the security and defence budgets of Member States have not been increased proportionally as consequence of the economic crises starting in 2008 (bank crisis) and 2010 (national liability crisis in various Member States). An alternative to an increase in budgets is to seek more synergies in the use of existing and the development of future cybersecurity and defence capabilities.

Under the guidance of NATO allies and EU Member States, the implementation could continue and the abovementioned elements could be addressed. This should enhance the interoperability between both organisations.

The following are some examples:

- definition of a common taxonomy on the basis of the multinational capability development campaign on defensive cyberspace operations;
- enhancing the exchange of operational policies and doctrines. This should support the synchronisation of each respective operational approach in cyberdefence. In particular, the recognition of cyberspace as a domain of operation by NATO changes the operational approach on how cyberdefence is implemented within NATO's operations and missions. NATO could support the EU to built on this step;
- enhancing common participation in EU and NATO exercises. This enhances the two organisations' mutual understanding of policy and procedures. Mutual participation in each other's exercises allows the development of interoperability between both organisations to be prepared on combined and comprehensive efforts in time of crisis;
- synchronising cyberdefence-related education. NATO and the EU could identify synergies in each respective curriculum to see which kind of courses could be joint courses;
- to have an appropriate level of expectations, further development should be in coherence with the development of the implementation of the joint declaration. A follow-on analysis seeking more political achievable synergy effects should be followed by the joint declaration implementation roadmap.

5.3.8. Prerequisites for closer cooperation

Currently, NATO and the EU are continuing to implement the idea of the joint declaration and are seeking further guidance from NATO allies and EU Member States on how to implement this agreement. However, political issues ([79]) are generating obstacles to full-throttle cooperation between

([79]) 'Time to end the EU-NATO standoff'. Source: http://carnegieeurope.eu/strategiceurope/?fa=57423 (accessed: 14 December 2016)

the two organisations. Such issues must be 'dealt with at the highest political level and not be reduced to a secondary issue' (European Parliament-Directorate General for External Policies 2016).

Furthermore, the European Union does not yet have yet in place a standing operational command structure for the CSDP, such as that of NATO. Closer cooperation at the operational level can only be achieved on a case-by-case basis if NATO and the EU are operating in a similar area of operation and the EU has established a CSDP command structure to enable links between both organisations. The development of an EU standing operational CSDP command structure as a potential outcome of the development of the European Defence Union ([80]) might be used to establish cyberdefence links at the operational level between the two organisations.

([80]) Draft report on the European Defence Union issued on 14 July 16. Source: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-584.127+01+DOC+PDF+V0//EN&language=EN (accessed: 14 December 2016).

6. Foresight options

This study aims to investigate ways to improve cybersecurity for the CSDP following a top-down approach. The European Commission established, at the highest level, its vision for cybersecurity for the CSDP in its cybersecurity strategy in 2013. It is important though that CSDP-specific challenges and opportunities be addressed through a prism of coherency with wider EU cybersecurity policies and also with the consideration of the cyberdomain as a separate domain of CSDP operations.

Coherency is also important for the development of policies and cybercapabilities across all levels of CSDP administration. Monitoring the maturity of these developments is key to capacity building because it allows targeted adjustments where necessary and a more efficient way of allocating resources. The use of a capability maturity model therefore facilitates foresight options. Our proposal for these options is to follow the five dimensions of the CMM, i.e. to:

- maintain coherent cyberpolicies and strategies at the EU level;
- promote cyberculture;
- develop cyberskills through education and training;
- enhance legal and regulatory frameworks;
- develop standards, organisations and capabilities.

These options are non-exclusive in the sense that one does not exclude the other. Each of these five foresight options is further broken down into specific policy options for the political/strategic, operational and tactical/technical layers and presented in detail in Annex C. Policy options are also summarised in the options briefing document that accompanies this study.

6.1. Maintain coherent cyberpolicies and strategies at the EU level

As stated in the policy challenges section (Section 3.1.2), coherency is a major challenge for EU policies regarding cybersecurity. The coherence of policies and strategies should span all EU institutions and bodies and not only within the CSDP administration. All EU-level cyberstakeholders (bodies, institutions, agencies) should coordinate and plan current and future capacity building by taking into account CSDP considerations in the fields of:

- cyberincident response;
- critical infrastructure protection;
- crisis management;
- cyberdefence;
- cyber-resilience.

6.2. Promote cyberculture

The human factor and the importance of responsible behaviour in the cyberdomain are often displaced in favour of building technical cybercapabilities. It is a fact though that an overwhelming percentage of successful cyberattacks are due to human errors. ([81]) We consider human behaviour as one of the weakest links in the cybersecurity chain. Promotion of a responsible cyberculture should be examined using the following four categories;

- a cybersecurity mind-set;
- trust and confidence;

([81]) https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ (accessed: 7 March 2017)

- identity and privacy;
- use of social media.

6.3. Develop cyberskills

Cyberskills building is also important. As the sophistication of cyberthreats evolves, cyberdefences need to be adopted and updated continuously. This cannot be done without skilled personnel to handle today's sophisticated technical cybercapabilities. In the CSDP context, education and training should be viewed not only as a development of cybercompetencies but also as another aspect of operational training. Cyberskills building aims at the:

- improvement of operational and tactical/technical cybercompetencies;
- integration of cyber within CSDP exercises and operations.

6.4. Enhance legal and regulatory frameworks

Throughout this study, the legal aspect of cyber has been noted as one of the most challenging for the EU. The adoption of the NIS directive by the European Parliament is a major step forward. However, the legal dimension of cybersecurity is lagging in the areas of international cooperation between states and also between states and the private sector. CSDP missions are especially vulnerable to this because most of the time these missions occur beyond the EU borders. The enhancement of legal and regulatory frameworks is considered under the following five categories:

- cybersecurity legislation;
- law enforcement and cybercrime;
- cybernorms and CBMs;
- international cooperation;
- public–private sector cooperation.

6.5. Develop standards, organisations and capabilities

The last dimension considered is the building of common standards, clear organisational structures and cybercapabilities not only at the EU level but also at the Member State level. More specifically these concern:

- agreeing on common cybersecurity standards;
- developing a standing cyberdefence organisational structure spanning all levels of CSDP administration;
- supporting the development of EU and Member State cybercapabilities for the CSDP.

Policy options that are presented in Annex C stem from the aforementioned foresight options. Options already identified within the EU cyberdefence policy framework are integrated into and emphasised within the same annex.

7. Conclusions

This study has attempted to provide a structured approach to the possible options for the development of cybercapacities in the CSDP context. It became apparent that some of the efforts needed require wider cooperation and extension to areas beyond the CSDP. It is not only the fact that the cyberdomain has no national or international boundaries, it is also that cybersecurity is more than technical capabilities and infrastructures; it is human beings, social behaviours, the rule of law and a harmonised vision from all cyberstakeholders at the EU and at the Member State levels. Trust building is important for this and should be one of the priorities.

In the EU there are currently many ongoing efforts towards the improvement of cybersecurity. What is needed is coherence and coordination. This study concludes that the use of a cybercapability maturity model is necessary for the coherent monitoring and further development of cybercapacities in the CSDP. Modelling is important, not only for covering all aspects of cybersecurity, but also for monitoring the maturity of efforts and diverting resources to the areas that need it most.

In the CSDP context, there are additional factors that need to be considered for the protection of military and civilian missions, personnel and infrastructures. The geographical dispersion of CSDP missions beyond the EU borders, the global nature of the threat agents, hybrid threats and the protection of deployed assets from cyberattacks are all challenges that require attention. Looking at NATO as an example, a tighter cyberdefence organisation and coordination is needed in order to deal decisively with these matters.

New innovative technologies also play an important role that affects the CSDP. Considerations and inputs from the CSDP are therefore necessary in the formulation of EU-wide policies and ongoing work like the ICT standardisation process, the NIS directive and the discussions on cybernorms.

The European private sector and its closer cooperation in the CSDP context is another finding of the study. Europe needs to be able to rely on its own cybercapabilities in the same way as for other CSDP capabilities (military and civilian).

Finally, the building of alliances with international partners that share the same moral values as the EU will help by not only drawing benefits from their experience but also by coordinating efforts towards a safer cyberspace.

8. List of abbreviations

AU	African Union, 12
BSA	Business Software Alliance, 25
C4ISR	Command Control Communications Computers Intelligence Surveillance and Reconnaissance, 49, 90
CB	Capacity Building, 19
CBM	Confidence-Building Measure, 19
CCDCoE	Cooperative Cyber Defence Centre of Excellence, 13
CERT-EU	Computer Emergency Response Team -EU, 10
CFSP	Common Foreign and Security Policy, 8
CMC	Crisis Management Concept, 44
CMM	Capability Maturity Model, 21
CnC	Command and Control, 34
CNI	Critical National Infrastructure, 17
CoE	Council of Europe, 29, 30
CONOPS	Concept of Operations, 44
CPX	Command Post Exercise, 53
CSDP	Common Security and Defence Policy, 1
CSIRT	cyb, 14
CSS	Cyber Security Strategy, 23
DSM	Digital Single Market, 22
E & T	Education and Training, 52
EEAS	European External Action Service, 8
ESDP	European security and defence policy, 51
EU-INTCEN	European Union Intelligence and Situation Centre, 32
EUMS	EU Military Staff, 44
GCSCC	Global Cyber Security Capacity Centre, 21
GFCE	Global Forum on Cyber Expertise, 32
GGE	Group of Governmental Experts, 17
HR	Human Resources, 52
ICT	Information and Communications Technology, 14
IGF	Internet Governance Forum, 29
IMD	Initial Military Directive, 44
Infosec	Information Security, 38
IP	Internet Protocol, 34

ISACA	Internal Systems Audit and Control Association, 30
ISP	Internet Service Provider, 28
IT	Information Technology, 5
ITU	International Telecommunication Union, 30
	International Tellecommunications Union, 29
MHQ	Mission Headquarter, 32
MNCD	Multi-National Cyber Defence, 52
MoU	Memorandum of Understanding, 46
NATO	North Atlantic Treaty Organisation, 2, 5, 6, 8, 9, 10, 12, 13, 14, 29, 48, 49, 51, 52, 53, 54, 55, 71, 72, 81, 82, 83, 84
NCIRC	NATO Computer Incident Response Capability, 13
NCS	Nato Command Structure, 53
NCSI	National Cyber Security Index, 24
NCSS	National Cyber Security Strategy, 8
NFS	Nato Force Structure, 53
NIS	Network and Information Systems, 22
NRI	Networked Readiness Index, 31
OAS	Organisation of American States, 12
OECD	Organisation for Economic Cooperation and Development, 10, 12, 13, 29, 30, 31
	Organisation for the Economic Cooperation and Development, 13
OHQ	Operational Headquarter, 32
OPLAN	Operational Plan, 44
OSCE	Organisation for Security and Cooperation in Europe, 10, 12, 13, 19, 29, 71, 83
OSINT	Open Source Intelligence, 34
ppps	Public Private Partnerships, 18
RoE	Rules of Engagement, 46
SIAC	Single Intelligence Analysis Capacity, 69
SOR	Statement of Requirements, 44
TNA	Training Needs Analysis, 52
UN	United Nations, 5, 10, 11, 12, 13, 18, 29, 83
UNGA	United Nations General Assembly, 29
WARCIP	West Africa Regional Communications Infrastructure Program, 32
WEF	World Economic Forum, 31
WSIS	World Summit on the Information Society, 29

9. Bibliography

Inter American Development Bank. 2016. "Cybersecurity, Are We Ready in Latin America and the Caribbean." http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-030/16 .

UN General Assembly. 1974. "Resolution adopted by the General Assembly 3314 (XXIX). Definition of Aggression." 14 12. Accessed 11 29, 2016. http://www.un-documents.net/a29r3314.htm.

Al-Rawi, Ahmed K. 2014. "Cyber warriors in the Middle East: The case of the Syrian Electronic Army." *Public Relations Review* 40: 420–428.

Bakowski, Piotr. 2013. "Cyber security in the European Union." 12 December. Accessed November 29, 2016. http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf.

Banks, Gary. 2009. "Challenges of evidence-based policy-making." 19 June. Accessed December 6, 2016. http://www.apsc.gov.au/publications-and-media/archive/publications-archive/evidence-based-policy.

Cîrlig, Carmen-Cristina. 2014. "Cyber defence in the EU." October. Accessed November 2016. http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

Cornish, P. 2009. *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks.* Directorate-General for External Policies of the Union, Directorate B, Policy Department, European Parliament.

Council of Europe . 2011. "Convention on Cybercrime ." Accessed December 5, 2016. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

Council of Europe. n.d. "Action against Cybercrime." Accessed December 5, 2016. https://www.coe.int/en/web/cybercrime/home.

—. 2011. *Convention on Cybercrime (Treaty No. 185).* Budapest: CoE.

—. 2016. "Octopus Conference 2016 Key messages." 20 November . Accessed December 6, 2016. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806be360.

Council of the European Union. 2015. "Council Conclusions on Cyber Diplomacy." 11 February . Accessed 12 1, 2016. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

—. 2001. "Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union." 22 January . Accessed March 02, 2017. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001D0080.

—. 2014. "EU Cyber Defence Policy Framework." 18 November. Accessed December 5, 2016. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.

Defence Science Board. 2013. *Resilient Military Systems and the Advanced Cyber Threat.* DoD.

Development, Concepts and Doctrine Centre. 2016. *Cyber Primer Second Edition.* U.K. Ministry of Defence.

Directorate General for Internal Market, Industry, Entepreneurship and SMEs. 2017. *Rolling plan for ICT standardisation.* European Commission.

Drent, Margriet, Kees Homan, and Dick Zandee. 2013. "Civil-Military Capacities for European Security." December. Accessed December 6, 2016. https://www.clingendael.nl/sites/default/files/Study-Civil-Military-Capacities-European-Security.pdf.

EDA. 2016. "Cyber: EDA, ENISA, EC3 and CERT-EU discuss future cooperation." *EDA Info Hub*, 23 November. Accessed December 5, 2016. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/11/23/cyber-eda-enisa-ec3-and-cert-eu-discuss-future-cooperation.

EEAS. 2016. *Common Foreign and Security Policy (CFSP).* Policy document, Brussels: EU. Accessed 12 1, 2016. https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp_en.

—. 2016. *CSDP structure, instruments, and agencies.* 8 July. Accessed December 2, 2016. https://eeas.europa.eu/topics/nuclear-safety/5392/csdp-structure-instruments-and-agencies_en.

—. 2016. *EU and NATO cyber defence cooperation.* 10 February. Accessed 12 2, 2016. http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm.

EEAS. 2016. *EU Concept on Cyber Defence for EU-led Military Operations and Missions.* Brussels: European Union Military Staff.

—. 2014. "EU-US cooperation on cyber security and cyberspace." 13 March. Accessed March 2, 2017. http://www.eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf.

EEAS. 2016. *The Common Security and Defence Policy (CSDP).* Policy document, Brussels: EU. Accessed 12 1, 2016. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en.

ENISA. 2014. "An evaluation Framework for National Cyber Security Strategies." November. Accessed November 29, 2016. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

ENISA. 2016. *ENISA Threat Taxonomy.* ENISA.

ENISA. 2016. *National Cyber Security Strategies Good Practice Guide - updated.* Good Practice Guide, EU: ENISA. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

ENISA. 2013. *National-level Risk Assessments: An Analysis Report.* Survey, Athens: ENISA. https://www.enisa.europa.eu/publications/nlra-analysis-report.

ENISA. 2014. *Report on Cyber Crisis Cooperation and Management.* Athens: ENISA. https://www.enisa.europa.eu/publications/ccc-study/at_download/fullReport.

EU. 2016. "Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union." *Official Journal of the European Union.* 7 June. Accessed 12 1, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EN.

EUR-Lex . n.d. "Glossary of summaries - Mutual defence clause." Accessed 12 1, 2016. http://eur-lex.europa.eu/summary/glossary/mutual_defence.html.

European Commission and High Representative of the EU for Foreign Affairs and Security Policy. 2013. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of The European Union: An Open, Safe and Secure Cyberspace." 1 February. Accessed 12 2, December. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=en.

European Commission. 2016. *Commission Decision to establish a contractual public private partnership on cybersecurity (cPPP)* . Decision, Brussels: EU.

European Commission. 2015. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe" {SWD(2015) 100 final}.* Strategy, Brussels: European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN.

European Commission. 2016. *Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410.* Communication, Brussels: EU. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546.

European Commission. 2013. *Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace.* Strategy, Brussels: EU. https://ec.europa.eu/digital-single-market/en/cybersecurity.

European Parliament and Council. 2013. *Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.* Brussels: Official Journal of the European Eunion.

European Parliament. n.d. "Fact Sheets on the European Union - Common Security and Defence Policy." Accessed March 2, 2017. http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_6.1.2.html.

—. 2014 . "Resolution on the use of armed drones." 27 February . Accessed 12 12, 2016. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0172.

European Parliament-Directorate General for External Policies . 2016. "On the way towards a European Defence Union - A White Book as a first step." Brussels.

GCSCC. 2015. "Building Cyber-security Capacity in the Kingdom of Bhutan." https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf .

GCSCC. 2015. "Cybersecurity Capacity Assessment of the Republic of Kosovo." https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pd.

GCSCC, University of Oxford. 2016. *Cyber Security Capability Maturity Model for Nations (CMM).* Oxford: University of Oxford.

Happa, Jassim, and Graham Fairclough. 2017. "A model to facilitate discussions about cyber attacks." In *Ethics and Policies for Cyber Operations*. Springer.

Herzog, Stephen. 2011. *Revisiting the Estonian Cyber Attacks:Digital Threats and Multinational Responses.* Washington D.C.: Journal of Strategic Security, p.54.

HM Government, UK. 2016. *UK National Cyber Security Strategy 2016-2021.* Policy paper, London: Cabinet Office, UK.

Howard, Michael, and John Pincus. 2003. *Measuring relative attack surfaces.* Carnegie Mellon university.

Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. 2016. "European Union and NATO Global Cybersecurity Challenges: A Way Forward." 28 July. Accessed Janaury 18, 2017. http://cco.ndu.edu/News/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/ .

Julish, Klaus. 2013. "Understanding and overcoming cyber security anti-patterns." *Computer Networks*, 14 March.

Kaiser, Robert. 2015. "The birth of cyberwar." *Political Geography* 46 : 11-20.

Klimburg, Alexander, and Heli Tirmaa-Klaar. 2011. *Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU, p.13 (International law and cyberwar).* European Parliament, Brussels: European Parliament, Directorate-General for external policies.

Lyngaas, Sean. 2015. "The thin line between military and civilian cyber defense." 9 October. Accessed December 6, 2016. https://fcw.com/articles/2015/10/09/cybercom-collaboration-civilian-cyber-lyngaas.aspx.

MACSSA. 2013. *Information Sharing Framework (ISF).* Framework, MACSSA. https://www.terena.org/mail-archives/refeds/pdfjJz1CRtYC4.pdf.

McKay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. 2015. "International Cybersecurity Norms." Accessed March 14, 2017. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

Michael Robinson, Kevin Jones, Helge Janicke. 2015. "Cyber warfare: Issues and challenges." *In Computers & Security 49* 49: 70-94.

NATO CCDCoE. n.d. "Tallinn Manual." Accessed January 18, 2017. https://ccdcoe.org/research.html.

NATO. 2016. "NATO and the European Union enhance cyber defence cooperation." 10 February. http://www.nato.int/cps/en/natohq/news_127836.htm.

—. 2016. "NATO Cyber Defence." July. Accessed December 5, 2016. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

—. 2014. *NATO launches Industry Cyber Partnership.* 18 September. http://www.nato.int/cps/en/natohq/news_113121.htm.

—. 2016. "Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers." 2016 June. Accessed December 2016, 2016. http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

—. 2014. "Wales Summit Declaration." 5 September. Accessed December 5, 2016. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

—. 2016. "Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016." 09 July. Accessed February 2017. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Nurse, Jason R.C., Ioannis Agrafiotis, Michael Goldsmith, Sandy Creese, and K. Lamberts. 2014. *Two sides of the coin: measuring and communicating the trustworthiness of online information.* Oxford,UK: Journal of Trust Management, 1(1),2014. Accessed February 3, 2017. http://link.springer.com/article/10.1186/2196-064X-1-5.

OECD, Working Party on Information Security and Privacy. 2005. "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries." http://www.oecd.org/internet/ieconomy/35884541.pdf.

OSCE . 2016. "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies." 10 March. Accessed 2016. http://www.osce.org/pc/227281?download=true.

Osula, A.M, and H. Rõigas, . 2016. *International Cyber Norms - Legal, Policy & Industry Perspectives.* Tallinn, Estonia: NATO CCD CoE. Accessed 1 22, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

Pawlak, Patryk. 2015. "Cyber diplomacy Confidence-building measures." October. Accessed November 29, 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI(2015)571302_EN.pdf.

—. 2015. "Cyber diplomacy: EU dialogue with third countries." June. Accessed December 1, 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf.

—. 2016. "Cybersecurity and cybercrime." July. Accessed November 29, 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586612/EPRS_BRI(2016)586612_EN.pdf.

—. 2015a. "Cybersecurity and cyberdefence - EU Solidarity and Mutual Defence Clauses." June. Accessed February 2017. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf.

Pindják, Peter. 2015. "Deterring hybrid warfare: a chance for NATO and the EU to work together?" *NATO Review magazine.* http://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm.

Renard, Thomas. 2014. "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security." June . Accessed 12 1, 2016. http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

Riccardi, Marco. 2016. *APPLYING INTELLIGENCE ANALYSIS WHILE ATTRIBUTING CYBER ATTACKS.* ResearchGate.

Rivera, Jason, and Forrest Hare. 2014. "The Deployment of of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures." Accessed 12 2, 2016. https://ccdcoe.org/cycon/2014/proceedings/d1r1s11_rivera.pdf.

Robinson, Michael, Kevin Jones, and Helge Janicke. 2015. "Cyber warfare: Issues and challenges." *In Computers & Security 49* 49: 70-94.

Robinson, Neil. 2016. "NATO: changing gear on cyber defence." Accessed 5 December, 2016. http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm.

Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, and Pablo Rodriguez. 2013. "Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) Unclassified Summary." Accessed December 5, 2016. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf.

Roehrig, Wolfgang. 2015. *Handbook-Missions and Operations- The Common Security and Defence Policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence and Sports of the Republic of Austria. https://eeas.europa.eu/csdp/structures-instruments-agencies/european-security-defence-college/pdf/handbook/handbook-for-decision-makers.pdf.

Schmitt, Michael N., and Liis Vihul. 2016. "The Nature of International Law Cyber Norms." In *International Cyber Norms: Legal, Policy & Industry Perspectives,*, by NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), edited by Anna-Maria Osula and Henry (Eds.) Rõigas. Accessed December 5, 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

Smeaton, Rob, and Wolfgang Roehrig. 2014. "Cyber Security and Cyber Defence in the European Union Opportunities, Synergies and Challenges." Accessed December 2, 2016. https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf.

Sommario, Emmanuele. 2016. "Applying the Jus in Bello in the Cyber Domain: Navigating between lex lata and lex ferenda." 30 04. Accessed 01 10, 2017. http://www.qil-qdi.org/applying-jus-bello-cyber-domain-navigating-lex-lata-lex-ferenda/.

STOA. 2016. *Annex II on Procedure Reference EPRS/STOA/SER/16/214 N. Cybersecurity in the EU Common Security and Defence Policy (CSDP)-Challenges and risks for the EU.* Brussels: STOA.

Troszczynska-Van Genderen, Wanda. 2015. "The Lisbon Treaty's provisions on CFSP/CSDP." October. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/570446/EXPO_IDA(2015)570446_EN.pdf.

2016. *UK National Cyber Security Strategy.* Cabinet Office National security and intelligence, HM treasury, The Rt Hon Philip Hammond MP, UK.

UN . 1945. "Charter of the United Nations." 45 June. Accessed October 29, 2016. http://www.un.org/en/charter-united-nations/index.html.

UN General Assembly. 2013. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 .

UN. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 22 July. Accessed December 5, 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

UN Human Rights Council. 2014. "Report of the Special Rapporteur [Ben Emmerson] on the promotion and protection of human rights and fundamental freedoms while countering terrorism." 10 March. Accessed 12 12, 2016. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session25/Documents/A-HRC-25-59.doc.

Vierucci, Luisa. 2015. "Drone Warfare: challenges to the law of armed conflict?" 22 April. Accessed 12 12, 2016. http://www.difesa.it/SMD_/CASD/IM/IASD/65sessioneordinaria/Documents/Dronewarfare.pdf.

Wheeler, David A., and Gregory N. Larsen. 2003. *Techniques for Cyber Attack Attribution.* Institute for defence analyses.

Annex A: EU cyberdefence policy framework action items

PRIORITIES	ITEM	ACTION ITEMS
Supporting the development of Member States' cyberdefence capabilities related to the 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 cyberdefence 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.
	b	Support current and future cyberdefence-related pooling and sharing projects for military operations (e.g. in forensics, interoperability development, standard setting).
	c	Develop a standard set of objectives and requirements defining the minimum level of cybersecurity and trust to be achieved by Member States, drawing on existing EU-wide experience.
	d	Improve cooperation between military CSIRTs of the Member States on a voluntary basis, to improve the prevention and handling of incidents.
	e	Facilitate exchanges between Member States on: • national cyberdefence doctrines; • training programmes and exercises; • cyberdefence -oriented recruitment, retention and reservist programmes.
	f	Consider developing cyberdefence training, in view of EU Battlegroup certification.
	g	To the extent that the improvement of cyberdefence capabilities depends upon civilian network and information security expertise, Member States may request assistance from ENISA.
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 mechanisms. A cooperation strategy with the CERT-EU and existing EU cybersecurity capabilities shall also be developed or, where available, further enhanced.
	b	Develop a coherent IT security policy and guidelines, also taking into account technical requirements for cyberdefence 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.
	c	Building on existing structures, strengthen cyberthreat analysis at strategic (SIAC) and operational levels to: • identify and analyse current and new cyberthreats; • integrate cyberthreat 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 analyses;

		• with CERT-EU create the capabilities responsible for the elaboration of operational cyberthreat analysis aiming at strengthening cybersecurity and network protection.
	d	Promote real-time cyberthreat 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.
	e	Develop and integrate into strategic level planning a unified cyberdefence concept for CSDP military operations and civilian missions.
	f	Enhance cyberdefence coordination to implement objectives related to the protection of networks used by EU institutional actors supporting the CSDP, drawing on existing EU-wide experiences.
	g	Review regularly resource requirements and other relevant policy decisions based on the changing threat environment, in consultation with the relevant Council working groups and other EU institutions.
Promotion of Civil–military cooperation and synergies with wider EU cyberpolicies, relevant EU institutions and agencies as well as with the private sector	a	Develop common cybersecurity and defence competence profiles based on international best practices and certification used by EU institutions, also taking into account private sector certification standards.
	b	Develop further and adapt public sector cybersecurity and defence organisational and technical standards for use in the defence and security sector. Where necessary, build on the ongoing work of ENISA and the EDA.
	c	Develop a working mechanism to exchange best practice on exercises, training and other areas of possible civilian-military synergy.
	d	Leverage existing EU cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyberdefence capabilities.
	e	Seek synergies in R & D efforts in the military sector with civilian research and development programmes, such as Horizon 2020, and consider the cybersecurity and defence dimension when setting up preparatory action on CSDP-related research.
	f	Share cybersecurity research agendas between EU institutions and agencies (e.g. cyberdefence research agenda), notably through European framework cooperation, and share resulting roadmaps and actions.
	g	Support the development of industrial ecosystems and clusters of innovation covering the whole security value chain by drawing on academic knowledge, SME innovation and industrial production.
	h	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 (cyberthreat analysis and assessment capability, 'security by design' initiatives, dependency management for technology access etc.).
	i	Contribute to improving the integration of cybersecurity and cyberdefence dimensions in the programmes that have a dual-use security and defence dimension, such as SESAR.
	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.

Improve training, education and exercises opportunities	a	Based on the EDA cyberdefence training needs analysis and the experiences gained in cybersecurity training of the ESDC, establish CSDP training and education for different audiences, including the EEAS, personnel from CSDP missions and operations and Member State officials.
	b	Propose the establishment of a cyberdefence dialogue on training standards and certification with Member States, EU institutions, third countries and other international organisations, as well as with the private sector.
	c	Based on the EDA feasibility assessment, explore the possibility and rationale of setting up a cybersecurity/cyberdefence training facility for the CSDP, possibly as an integral part of the ESDC, making use of its training experience and expertise.
	d	Develop further EDA courses to meet the CSDP cyberdefence training requirements in cooperation with the ESDC.
	e	Follow the established ESDC certification mechanisms for training programmes in close cooperation with the relevant services in the EU institutions, based on existing standards and knowledge. Cyber-specific modules in the framework of the Military Erasmus initiative are planned as a pilot activity in November 2015, following the abovementioned mechanisms.
	f	Create synergies with the training programmes of other stakeholders such as ENISA, Europol, ECTEG and the European Police College (CEPOL).
	g	Explore the possibility of joint ESDC–NATO Defence College cyberdefence training programmes, open to all EU Member States, in order to foster a shared cyberdefence culture.
	h	Engage with European private sector training providers, as well as academic institutions, to improve the cybercompetencies and skills of personnel engaged in CSDP operations and missions.
	i	Integrate a cyberdefence dimension into existing exercise scenarios for MILEX and MULTILAYER.
	j	Develop, as appropriate, a dedicated EU CSDP cyberdefence exercise and explore possible coordination with pan-European cyberexercises such as Cyber Europe, organised by ENISA
	k	Consider participating in other multinational cyberdefence exercises.
	l	Once the EU has developed a CSDP cyberdefence exercise, involve relevant international partners, such as the OSCE and NATO, in accordance with the EU exercise policy.
Enhancing cooperation with relevant international partners	a	Exchange best practice in crisis management as well as military operations and civilian missions.
	b	Work on coherence in the development of cyberdefence capability requirements where they overlap, especially in long-term cyberdefence capability development.
	c	Enhance cooperation on concepts for cyberdefence training and education as well as exercises.
	d	Further utilise the EDA liaison agreement with NATO's Cooperative Cyberdefence Centre of Excellence as an initial platform for enhanced collaboration in multinational cyberdefence projects, based on appropriate assessments.

	e	Reinforce cooperation between the CERT-EU and relevant EU cyberdefence bodies and the NCIRC (NATO Cyber Incident Response Capability) to improve situational awareness, information sharing and early-warning mechanisms and anticipate threats that could affect both organisations.
	f	Follow strategic developments and hold consultations on cyberdefence issues with international partners (international organisations and third countries).
	g	Explore possibilities for cooperation on cyberdefence issues, including with third countries participating in CSDP missions and operations.
	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.

Annex B: ENISA cyberthreat taxonomy

CYBERTHREATS

No	TIER 1	TIER 2	TIER 3
1	Physical attacks	Fraud	
		Sabotage	
		Vandalism	
		Theft of devices, storage media and documents	Mobile devices
			Fixed hardware
			Documents
			Backups
		Information leak/sharing	
		Unauthorised physical access/entry to premises	
		Coercion, extortion or corruption	
		Damage from warfare	
		Terrorist attack	
2	Unintentional damage/loss of information or IT assets	Information leak/sharing due to human error	Accidental leaks/sharing of data by employees
			Leaks of data via mobile communication
			Leaks of data via web application
			Leaks of information transferred by network
		Erroneous use or administration of devices and systems	Loss of information due to maintenance errors/operators' errors
			Loss of information due to configuration/installation errors
			Increasing recovery time
			Loss of information due to user errors
		Using information from an unreliable source	
		Unintentional change of data in information system	
		Inadequate design and planning or improper adaptation	

		Damage caused by a third party	Security failure caused by third party
		Damage resulting from penetration testing	
		Loss of information in the cloud	
		Loss of (integrity of) sensitive information	Loss of integrity of certificates
		Loss of devices, storage media and documents	Loss of devices/mobile devices
			Loss of storage media
			Loss of documentation of IT infrastructure
		Destruction of records	Infection of removable media
			Abuse of storage
3	Disaster (natural, environmental)	Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)	
		Fire	
		Pollution, dust, corrosion	
		Thunder strike	
		Water	
		Explosion	
		Dangerous radiation leak	
		Unfavourable climatic conditions	Loss of data or accessibility of IT infrastructure as a result of heightened humidity
			Loss of data or accessibility of IT infrastructure as a result of very high temperature
		Threats from space/ electromagnetic storm	
		Wildlife	
4	Failures/malfunction	Failure of devices or systems	Failure of data media
			Hardware failure
			Failure of applications and services
			Failure of parts of devices (connectors, plugins)
			Failure or disruption of power supply

		Failure or disruption of communication links (communication networks)	Failure of cooling infrastructure
		Failure or disruption of service providers (supply chain)	
		Failure of cooling infrastructure (devices or systems)	
5	Outages	Absence of personnel	
		Strike	
		Loss of support services	
		Internet outage	
		Network outage	Outage of cable networks
			Outage of short-range wireless networks
			Outages of long-range wireless networks
6	Eavesdropping/interception/hijacking	War driving (Threat of locating and possibly exploiting connection to the wireless network)	
		Intercepting compromising emissions (Threat of disclosure of transmitted information using interception and analysis of compromising emission)	
		Interception of information (Threat of interception of information which is improperly secured in transmission or by improper actions of staff)	Corporate espionage
			Nation state espionage
			Information leak due to unsecured wi-fi rogue access points
		Interfering radiation (Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source)	
		Replay of messages (Threat in which data transmission is maliciously or fraudulently repeated or delayed)	
		Network reconnaissance, network traffic manipulation and information gathering (Threat of identifying information about a network to find security weaknesses)	

		Man in the middle/session hijacking (Threats that relay or alter communication between two parties)	
7	Nefarious activity/abuse	Identity theft (identity fraud/account)	Credentials- stealing Trojans
		Receiving unsolicited email	
		Denial of service	Distributed denial of network service (DDoS) (Network layer attack i.e. protocol exploitation; malformed packets/flooding/spoofing)
			Distributed denial of application service (DDoS) (Application layer attack i.e. Ping of Death/XDoS/ WinNuke/HTTP floods)
			Distributed DoS (DDoS) to both network and application services (Amplification/reflection methods i.e. NTP/DNS/../Bit Torrent)
		Malicious code/software/activity	Search engine poisoning
			Exploitation of fake trust of social media
			Worms/Trojans
			Rootkits
			Mobile malware
			Infected trusted mobile apps
			Elevation of principles
			Web application attacks/ injection attacks (Code injection: SQL,XSS)
			Spyware or deceptive adware
			Viruses
			Rogue security software/ Rogueware/Scareware
			Ransomware
			Exploits/Exploit kits
		Social engineering	Phishing attacks (Threat of an email fraud method in which the perpetrator sends out

			legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known trustworthy websites)
			Spear phishing attacks (A targeted email message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary)
		Abuse of information leakage	Leakage affecting mobile privacy and mobile applications
			Leakage affecting web privacy and web applications
			Leakage affecting network traffic
			Leakage affecting cloud computing
		Generation and use of rogue certificates	Loss of (integrity of) sensitive information
			Man in the middle/session hijacking
			Social engineering/signed malware
			Fake SSL certificates
		Manipulation of hardware and software	Anonymous proxies
			Abuse of computing power of cloud to launch attacks (cybercrime as a service)
			Abuse of vulnerabilities, 0-day vulnerabilities
			Access of web sites through chains of HTTP proxies (obfuscation)
			Access to device software
			Alternation of software
			Rogue hardware
		Manipulation of information	Repudiation of actions (Threat of intentional data

			manipulation to repudiate action)
			Address space hijacking (IP prefixes)
			Routing table manipulation
			DNS poisoning/DNS spoofing/DNS manipulations
			Falsification of record (Threat of intentional data manipulation to falsify records)
			Autonomous System hijacking (Threat of overtaking by the attacker of the ownership of a whole autonomous system and its prefixes despite origin validations)
			Autonomous System manipulation (Threat of manipulation by the attacker of a whole autonomous system in order to perform malicious actions)
			Falsification of configurations (Threat of intentional manipulation due to falsification of configurations)
		Misuse of audit tools	
		Misuse of information/information systems (including mobile apps)	
		Unauthorised activities	Unauthorised use of administration of devices and systems
			Unauthorised use of software
			Unauthorised access to the information systems/ networks (IMPI Protocol/ DNS Registrar hijacking)
			Network intrusion (Threat of unauthorised access to network)
			Unauthorised changes of records

		Unauthorised installation of software	Web-based attacks (Drive-by download/malicious URLs/ browser-based attacks)
		Compromising confidential information (data breaches)	
		Hoax (Threat of loss of IT assets security due to cheating)	False rumour and/or fake warning
		Remote activity (execution)	Remote command execution
			Remote Access Tool (RAT)
			Botnets/remote activity
		Targeted attacks (APT etc.)	Mobile malware (Threat of mobile software that aims to gather information about a person or organisation without their knowledge)
			Spear phishing attacks
			Installation of sophisticated and targeted malware
			Watering Hole attacks (Threat of malware residing on the websites which a group often uses)
		Failed business process (Threat of damage or loss of IT assets due to an improperly executed business process)	
		Brute force	
		Abuse of authorisations	
8	Legal	Violation of rules and regulations. Breach of legislation.	
		Failure to meet contractual requirements.	Failure to meet contractual requirements by third party. (Threat of financial penalty or loss of trust of customers and collaborators due to a third party's failure to meet contractual requirements)
		Unauthorised use of intellectual property rights (IPR)-protected resources. (Threat of financial or legal penalty loss of trust of customers due to improper/illegal use of IPR-protected material)	Illegal usage of file-sharing services
		Abuse of personal data.	

Annex C: Policy options for CSDP cybersecurity

Policy options presented in this annex follow the five foresight dimensions described in Section 6 of this study. Policy options span the three CSDP administration layers. Options already included in the EU cybersecurity framework are highlighted. This is not an exhaustive but an indicative list of policy options though all options should adhere to the five high-level foresight dimensions C.1 to C.5.

Option 1: Maintain coherent cyber policies and strategies across the EU

<table>
<tr><th>Area</th><th colspan="2">Political/strategic</th><th>Operational</th><th>Technical/tactical</th></tr>
<tr><td rowspan="2">Incident response</td><td colspan="2">Consider the development of a CSDP CSIRT for classified and unclassified networks.</td><td>Develop Cyber SOPs ensuring compatibility between civil and military incident response.</td><td rowspan="2">Develop mechanisms to enhance cooperation regarding information exchange and best practices between EU Member States' military and civilian CSIRTs.</td></tr>
<tr><td>EU cybersecurity framework</td><td>'Improve cooperation between military CSIRTs of the Member States on a voluntary basis, to improve the prevention and handling of incidents.'</td><td>Pilot the establishment of a cybersecurity rapid response team (RRT) for CSDP missions.</td></tr>
<tr><td rowspan="2">Critical infrastructures</td><td colspan="2">Provide the necessary instruments to support Member States and hosting countries of CSDP missions for the cyberprotection of critical infrastructure utilised by CSDP missions.</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>EU cybersecurity framework</td><td>'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.'</td></tr>
</table>

		'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' (cyberthreat assessment and analysis capability, 'security by design' initiatives, dependency management for technology access etc.).	Develop policies for critical infrastructure cyber-risk assessment for CSDP HQs and missions.	
Crisis management	Support the development of the pan-European cybercrisis management system based on the CSIRT network.		Develop policies for coordination of efforts between civilian and military structures during cybercrises.	
	EU cybersecurity framework	'Support the exchange of best practice in crisis management as well as military operations and civilian missions.'		
Cyberdefence	Provide adequate resources for the development of CSDP cyberdefence capabilities.		Consider cyberdefence as an operational task for CSDP missions and include cyberdefence considerations in CSDP operational planning processes.	
	Sponsor synergies for capabilities development with civilian research and development programmes			
	EU cybersecurity framework	'Support the coherent development of cyberdefence capability requirements where they overlap, especially in the long-term cyberdefence capability development.'		
		'Support the further utilisation of the EDA liaison agreement with NATO's Cooperative Cyberdefence Centre of Excellence as an initial platform for enhanced collaboration in multinational cyberdefence projects, based on appropriate assessments.'		

		'Support the development of coherent IT security policy and guidelines, also taking into account technological requirements for cyberdefence 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.'		
		'Support the further development and integration into strategic level planning of a unified cyberdefence concept for CSDP military operations and civilian missions.'	Develop further collaboration between CSDP OHQs, EU cyber stakeholders (e.g. ENISA,EC3) and strategic allies (e.g. NATO) at the operational layer.	
		'Support synergies in research and development efforts in the military sector with civilian research and development programmes, such as Horizon 2020, and consider the cybersecurity and defence dimension when setting up the preparatory action on CSDP-related research.'		
		'Improve the integration of cybersecurity and cyberdefence dimensions in the programmes that have a dual-use security and defence dimension, e.g. SESAR.'		
Cyber-resilience	Support the interoperability of cybercapabilities of EU and Member State IT systems and services used in CSDP missions (e.g. crypto).		Define and agree on specific levels of services for all EU and Member State IT systems used in the CSDP.	Agree on common set of security measures for cyber-resilience on the EU and Member State IT systems used in CSDP missions.
	EU cybersecurity framework	'Support the regular review of resource requirements and other relevant policy decisions based on the changing threat environment, in consultation with the relevant Council working groups and other EU institutions.'		

Option 2: Promote cyberculture

<table>
<tr><th>Area</th><th colspan="2">Political/strategic</th><th>Operational</th><th>Technical/tactical</th></tr>
<tr><td rowspan="2">Cybersecurity mindset</td><td rowspan="2">EU cybersecurity framework</td><td rowspan="2">‘Support the enhancement of cyberdefence coordination to implement objectives related to the protection of networks used by EU institutional actors supporting CSDP, drawing on existing EU-wide experiences.’</td><td>Promote cooperation between EU agencies, bodies and institutions on information sharing.</td><td rowspan="2">Conduct cyberawareness campaigns (general and mission specific) targeting tactical/technical personnel.</td></tr>
<tr><td>Develop/promote cyberawareness campaigns targeting CSDP command structures.</td></tr>
<tr><td rowspan="4">Trust and confidence</td><td colspan="2">Establish a minimum level of trust required in the CSDP context between:
o EU bodies, institutions and Member States;
o EU and international organisations (e.g. NATO, OSCE, UN);
o EU and third countries hosting CSDP missions.</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td colspan="2">Sponsor confidence-building measures between:
o EU bodies, institutions and Member States;
o EU and international organisations (e.g. NATO, OSCE, UN);
o EU and third countries hosting CSDP missions.</td></tr>
<tr><td rowspan="2">EU cybersecurity framework</td><td>‘Support the development of 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.’</td></tr>
<tr><td>‘Support the promotion of real-time cyberthreat information sharing between Member States and relevant EU entities. Promote the development of information-sharing mechanisms and trust-building measures between relevant national and European</td></tr>
</table>

		authorities, through a voluntary approach that will build on existing cooperation.'		
		'Support the reinforcement of the cooperation between the CERT-EU, relevant EU cyberdefence bodies and the NATO Cyber Incident Response Capability to improve situational awareness, information sharing, early-warning mechanisms and anticipation of threats that could affect both organisations.'		
		'Follow strategic developments and consultations on cyberdefence issues with international partners (international organisations and third countries).'		
		'Explore possibilities for cooperation on cyberdefence issues, including with third countries participating in CSDP missions and operations.'		
		'Support the development of confidence-building measures in cybersecurity in order to increase transparency and reduce the risk of misperceptions in state behaviour, by promoting the ongoing establishment of international norms in this field.'		
Identity protection and privacy			Develop measures to safeguard the privacy of CSDP staff according to the general data protection regulation (GDPR).	Develop awareness campaigns for CSDP staff on privacy, data and identity protection.
			Develop measures to protect the identity of CSDP staff during missions.	
			Develop policies on social media usage for CSDP staff.	

Social media	Leverage social media to the benefit of CSDP missions (trust building, promotion, social feedback).	Reinforce the utilisation of social media open source intelligence for CSDP missions .	

Option 3: Develop cyberskills through education and training

Area	Political/strategic		Operational	Technical/tactical
Cyber-competencies	Consider the development of an EU-wide cyberdefence education and training framework providing training standards career paths and certification requirements for cyberduties at the operational, technical and tactical layers of CSDP structures.		Develop training paths/requirements for cyberduties for CSDP HQs.	
	EU cybersecurity framework	'Support the establishment of CSDP training and education for different audiences, including EEAS, personnel from CSDP missions and operations and Member States' officials, based on the EDA cyberdefence training needs analysis.'		
		'Support the establishment of a cyberdefence dialogue on training standards and certification with Member States, EU institutions, third countries and other international organisations, as well as with the private sector.'		
		'Examine the possibility and feasibility of the establishment of a cybersecurity/cyberdefence, training facility for the CSDP, possibly as an integral part of ESDV, making use of their training experience and expertise.'		
		'Support the development of further EDA courses to meet the CSDP cyberdefence training requirements in cooperation with the ESDC.'		

		'Support 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.'		
		'Build synergies with the training programmes of other stakeholders such as ENISA, Europol, ECTEG and the European Police College.'	Explore NATO's cyberdefence education and training opportunities and synergies for the CSDP operational planners.	Utilise technical training opportunities offered by EU agencies and institutions (e.g. ENISA, CERT-EU).
		'Explore possibilities of joint ESDC–NATO Defence College cyberdefence training programmes, open to all EU Member States, in order to foster a shared cyberdefence culture.'		
		'Engage with European private sector training providers, as well as academic institutions, in raising cyber competencies and skills of personnel engaged in CSDP operations and missions.'		
		'Enhance cooperation for cyberdefence training and education as well as exercises with international partners.'		
Cyber into exercises and operations	**EU cybersecurity framework**	'Facilitate exchanges between Member States on: o national cyberdefence doctrines training, programmes and exercises; o cyberdefence -oriented recruitment, retention and reservists programmes'.	Integrate cyber into existing operational exercises (planning, execution, evaluation, lessons learned).	Introduce cyberdefence injects in tactical/technical exercises.
		'Integrate a cyberdefence dimension into existing exercise scenarios for MILEX and MULTIPLAYER.'	Consider the involvement of CSDP OHQs in future pan-European cybersecurity exercises (e.g. Cyber Europe).	
		'Develop a dedicated EU CSDP cyberdefence exercise and possible coordination with pan-European cyberexercises such as		

		Cyber Europe, organised by ENISA.'	'Consider cyberdefence training in view of EU Battlegroup certification.'	
		'Participate in other multinational cyberexercises.'		
		'Involve relevant international partners, such as the OSCE and NATO, in accordance with the EU exercise policy, in the EU CSDP cyberdefence exercise proposed earlier.'		

Option 4: Enhance legal and regulatory frameworks

Area	Political/strategic	Operational	Technical/tactical
Cybersecurity legislation	Future NIS directive revisions should include CSDP considerations.	Provide legal support for cyberdefence options to the CSDP operational commanders/directors.	
Law enforcement and cybercrime	Enhance collaboration of CSDP structures with cybercrime authorities within and beyond the EU borders, for law enforcement challenges in the CSDP context, attribution information and cybercrime-related incidents.	Stimulate the awareness of CSDP staff on cybercrime threats in general as well as in the context of CSDP missions.	
Cybernorms and CBMs	Provide CSDP inputs to EU-wide discussions and initiatives on the development of cybernorms.		
	Support confidence-building measures for cyberintelligence sharing between relevant EU stakeholders.		
	EU cybersecurity framework: 'Support synergies with the civilian cybersecurity industrial policy development undertaken at national level by the Member States and at European level by the Commission.'		
	Engage in a discussion on attribution and cyberintelligence information exchange		

International cooperation	with international organisations defining a set of minimum requirements.		
	Promote dialogue between EU bodies and institutions and international organisations on legal challenges related to cyberconflicts.		
	Consider legal issues for cyber in agreements between the EU and third countries hosting CSDP missions.		
Public–private sector cooperation		Enhance the regulatory frameworks for the cooperation between the private sector and CSDP HQs for the delivery of cybersecurity services.	

Option 5: Develop standards, organisations and capabilities

Area	Political/strategic		Operational	Technical/tactical
Standards	Produce/adopt common cybersecurity standards in the EU area for classified and unclassified networks.		Produce and adopt specific cybersecurity standards/requirements for military systems (C4ISR) used in CSDP missions.	
	Include CSDP considerations in the EU ICT standardisation processes.		Adopt a common cyber-taxonomy for the CSDP.	
	EU cybersecurity framework	'Support the further development and adaptation of public sector cybersecurity and defence organisational and technical standards for use in the defence and security sector, building on the ongoing work of ENISA and EDA where necessary.'		

Organisational	Develop a permanent cyberdefence organisational structure within the CSDP.		Develop standing cyberdefence duties in the CSDP operational structure.	Consider the development of cybercells at the tactical/technical layer (FHQs, MHQs).
	Monitor regularly the cybersecurity capacity building in the context of the CSDP using a capacity maturity model, such as the Cybersecurity Capability Maturity Model.			
Capabilities	**EU cybersecurity framework**	'Use of 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 cyberdefence 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 backups.'	Consider a cyberthreat assessment capability.	Develop a technical cyberintelligence capability.
			Consider a cyber-resilience assessment capability for the CSDP OHQs.	
		'Support current and future cyberdefence-related pooling and sharing projects for military operations (e.g. in forensics, interoperability development, standard setting).'		
		'Seek assistance from ENISA on the improvement of cyberdefence capabilities where these capabilities depend upon civilian network and information security expertise.'		
		'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	Integrate cyber within the mission's common	Develop well-defined cyberdefence perimeters for classified and unclassified networks (centrally

		early-warning mechanisms. Support of further cooperation with CERT-EU and existing EU cybersecurity capabilities.'	operational picture (COP).	managed, monitored and protected).
		'Leverage existing EU cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyberdefence capabilities.'		
		'Build on existing structures, strengthen at strategic (SIAC) and operational levels to: • identify and analyse current and new cyberthreats; • integrate cyberthreat 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 abovementioned threat and intelligence assessments include contributions from CERT-EU. Drawing on their cyber risk analyses, together with CERT-EU create the capabilities responsible for the elaboration of operational cyberthreat analysis aiming at strengthening cybersecurity and network protection.'	Integrate technical cyberintelligence and operational intelligence	Develop a collaboration capability between military CSIRTs and the CSIRT network

		'Leverage existing EU cybercrime prevention, investigation and forensics capabilities and their enhanced utilisation in the development of cyberdefence capabilities.'		

This study is the result of work conducted by the European Union Agency for Network and Information Security (ENISA) for the European Parliament's Science and Technology Options Assessment (STOA) Panel with the aim of identifying risks, challenges and opportunities for cyber-defence in the context of the EU Common Security and Defence Policy (CSDP). Acceptance of cyber as an independent domain calls for the investigation of its integration with the EU's current and future policies and capabilities. ENISA analysed the related literature and work on cybersecurity, including its own publications, to form the basis for this study. In addition, a number of stakeholders, experts and practitioners, from academia, EU institutions and international organisations, were consulted in order to ensure the study is well-founded and comprehensive.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service, European Parliament

PE 603.175
ISBN 978-92-846-1058-7
doi: 10.2861/853031
QA-04-17-454-EN-N