Supporting European Civilian External Action

Project funded by the European Commission within H2020 Programme

DELIVERABLE

Project acronym: CIVILEX

Start date of the project: 01/05/2016

Duration: 12 months

Grant agreement number: 700197

D2.1 Analysis of CSDP institutional and policy aspects and lessons learned

Abstract

The aim of the report is to map the Common Security and Defence Policy (CSDP) institutional and policy landscape in order to achieve an understanding of the state of the art concerning situational awareness, information exchange and operational control within EU CSDP civilian missions. In doing so, the project seeks to describe the political and institutional background in which the possible establishment of a future Situational Awareness, Information Exchange and Operational Control Platform (OCP) will take place.

Due date of the deliverable	**31 March 2017**
Authors	Yannick Arnaud (EU SATCEN), Cristian Barbieri, (IAI), Matthias Deneckere (ECDPM), Tommaso De Zan (IAI), Tobias Flessenkemper (ECDPM)
Contributors	Volker Hauck and Damien Helly (ECDPM), Nicolò Sartori (IAI)
Reviewers	Saria Diez Minguez (ATOS), Martijn Neef (TNO)

Dissemination Level		
P	Public	**X**
C	Confidential, only for members of the consortium and the Commission Services	

Release history

Version	Date	Description	Release by
0.1	29/07/2016	Structure and possible contents	ECDPM
1	21/09/2016	First draft shared within Consortium	ECDPM
2	27/01/2017	Second draft shared within WP	IAI
2	28/02/2017	Second draft shared within Consortium	ECDPM
3	24/03/2017	Third draft sent to reviewers	IAI
4	07/04/2017	Final version uploaded on the European Commission's portal	ATOS

Table of Contents

List of Tables and Figures

List of Figures

List of Acronyms

Acronym	Description
ACMN	Atalanta's Classified Mission Network
AMISOM	African Union Mission in Somalia
AOO	Area of Operation
BiH	Bosnia and Herzegovina
BMP	Best Management Practice
C2	Command and Control
CCC	Central Crisis Centre
CCDP	Civilian Capability Development Plan
CCM	Civilian Crisis Management
CFSP	Common Foreign and Security Policy
CHG	Civilian Headline Goal
CIMA	Centralized Information Management Application
CIS	Communication and Information System
CivCom	Committee for Civilian Aspect of Crisis Management
CivOpCdr	Civilian Operation Commander
CMC	Crisis Management Concept
CMF	Combined Maritime Forces
CMN	Classified Mission Network
CMPD	Crisis Management and Planning Directorate
COREPER II	Committee of Permanent Representatives II
COS	Chief of Staff
CPCC	Civilian Planning and Conduct Capability
CRS	Crisis Response System
CRT	Civilian Response Team
CSDP	Common Security and Defence Policy
CSO	Civilian Strategic Options
DG DEVCO	Directorate-General for International Cooperation and Development
DG ECHO	Directorate-General for European Civil Protection and Humanitarian Aid Operations
DG HOME	Directorate-General for Migration and Home Affairs
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations
EASO	European Asylum Support Office
ECDPM	European Center for Development Policy Management
EC3IS	Corporate Classified Communication and Information System
EDA	European Defence Agency
EDPS	European Data Protection Supervisor

EEAS	European External Action Service
EPC	European Political Cooperation
ESDI	European Security and Defence Identity
ESDP	European Security and Defence Policy
EU	European Union
EUCAP	European Union Maritime Capacity Building Mission to Somalia
EUCCIS	Command and Control Information System
EUCI	European Union Classified Information
EUGS	European Union Global Strategy
EULEX	European Union Rule of Law Mission in Kosovo
EUMM	European Union Monitoring Mission
EUMS	European Union Military Staff
EUNAVFOR	European Union Naval Force Atalanta
EUNAVFOR MED	European Union Naval Force for Mediterranean
EUROPOL	European Union Police Office
EUTM	European Union Multinational Military Training Mission
FAC	Foreign Affairs Council
FHQ	Field Headquarters
FPI	Foreign Policy Instrument
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FSJ	Freedom, Security and Justice
GSM	Global System for Mobile Communications
HoM	Head of Mission
HR/VP	High Representative / Vice President
IAI	Istituto Affari Internazionali
ICO	International Civilian Office
IcSP	Instrument contributing to Stability and Peace
INTCEN	Intelligence and Situation Centre
INTERPOL	International Criminal Police Organisation
IPCR	Integrated Political Crisis Response
ISAA	Integrated Situational Awareness and Analysis
JHA	Justice and Home Affairs
JSCC	Joint Support Coordination Cell
LNO	Liaison Officer
MAC	Mission Analytical Capability
MPCC	Military Planning and Conduct Capability
MSC	Maritime Security Capacity
MSCHoA	Maritime Security Centre for the Horn of Africa
MSO	Maritime Security Operations
MSP	Mission Support Platform

MTISC	Maritime Trade Information Sharing Centre
NATO	North Atlantic Treaty Organisation
NGO	Non-governmental Organisation
NPD	Non-Proliferation and Disarmament
NSC	NATO Shipping Centre
OBP	Oceans Beyond Piracy
OCP	Operational Control Platform
OECD	Organisation for European Economic Co-operation
OHQ	Operation Headquarter
OpCdr/OpsCmdr	Operation Commander
OPLAN	Operation Plan
PSC	Political and Security Committee
EU SATCEN	European Union Satellite Centre
SCOPE	Synergies and Coordination Portal
SECPOL	Security Policy and Conflict Prevention
SG/HR	Secretary-General / High Representative
SHADE	Shared Awareness and De-confliction
SHADE-MED	Shared Awareness and De-confliction in the Mediterranean
SIAC	Single Intelligence Analysis Capacity
SMART	Service-oriented infrastructure for MARitime Traffic
SOP	Standard Operating Procedures
SSR	Security Sector Reform
UK	United Kingdom
UN	United Nations
UNMIK	United Nations Mission in Kosovo
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
USA	United States of America
VoIP	Voice over Internet Protocol
VoSIP	Secure Voice Over IP
VTC	Video Telephone Conference
WEU	Western European Union
WFP	World Food Programme
WKC	Watchkeeping Capability

Executive Summary

The aim of this report is to map the Common Security and Defence Policy (CSDP) institutional architecture and policy landscape in order to contribute to a deeper understanding of the state of information exchange, situational awareness, and operational control within EU CSDP civilian missions. While focusing primarily on CSDP civilian missions, this mapping exercise also includes the wider aspects and actors of EU Civilian Crisis Management (CCM). In doing so, the report seeks to describe the political and institutional background in which the possible establishment of a future *Situational Awareness, Information Exchange and Operational Control Platform (OCP)* will take place. In this research, the term information exchange is used to describe missions' activities related to the sending and receiving of information. Situational awareness is conceptualised in this report as the outcome of a process of data collection and analysis taking place among CSDP and EU actors concerning the environment in which CSDP operates. Operational control is described by the Council as "a continuous sense, assess, decide and act cycle executed in order to accomplish an assigned mission."

The CSDP originated for the task of crisis management or "crisis response operations", similar to the United Nations (UN) but more forceful, as it acts on the will of its own member states. The EU CSDP effort has always been both a civilian and a military endeavour, so as to create synergies between the various instruments at the EU's disposal. Javier Solana, the first permanent High Representative for the Common Foreign and Security Policy (HR/VP), always stressed the notion that all EU missions had to combine both military and civilian aspects in dealing with external crises and conflicts. The notion stemmed from the idea that military power was not in itself enough to solve complex situations. In the EU, the concept of civilian crisis management refers "to the entire range of non-military instruments which are called for in crisis situations—whether pre or post-conflict".

In June 2016, the HR/VP Federica Mogherini presented the European Union Global Strategy on Foreign and Security Policy (EUGS), suggesting that the EU will further improve its civilian missions by supporting force generation, make deployment faster and provide better training. The EU will also pursue better information-sharing, joint reporting, analysis and response planning between member state embassies, EU delegations, Commission services, EU Special Representatives and CSDP missions. In November 2016, the HR/VP presented the Implementation Plan on Security and Defence**,** a practical instrument to translate the vision outlined in the Strategy into concrete actions. The Implementation Plan reiterated the importance of effectively responding to conflict and crises through anticipation, situational awareness, enhanced civil/military intelligence and strategic foresight. The Plan suggested revisiting the Feira priorities and evaluating how CSDP civilian missions can better respond to challenges such as migration, hybrid terrorism, cyber-attacks, organized crime and border

management. Also necessary are faster force generation, improvement in training, but above all "strengthen[ing] capacities available for the generic functions common to all missions, such as in the area of command and control, information/strategic communication, mission support, including logistics (e.g. Mission Support Platform, a more ambitious warehouse concept) and duty of care". In terms of situational awareness, the Plan proposes to enhance civil/military intelligence through the Single Intelligence Analysis Capacity (SIAC) as the main structure for strategic information, early warning and comprehensive analysis. These proposals were later partially endorsed by the Council Conclusions on 14 November. On 6 March 2017, the Council reviewed the implementation of its November conclusions and took important decisions by approving the "Concept Note on the operational planning and conduct capabilities for CSDP missions and operations". In particular, the Council decided to establish a Military Planning and Conduct Capability (MPCC) within Brussels' EU Military Staff (EUMS), as the body responsible for all non-executive military missions, to work in close collaboration with its civilian counterpart, the CPCC; to create a Joint Support Coordination Cell (JSCC) with staff from both the CPCC and the MPCC, in order to enable effective civilian–military coordination. There are some important takeaways from these latest policy developments concerning EU CSDP civilian missions, with straightforward implications for a future OCP platform. The most important is that there seems to be a clear political mandate to design and establish a tool dedicated to situational awareness, information exchange and operational control. The second relevant implication is that, in order for the EU to be an effective crisis manager in this increasingly perilous security context, a future OCP should be able to pursue its objectives by linking up the variety of actors engaged in CCM.

The EU institutional complexities, as well as the plethora of actors composing the EU civilian crisis management system, make information exchange, situational awareness and operational control for CSDP civilian missions not an easy task. This institutional complexity inevitably shapes how situational awareness, information exchange and operational control occur and should be envisaged. The immediate implication of having such a variety of actors is that the design of a possible platform should consider the technical difficulties of linking up actors that obey to different chain of commands, receive funds from different lines of the Union's budget, perform complementary but different tasks and pursue different agendas as they belong to different institution within the EU. According to some interviewees, actors are so diverse that it would be too difficult to conceive a system able to connect them all. Nonetheless, improvements to better connect CSDP Brussels entities with missions in the field, as well as Brussels structures with the relevant European Commission services are possible. Moreover, interviewees highlighted that connecting actors and entities such as the EU delegations, EC services and CSDP civilian missions, and possibly Justice and Home Affairs (JHA) actors, in the field should be treated as a matter of priority.

In addition to the study of the institutional architecture and dynamics shaping how a future

OCP platform should be conceived, the CIVILEX project decided to analyse five case studies in order to gain a deeper understanding of how missions are run and how info management and communication issues are addressed in the field. The five case studies are: 1) EUCAP Nestor, 2) EUNAVFOR Atalanta 3) EUCAP Sahel Mali and Niger, 4) EULEX Kosovo, and 5) EUNAVFOR MED Operation SOPHIA. These operations and missions were chosen because of several factors: EUCAP Nestor as a civilian mission in a complex security environment interacting, under the coordination of the EU Operations Centre (EU OPCEN), with two EU military missions such as EUNAVFOR Atalanta and EUTM Somalia; EUCAP Sahel Mali and Niger as two civilian missions interacting with an EU military mission (EUTM Mali), after 2014 under the coordination of the EU OPCEN; EULEX Kosovo as the most extensive EU civilian mission, with executive powers, ever to be deployed in EU CSDP history; and finally, EUNAVFOR MED as a military mission being deployed in the policy context of the EU internal–external security nexus, where a previous civilian mission was already operating (EUBAM Libya).

The analysis of the case studies underlines several important features that should be taken into account in the design of a future platform. Over the years, CSDP civilian missions have been changing their mandates and tasks, so that a future platform should be "flexible" enough to support a variety of actors and actions. Missions have been differing in size and length, changing inevitably the quantity of data exchanged, stored and retrieved. CSDP civilian mission have been strengthening ties with their military and area of Freedom Security and Justice (FSJ) colleagues, therefore suggesting that a future platform should be able to connect actors that are not necessarily representatives of their institutional family (EEAS VS Commission VS EU agencies) and have different chains of commands and budget line to respond to. This closer relationship between these actors stem from the concept that security challenges will be tackled along the internal-external security continuum. Better links with EU delegations, but also easiness in communicating with main international actors such as the North Atlantic Treaty Organization (NATO), UN, OSCE, AU will have to be pursued. Finally, security of networks and data, as well as data protection rules, will have to be seriously considered to allow swift and fast exchange of information, while ensuring that the data are secured properly.

Whereas the study of civilian missions' needs and requirements is a necessary step in the design of a future information system, one should be aware that these primarily stem from the mission's task, duty and mandate. Consequently, if task, duty and mandate change, needs and requirements also will. The EUGS has outlined a strategic vision that will prompt changes in how the EU conducts its foreign and security affairs. These changes will in turn modify needs and requirements. Although this is difficult to completely foresee, the "paradigm shift" in which civilian missions now find themselves is likely to make missions evolve in the same direction we have observed in this report: more civil–military–JHA synergies in the framework of the internal–external security nexus rather than large missions

with the ultimate goal of state-building. Although their full implications are difficult to foresee as of now, but which will have to be fully taken into account when imagining the future of civilian missions, and as a consequence the design of a possible future OCP platform to support them.

The report envisages information exchange, situational awareness and operational control from three interlocking perspectives:

- the institutional-administrative dynamics of the operational life-cycle of civilian CSDP operations, and how information exchange, situational awareness and operational control issues impact on the phasing-in, implementation and phasing-out of CSDP operations;
- the institutional-technological landscape in which missions are conceived and which form the backdrop of the recommendations for developing an OCP; since the emergence of CSDP some 15 years ago and the EEAS almost seven years ago a number of initiatives, mechanisms and technological solutions have been developed in the field of civilian external action which also aim at improving their effectiveness and which have an impact on the conceptualisation of a future OCP;
- the management of sensitive data and EUCI (EU classified information); a field that has seen considerable development with the growth of the CFSP and CSDP as well as the evolution of Community legislation in the area of data protection and information security .

All three perspectives, while analysed distinctively, are interlocking as the institutional-administrative mission life-cycle management is confronted with legacy technology and communication solutions as well as the thickening web of data management regulations and legislation.

The study makes recommendations on the institutional policy aspects to define during the further development of the OCP:

- **The scope of the OCP**: The study found that the OCP should add value to CSDP missions that require better access to information within the EU system (EEAS, Commission, Council); that the CPCC should be provided with systematic access to information and data, political background analysis and archival information on the theatre of operations and on EU activities, throughout the operational life-cycle; and that “dedicated information windows” in the OCP should be provided to EEAS, Commission (especially FPI) and Council stakeholders to contribute to their information and knowledge on EU activities in the domain of civilian CSDP and its theatres of operations.
- **The information management approach**: The study identified that a facilitator for the success of the OCP will be to encourage, develop and support a culture of institutional memory-building and knowledge-sharing, including through enhanced

training and in-mission learning; to develop and adapt standardized information storing and archiving tools and procedures; and to develop information plans for various theatres of operation, in conjunction with all EU external action bodies, that identify common information needs.

- **The civilian CSDP context**: To add value and move beyond current limitations, there is a need to design an OCP for all CSDP civilian missions and place it under the responsibility of the Civilian Operations Commander who sets rules and provides guidance. Furthermore the OCP should allow for the creation of individual "mission branches" with the official start of mission planning and allow for mission-internal information exchange and management. It should hereby respect the "legal personality" of missions, and in particular the right to manage and control parts of the OCP (e.g., in the area of finance, etc.) should be reserved at the appropriate level. Overall effectiveness and acceptance by the CSDP community will stem from a modular design concept to flexibly respond to the diverse needs and contexts of CSDP civilian missions.
- **The data security and protection context**: The current institutional arrangements are not fostering a data classification- and security-aware working culture and practice. It is paramount to distinguish more clearly between classification of information (which happens by decision) and information security (which will need to become the rule). The study found that the OCP development provides an opportunity to consider a review of existing classification rules and their respective technological requirements.
- **The ownership of the OCP**: Ownership in the physical and legal sense will need to be decided by the end of the development phase. With the suggested scope of the OCP a tension may arise as the CPCC technological infrastructure is financed through the administrative budget of the EEAS, while the missions are financed through the CFSP operational budget managed by the FPI.
- **The OCP within the overall context of EU external action beyond CSDP**: For the OCP to contribute the advancement of EU external action, it is necessary to provide strategic guidance through a joint Political and Security Committee-Standing Committee on Internal Security (PSC–COSI) agenda to open dedicated windows within the OCP for freedom, security and justice (Frontex, Europol) actors; to review and adapt existing CSDP civil–military information exchange for the OCP; and to take into account the EU–UN cooperation agreement, as well as cooperation with NATO and third states.

Regardless of the specifics—certainly important in the context of the design of an information system platform—the changing security environment coupled with the a renewed political mandate to seek more information exchange, improved situational awareness and better conduct of missions make the establishment of an OCP a matter of priority. The OCP has the potential to become an important part of the CSDP operational set-up. This study identifies the strategic and policy drivers and describes the institutional

barriers and facilitators for the development of an OCP. The changes required to allow for a more effective information exchange, situational awareness and operational control approach within the field of civilian CSDP remain within reach, provided that the cause of establishing a modern operational environment for civilian CSDP can find enough institutional champions with determined vision and leadership.

1 Introduction

"We will also pursue greater information sharing and joint reporting, analysis and response planning between Member State embassies, EU Delegations, Commission services, EU Special Representatives, and CSDP missions."[1]

The European Union Global Strategy, June 2016

This statement in the newly released European Union Global Strategy on Foreign and Security Policy (EUGS, June 2016) emphasizes that improving communication in European external action is a priority for the EU. Yet, it is also an acknowledgment that the current situation of information exchange and communication can be improved, notably among key EU civilian external actors. The ambition formulated in the EUGS depicts the strategic and political context in which the CIVILEX project operates. The project has the objective "to identify, characterise and model the communication and information systems in use within the European Union (EU) Civilian missions, understand the stakeholders' requirements and provide possible solutions for a future interoperable Situational Awareness, Information Exchange and OCP."[2] Overall, the CIVILEX project is expected to contribute to building a better understanding among all stakeholders involved in EU civilian action on how to improve information management and exchange within the institutional setting that governs the implementation of civilian CSDP missions.

This report (D2.1) is one of the two deliverables foreseen under Work Package 2 ("Policy and institutional mapping") of the CIVILEX project and it has been jointly produced by the Istituto Affari Internazionali (IAI) and the European Centre for Development Policy Management (ECDPM), with a dedicated contribution from the European Union Satellite Centre (EU SATCEN).[3] The outcomes of this research were presented and discussed during two stakeholder workshops, and informed the field scenario research (D2.2).

The aim of D2.1 is to map the CSDP institutional architecture and policy landscape in order to contribute to a deeper understanding of the state of information exchange, situational awareness, and operational control within EU CSDP civilian missions. In doing so, the report seeks to describe the political and institutional background in which the possible

[1] EEAS, Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign And Security Policy, July 2016, http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

[2] http://civilex.eu/

[3] The other deliverable of WP2 (D2.2) is a field mission case study on the EUCAP Nestor CSDP operation, submitted to the European Commission on 31 January 2017.

establishment of a future *Situational Awareness, Information Exchange and OCP* will take place. While focusing primarily on CSDP civilian missions, this mapping exercise includes the wider aspects and actors of EU Civilian Crisis Management (CCM). In this research, the term information exchange is used to describe missions' activities (either formalised or not) related to the sending and receiving of information. Situational awareness is conceptualised in this report as the outcome of a process of data collection and analysis taking place among CSDP and EU actors concerning the environment in which CSDP operates. Operational control is described by the Council as "a continuous sense, assess, decide and act cycle executed in order to accomplish an assigned mission."[4]

Hence, this report investigates ongoing initiatives and previous approaches aimed to standardize systems for information management and communication in support of CSDP and the wider EU external action. This investigation identified institutional barriers and facilitators for success. Lessons learned informed the formulation of observations and recommendations for the development of an OCP taking into account the institutional policy aspects.

This report is organized as follows. Chapter 2 outlines the main strategic and policy documents that provide the foundation of EU CSDP civilian missions needs in terms of situational awareness, information exchange and operational control. It highlights the complex institutional system in which CSDP civilian missions interact and induces a reflection on the possible institutional challenges in the establishment of a future OCP. Chapter 3 presents a general overview of CSDP civilian missions, as well as some selected case studies: EUCAP Nestor (see D2.2 for further reference), EUNAVFOR Somalia Operation Atalanta, EUCAP Sahel Mali and Niger, EULEX Kosovo and EUNAVFOR MED - Sophia. The scope of this exercise is to highlight missions' tasks and related needs in terms of situational awareness, information exchange and operational control and to shed light on their potential evolution after the release of the EUGS and the Implementation Plan on Security and Defence. The last part of the chapter also offers some insights on future possible developments of the nature and tasks of CSDP civilian missions. Chapter 4 brings together the institutional administrative and technological perspectives through a look at the life-cycle of CSDP missions, and by scoping into past and current initiatives in the fields of situational awareness, information exchange and operational control, and in relation to EU Classified Information (EUCI) and the management of sensitive data. In chapter 5, the findings on institutional policy aspects and lessons learned are drawn together to present recommendations for the OCP. Conclusions are presented in chapter 6.

The work carried out in D2.1 also informed other deliverables in the project, namely D3.1 and D4.1. D3.1 provides an overview of the OCP core requirements as defined through

[4] Council of the EU, Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management, 9919/07, 23 May 2007.

analysis of the working domain: these requirements cover a technical/architectural point of view, but also include a working process and institutional perspective. The requirements will be described using the MoSCoW typology (must-have, should-have, could-have, would-have). D4.1 gives an overview of the technical options for the OCP, which will derive from the requirements identified and defined in WP3. The options will cover the general architecture of the intended system and the system's components, the interfaces, information exchange processes and how they are supported, security aspects and the UN practices and perspectives under the technical angle.[5] The final aim of these deliverables (D2.1, D3.1 and D4.1) is to be a working basis for end-users in order to finally develop and express recommendations for a future OCP in WP5. Indeed, D5.3, "Roadmap and recommendations for implementation" outlines a roadmap towards the implementation of a future OCP and its surrounding information exchange infrastructure.

[5] Lessons learned from the UN are presented in D4.2.

2 CSDP civilian missions in the context of EU external action

According to the Lisbon Treaty, "The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the UN Charter and international law."[6]

The EU has supported peace around the globe in a variety of venues. In July 2015 it was a broker, together with China, France, Germany, Russia, the United Kingdom (UK) and the United States, of an international agreement on Iran's nuclear programme, in which the EU has now a role in overseeing implementation. Likewise, the EU supports negotiations between the Colombian government and the FARC movement to put an end to years of internal strife. The EU also plays a critical role in the Western Balkans, especially regarding Serbia–Kosovo relations, although some could contest what the EU has achieved after years of presence on the terrain and political pressure. Concurrently, with its Neighbourhood Policy the EU has tried to establish friendly ties with countries at its borders, promoting EU values such as democracy, good governance and human rights. The EU has also stepped up its efforts to curb climate change, and played an active role in promoting the first legally binding global climate agreement in Paris in December 2015. The EU, together with its member states, provides more than a half of the official development assistance globally, making it collectively the largest donor of development aid. It is also collectively the largest donor of humanitarian aid, which is delivered in cases of human and natural disaster. In these critical situations, the EU can also introduce the instrument of civil protection. Moreover, through the Instrument contributing to Stability and Peace (IcSP), the EU can fund a variety of activities in the fields of relief, crisis prevention, peacebuilding and resilience support.

In the last two decades, the EU has also developed its CSDP, subsumed under the Common Foreign and Security Policy (CFSP). The main representations of CSDP are the military and civilian missions that the EU has deployed around the world, although mainly in its immediate neighbourhood and in Africa. Nevertheless, the full emergence of the EU as a security actor has been constrained in part by some member states, which saw and still see foreign and security policy largely as a national prerogative, but also by some institutional

[6] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art.21, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M021.

limitations and complexities of the EU itself. In this sense, the development of the EU as a security actor is still a "work in progress."

This chapter is organised as follows. Section 2.1 describes the historical genesis of EU CSDP civilian missions in order to describe the rationale leading to the creation of the Union's civilian instrument; section 2.2 outlines the main strategic and policy documents that provide the foundation of CSDP civilian missions, with a view to defining EU needs in relation to situational awareness, information exchange and operational control; section 2.3 details the actors involved in civilian crisis management, highlighting the complex institutional system in which CSDP civilian missions interact with other EU institutions; section 2.4 outlines the decision-making process that leads to the establishment of a CSDP civilian mission, reinforcing the argument that CSDP civilian missions take place in a wider CCM management environment with a convoluted decision-making and complex systems of interactions; finally section 2.5 presents the findings from the interviews and induces a reflection on the possible institutional challenges in the establishment of a future OCP.

2.1 The origins of CSDP civilian action

This section briefly describes the historical genesis of EU CSDP civilian missions in order to describe the rationale leading to the creation of the Union's civilian instrument. EU CSDP missions were conceived as an instrument enabling EU foreign policy to manage complex crises outside EU borders, in which the military dimension of security and defence policy is not enough or has to be complemented with a more rounded approach.

In the years of the European Community's history, coordination of foreign policy preferences was done through the informal channel of the European Political Cooperation (EPC), in which the formula of consensus and lowest common denominator prevailed.[7]

One of the most serious attempts to bring security to the table occurred in 1948 with the creation of the Western European Union (WEU), a body established with the intention to coordinate the defence policies of the UK, France, Belgium, the Netherlands and Luxembourg. Though remaining active until 2011, the WEU was supplanted by NATO in 1949 as the preeminent defence organization in the EU.[8]

In the 1980s, Europe started to manifest its intention to assume a greater control over its own security fate, and in The Hague in 1987 the WEU asserted that European integration would still be unfulfilled if it had not included security and defence.[9]

[7] Howorth J., Security and defence policy in the European Union, Palgrave Macmillan, 2014, https://he.palgrave.com/page/detail/Security-and-Defence-Policy-in-the-European-Union/?K=9780230362352.
[8] Ibid.
[9] Ibid.

However, the task seemed immediately challenging when Europeans realized their reliance on American hard power with the 1991 Gulf War. The US military instrument and its technological advancement became the benchmark for every country aspiring to become a credible actor in post-Cold War crisis management operations. But the war against Saddam Hussein was not the only major political event that shaped the creation of EU security and defence policy.[10]

Between 1990 and 1991, Yugoslavia's breakup was unfolding. The internal and external wars that were tearing apart an entire sub-region of Europe were a wakeup call for an organization with the ambition to become a reliable security operator. The Balkan conundrum prompted the emergence of a European Security and Defence Identity (ESDI),[11] according to which the WEU and NATO would identify "separable but not separate capabilities, assets and support assets […] in order to prepare, support, command and conduct WEU-led operations" within NATO.[12]

In Maastricht (1992), Amsterdam (1997) and Nice (2000), EU countries found an accord to make EU foreign and security policy an intergovernmental pillar, where the Heads of State and Government would have the final decision on all related policies.[13]

In 1998, the Saint-Malo Declaration became the onset of a new policy area for the EU. Jacques Chirac and Tony Blair, the Prime Ministers of France and the UK, agreed upon three main principles: 1) the EU needed to play its role on the international stage, and hence the need to give full force to the Treaty of Amsterdam, especially the provisions on CFSP; 2) the Union "must have the capacity for autonomous action, backed by credible military force;" 3) the Union "must be given appropriate structures." This new approach—called the Common European Security and Defence Policy (ESDP), later abbreviated to ESDP and eventually CSDP—was officially launched at the Cologne European Council summit in June 1999.[14]

While at the time of Saint-Malo and Cologne the focus was on military crisis management, the European approach to security and defence policy evolved, developing a civilian dimension of ESDP and building on the comprehensive approach of the EU to crisis management, from conflict prevention to post-conflict stabilization.[15]

The CSDP originated for the task of crisis management or "crisis response operations," similar to the UN but more forceful, as it acts on the will of its own member states. The EU

[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid.

CSDP effort has always been both a civilian and a military endeavour, so as to create synergies between the various instruments at the EU's disposal. Javier Solana, the first permanent HR/VP, always stressed the notion that all EU missions had to combine both military and civilian aspects in dealing with external crises and conflicts. The notion stemmed from the idea that military power was not in itself enough to solve complex situations.[16]

In the EU, the concept of civilian crisis management refers "to the entire range of non-military instruments which are called for in crisis situations—whether pre or post-conflict."[17] Examples of such missions are police training, state-building capacity, security sector reform (SSR), civil protections, etc. The concept first emerged at the Helsinki European Council meeting in December 1999, where an Action Plan was agreed on to list the available resources, a database of capabilities and know-how, and finally the setting of specific targets for civilian crisis management.[18]

At the Lisbon Council in 2000, the Committee for Civilian Aspects of Crisis Management (CivCom) was established within the Council of the EU, and Solana later initiated a mechanism to coordinate the Council Secretariat and the Commission. At the Feira European Council (2000), civilian crisis management was specifically subsumed to CSDP, while four main areas were established as key: police, rule of law, civilian administration and civil protection.[19]

The Swedish Presidency in 2001 made the first real breakthrough in civilian crisis management, redacting a report on CSDP that mainly concerned its civilian side. The Goteborg European Council in June 2001 released the report "The Prevention of Violent Conflicts."[20] At the Laeken European Council meeting in 2001, a new goal was set for the EU: to be able to perform the full range of Petersberg tasks (humanitarian and rescue tasks; peacekeeping tasks; and tasks of combat forces in crisis management, including peacemaking) by 2003.[21]

In November 2002, EU ministers gathered in a first Civilian Crisis Management Capability Conference. On 1 January 2003, the EU launched its first mission in Bosnia and Herzegovina (EUPM BiH), which lasted until 2012. EUPM was instrumental in the development of a number of CSDP-related initiatives including areas of concern for the development of the OCP. In December 2003, the first European Security Strategy was issued, stressing the need

[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Rutten M., From Saint-Melo to Nice. European Defence: core documents, EUISS, Chailot Paper N.47, 2001, http://www.iss.europa.eu/uploads/media/cp047e.pdf; Howorth Jolyon, Security and defence policy in the European Union, Ibid.
[20] Ibid.
[21] Ibid.

for an increased civilian crisis management.[22]

2.2 The development of CSDP civilian action

This section outlines the main strategic and policy documents that provide the foundation of CSDP civilian missions, with a view to defining EU needs in relation to situational awareness, information exchange and operational control. In particular, this section demonstrates how, over the course of the years, the need for a better situational awareness, information exchange and operational control have been constantly increasing and how this need has been consistently reflected in the latest policy documents.

In December 2004, the Council finalized the **Civilian Headline Goal (CHG) 2008**, which pinpointed a number of key objectives: elaboration of key planning assumptions in addition to possible scenarios for stabilization and reconstruction, conflict prevention, strengthening of institutions and civilian support for humanitarian operations; a Capabilities Requirements List and assessment of national contributions; and finally, a CHG review process. Under the CHG, it was decided to set up Civilian Response Teams (CRTs). The Civilian Planning and Conduct Capability (CPCC) was established in Brussels with the objective of planning and conducting civilian missions under the authority of a civilian commander.[23]

In 2008, the European Council adopted a new **Civilian Headline Goal 2010**, which had the following aims: better training for the deployed personnel, enhancing the availability of secondable civilian personnel, refinement of available instruments, lessons learned process, improvement of security in field missions and more synergies between institutional actors. Finally, the CHG also resolved to carry forward work on information exchange requirements.[24]

In December 2011, the "**Strengthening Ties between CSDP and FSJ Road Map"** was established with the aim to reinforce links across institutions in the EU working at the intersection between internal and external security. Five areas of cooperation were outlined: 1) comprehensive situational awareness and intelligence support to the EU; 2) exchange of information and mutual support; 3) improving mechanisms in the decision-making process; 4) improving cooperation in planning EU external action; and 5) capabilities: human resources and training. Five years later (2016), the Crisis Management and Planning Directorate (CMPD) suggested that the Comprehensive Approach "might entail the need to blur the lines between internal and external security", and urged "an even closer

[22] Ibid.
[23] Council of the EU, Civilian Headline Goal 2008, doc. 15863/64, 7 December 2004, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015863%202004%20INIT
[24] Council of the EU, Civilian Headline Goal 2010, doc. 14823/07, 19 November 2007, https://www.consilium.europa.eu/uedocs/cmsUpload/Civilian_Headline_Goal_2010.pdf.

cooperation between all EU actors in the future in order to achieve better synergies and avoid duplication of efforts."[25] Because of this, it identified three prioritized areas for further progress: 1) improving situational awareness and exchange of Information within the EU; 2) operationalizing the nexus between internal and external security; and 3) civilian–military convergence and synergies.[26]

In July 2012, on the basis of the two CHGs, the EU adopted the multiannual **Civilian Capability Development Plan (CCDP)**, which aimed to shore up civilian capabilities in the context of current financial constraints.[27] The CCDP sought to resolve the existing gaps through concrete actions in four main domains: EU ambitions, national strategies, lessons learned and capability trends. The CCDP is still a lasting framework that will vary according to EU ambitions, political strategic context, operational feedback and other variables.[28]

In 2013, the Joint Communication on the **EU's comprehensive approach to external conflict and crises** put forward some concrete actions to provide a common understanding of the EU's comprehensive approach across the whole spectrum of EU actors dealing with conflict-related activities. The comprehensive approach called for a shared responsibility of all EU stakeholders involved in conflict prevention and management, to deal with all stages of the conflict cycle, from early warning, conflict prevention and response, to early recovery, stabilization and peace-building. The Joint Communication focused on aspects such as developing a shared analysis, defining a common strategic vision, focusing on prevention, mobilizing the different strengths and capacities of the EU, committing to the long term, linking policies and internal and external action, making better use of EU delegations and working in partnership. Specifically, it urged the development of "a shared analysis," improving combined situational awareness and analysis capacity. This should be done by better connecting the dedicated services, which include the Emergency Response Coordination Centre (based in DG ECHO) and the EU Situation Room (housed in the European External Action Service, the EEAS). The Joint Communication also suggested reinforcing early, proactive, transparent and regular information sharing and coordination among institutional actors.[29] In 2015, the **Taking Forward the EU's Comprehensive Approach to External Conflict and Crises: Action Plan 2015** prioritized three key issues:

[25] EEAS, CMPD Food for Thought Paper: From strengthening ties between CSDP/FSJ actors towards more security in EUROPE, doc. 10934/16, 5 July 2016, http://statewatch.org/news/2016/jul/eeas-food-for-thought-more-security-in-europe-10934-16.pdf.
[26] Ibid.
[27] Azzoni A. and Pirozzi N., Civili in missione: l'esperienza italiana nelle missioni dell'Unione europea, Roma, Nuova Cultura, March 2016, http://www.iai.it/sites/default/files/civili_in_missione.pdf.
[28] EEAS, Multi-annual Civilian Capability Development Plan: Action Lines for 2012-2013, doc. 12111/12, 6 July 2012, http://www.statewatch.org/news/2012/aug/eu-eeas-civilian-capability-action-plan-2012-2013-12111-12.pdf.
[29] European Commission and the High Representative of the European Union and for foreign affairs and security policy, Joint Communication to the European Parliament and the Council: The EU's comprehensive approach to external conflict and crises, Brussels, JOIN(2013) 30 final, 11 December 2013, http://www.eeas.europa.eu/archives/docs/statements/docs/2013/131211_03_en.pdf.

definition of a common strategic vision, mobilization of the different strengths and capacities of the EU and identification of the priorities of specific countries. In the annex of the document, however, other important initiatives were listed. One of these was "Sharing Information": while acknowledging the work of the EU Situation Room, it stressed the importance of enhancing cooperation through existing platforms, linking up EU institutions, agencies and member states and exchanging situational reports. It finally suggested facilitating access to intelligence products, including those produced by member states.[30]

In July 2016, the HR/VP Federica Mogherini presented the **European Union Global Strategy on Foreign and Security Policy (EUGS)**, suggesting that the EU will further improve its civilian missions by supporting force generation, make deployment faster and provide better training. The EU should also shore up its operational planning and streamline institutional structures, while integrating civilian and military structures, knowing that these forces might be deployed in the same operational context. The EU will also pursue better information-sharing, joint reporting, analysis and response planning between member state embassies, EU delegations, Commission services, EU Special Representatives and CSDP missions. Further, it will invest in the EU Conflict Early Warning System. Information and communication technologies should be used to gain a deeper situational awareness. Finally, EU external action should become more "joined up" across internal and external policies, as well as security and development policies. For example, to tackle migration, different external policies and other tools should be reconsidered to become more migration-sensitive and be coordinated with internal policies such as border management, internal security and asylum.[31]

In November 2016, the HR/VP presented the **Implementation Plan on Security and Defence,** a practical instrument to translate the vision outlined in the Strategy into concrete actions. The Implementation Plan reiterated the importance of effectively responding to conflict and crises through anticipation, situational awareness, enhanced civil/military intelligence and strategic foresight. In this regard, of particular importance is to prioritize the Hybrid Fusion Cell and CT analytical capacity in the Intelligence and Situation Centre (INTCEN) and to exploit the EU Satellite Centre. Civilian and military experts should reinforce the EU delegations' capacity of analysis. Civilian and military capacity building should be buttressed based on a more integrated EU approach. The Plan suggested revisiting the Feira priorities and evaluating how CSDP civilian missions can better respond to challenges such as migration, hybrid terrorism, cyber-attacks, organized crime and border management. To do that, the Civilian Capability Development process should be reinvigorated and, on the basis of the list of generic civilian CSDP tasks (see chapter 3.1), a list of required capabilities should

[30] Council of the EU, Joint Staff Working Document Taking forward the EU's Comprehensive Approach to external conflict and crises - Action Plan 2015, doc. 7913/15, Brussels, 14 April 2015, http://data.consilium.europa.eu/doc/document/ST-7913-2015-INIT/en/pdf.

[31] EEAS, Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign And Security Policy, ibid.

be outlined. Also necessary are faster force generation, improvement in training, but above all "strengthen[ing] capacities available for the generic functions common to all missions, such as in the area of command and control, information/strategic communication, mission support, including logistics (e.g. Mission Support Platform (MSP), a more ambitious warehouse concept) and duty of care."[32] There should also be revision of the existing structures to ensure a seamless planning and conduct, with a view to enhancing civilian and military synergies. In terms of situational awareness, the Plan proposes to enhance civil/military intelligence through the SIAC[33] as the main structure for strategic information, early warning and comprehensive analysis. Finally, the Implementation Plan invites the Union to strengthen partnerships with main international organizations such as the UN, OSCE, the African Union and partner countries. These proposals were later partially endorsed by the **Council Conclusions** on 14 November. The Council invited the HR/VP to review by Spring 2017 the priority areas of CSDP civilian missions, especially by considering when CSDP missions can have an added value in the context of EU's comprehensive approach; to enable the responsiveness of civilian crisis management through "strengthening capacities for the generic functions common to all missions and build on the establishment of the MSP as a part of an effort to take forward a Shared Services Centre concept;"[34] to shape the extant EEAS structure for the establishment of a permanent planning and conduct of CSDP missions to enhance civil–military synergies, with distinct but coordinated chains of command.[35] Finally, the Council invited EEAS and member states to contribute and reinforce the structures providing autonomous situational awareness to better inform EU decision making. On 6 March 2017, the **Council reviewed the implementation** of its November conclusions and took an important decision by approving the "Concept Note on the operational planning and conduct capabilities for CSDP missions and operations". In particular, the Council decided to establish a MPCC within Brussels' EUMS, as the body responsible for all non-executive military missions, to work in close collaboration with its civilian counterpart, the CPCC (see below); to create a JSCC with staff from both the CPCC and the MPCC, in order to enable effective civilian–military coordination. Finally, "Without prejudice to the tasks performed by the existing MSP", the JSCC would comprise the Watchkeeping capability (WKC) within EUMS, legal advice, expertise on UNSCR1325, Stratcom, Logistics, CIS, and Medical and Field Security.[36]

[32] Council of the EU, Implementation Plan on Security and Defence, 14392/16, Brussels, 14 November 2016, https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf.
[33] Functional arrangement between EU INTCEN and EUMS Intelligence Directorate (see section 2.3).
[34] To the best of our knowledge, the Shared Services Centre concept emerged in 2012, when the Council encouraged the EC and EEAS to take forward its establishment. In the latest conclusions on the topic (18/04/2016), the Council welcomed the establishment of the Mission Support Platform (MSP) in order to rationalize the provision of mission support functions, the improvement of early deployment, and the effective conduct of CSDP missions (see section 4.2).
[35] Council of the EU, Outcome of the Council Meeting, 3498th Council meeting, Foreign Affairs (including defence issues), 14418/16, Brussels, 14 and 15 November 2016, http://www.consilium.europa.eu/en/meetings/fac/2016/11/14-15/.
[36] Council of the EU, Outcome of the Council Meeting, 3525th Council meeting, Foreign Affairs, 7019/17, Brussels, 6 March 2017, http://www.consilium.europa.eu/en/meetings/fac/2017/03/06/.

There are some important takeaways from this section on the latest policy developments concerning EU CSDP civilian missions.

Firstly, there is now a clear intention from both EU practitioners and policymakers to pursue better situational awareness, information exchange and operational control to improve the conduct of EU CSDP civilian missions. Since 2008, all the major documents on the topic have stressed the importance of these elements to achieve EU CSDP objectives. The latest Council's conclusions have provided a clear political mandate to increase efforts in sharing information more effectively between actors involved in CCM, to achieve stronger results in intelligence gathering in order to have a full picture in crisis situations and to streamline the planning and conduct phase of CSDP civilian missions. Secondly, these documents propel EU actors involved in CCM to enhance synergies between them to tackle the complex security challenges the EU has to face. They distinctively ask for more links between the civilian and the military sides of CSDP, but also to enhance ties between CSDP and FSJ actors, the latter usually belonging not to EEAS but to institutions such as the European Commission and EU agencies. The underlying reason is to tackle security challenges along the internal-external continuum, whereby internal threats such as terrorism can be mitigated through external policies and interventions such as – but not limited to – CSDP missions.

The implications for a future OCP platform are straightforward. The most important is that there seems to be a clear political mandate to design and establish a tool dedicated to situational awareness, information exchange and operational control. The second relevant implication is that, in order for the EU to be an effective crisis manager in this increasingly perilous security context, a future OCP should be able to pursue its objectives by linking up the variety of actors engaged in CCM.

2.3 EU institutions in civilian crisis management

Following considerations in section 2.2, this part details the actors involved in civilian crisis management, with a particular attention on those institutions that are most relevant in CSDP civilian missions, which remains the focus of the CIVILEX project. This effort is done with a view to highlight the complex institutional system in which CSDP civilian missions interact with other EU institutions. This institutional complexity inevitably shapes how situational awareness, information exchange and operational control occur and should be envisaged. The immediate implication of having such a variety of actors is that the design of a possible platform should consider the technical difficulties of linking up actors that obey to different chain of commands, receive funds from different lines of the Union's budget, perform complementary but different tasks and pursue different agendas as they belong to different institution within the EU.

2.3.1 The European Council and the Council of the EU

At the highest level, there is the **European Council**, comprised of Heads of State and Government, which has the final word on every matter on foreign and security policy. The Lisbon Treaty introduced the figure of the **President of the European Council** who should chair and drive forward the work of the Council, as well as "ensure the external representation of the Union on issues concerning its common and security policy."[37] In spite of these new powers, some of the President's functions are essentially secretarial.[38]

Within the Council of the EU, the **Foreign Affairs Council** (FAC) acts as the main decision-making body for CFSP and CSDP. It meets monthly and is made up of all EU member states' foreign ministers.[39] The meetings of the FAC are organized and prepared by the **Committee of Permanent Representatives II** (**COREPER II**), usually composed of the permanent representatives of the EU member states.[40] The COREPER gathers at least once per week in Brussels and is seen as a considerable shaper of the European security/defence decision-making process: usually the FAC adopts without further debate what has been agreed upon in the COREPER.[41] The **Political and Security Committee** (**PSC**) is a Brussels body that became permanent in 2001, and that is made up of member states' ambassadors. The role of the PSC, according to the Treaty of Nice, is to monitor the international situation and formulate policies, providing feedback to the Council and the HR/VP. Under the authority of the Council, it can "take relevant decisions concerning the political and control and strategic direction" of crisis management operations.[42] The issue of hierarchical authority between the PSC and the COREPER was resolved in favour of the latter: formally, the COREPER is superior to the PSC, whose decisions pass via COREPER to FAC. If PSC ambassadors cannot reach a consensus on a certain topic, the COREPER has the final word.[43] Its work is supported by the "European Correspondents" within the member state MFAs, the Politico-Military Group and the "Nicolaidis" working group.[44] When it comes to specific decisions concerning civilian aspects, the **CivCom** play a key role, supporting the PSC, preparing planning documents, drafting recommendations and providing workable options for civilian crisis management. CivCom, in practice, is the civilian counterpart of the European Union Military Committee (EUMC) and is made of civilian and diplomatic representatives of EU member

[37] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art.15, Ibid.
[38] Howorth J., Security and defence policy in the European Union, Ibid.
[39] European Council and Council of the European Union, Foreign Affairs Council configuration (FAC), Last reviewed 24 January 2017, http://www.consilium.europa.eu/en/council-eu/configurations/fac/.
[40] European Council and Council of the European Union, Coreper II, Last reviewed 7 April 2016, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coreper-ii/.
[41] Howorth J., Security and defence policy in the European Union, Ibid.
[42] European Council and Council of the European Union, Political and Security Committee (PSC), Last reviewed 20 February 2017, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/.
[43] Howorth J., Security and defence policy in the European Union, Ibid.
[44] Ibid. The Politico-Military Group covers all aspects of EU military and civil–military issues.

states.[45] Established in May 2000, it is permanently chaired by the EEAS, and gathers in Brussels approximately three times per week.[46] Despite the generalist nature of the diplomats and representatives composing the CivCom, the body has progressively gained experience in the planning and conduct of civilian crisis management missions, contributing to raising awareness of the strong demand for EU civilian crisis management and of the consequent capability requirements in the national capitals.[47] The **RELEX working party** is also an important body within the Council as it deals with the legal and financial aspects of CFSP, including EU crisis management operations.[48]

2.3.2 The High Representative and the European External Action Service (EEAS)

The Lisbon Treaty also enhanced the role of the **HR/VP**, who also received the hat of Vice President of the Commission. According to the Treaty, the HR/VP shall:

- "conduct the Union's common foreign and security policy;"[49]
- "preside over the Foreign Affairs Council;"[50]
- "ensure the implementation of the decisions adopted by the European Council and the Council[51]; and
- "be assisted by a European External Action Service."[52]

The Treaty of Lisbon also established the EEAS, which "is intended to act as a unified diplomatic corps for the EU, in the service of both CFSP and CSDP". It has a staff of over 3,400 personnel and 140 Delegations around the world. It is organized around geographic and functional desks.[53] The key CSDP and crisis response bodies within the EEAS include: the

[45] The EUMC is the principal EU military body, comprising the Chiefs of the Defence Staff of member states, and meets at least biannually. The Chiefs are normally supplanted by their military representatives, who often have a double hat as NATO representative. Via PSC, the EUMC advises the European Council on the military dimension of different topics and issues. It reaches decisions unanimously. According to Mai'a Cross, expertise, common recruitment and culture, frequency of meetings and the ability to influence member states is exceptional. Cross continues: "since their primary goal is to execute successful CSDP operations, and provide for the common security of EU citizens, they realize that working together will be necessary for the EU to have efficient and effective planning and procurement, particularly in the light of declining populations and defence budgets". Howorth concludes that "there is little doubt that this key military committee of experts plays a fundamental role in the shaping of policy options on CSDP".

[46] European Council and Council of the European Union, Committee for Civilian Aspects of Crisis Management (CivCom), Last reviewed 20 March 2015, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/committee-civilian-aspects-crisis-management/.

[47] Howorth J., Security and defence policy in the European Union, Ibid.

[48] European Council and Council of the European Union, Working Party of Foreign Relations Counsellors (RELEX), Last reviewed 8 January 2015, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-foreign-relations-counsellors/.

[49] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art.18, Ibid.

[50] Ibid.

[51] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art.27, Ibid.

[52] Ibid.

[53] Howorth J., Security and defence policy in the European Union, Ibid.

CPCC, the **Crisis Management and Planning Directorate** (**CMPD**), the **Security Policy and Conflict Prevention** (**SECPOL**) **Directorate** and the **EU Analysis Intelligence Centre** (**INTCEN**). All four Directorates report to the Deputy Secretary-General for crisis response and CSDP. Finally, the Lisbon Treaty established the **EU Delegations**, under the authority of the HR/VP.

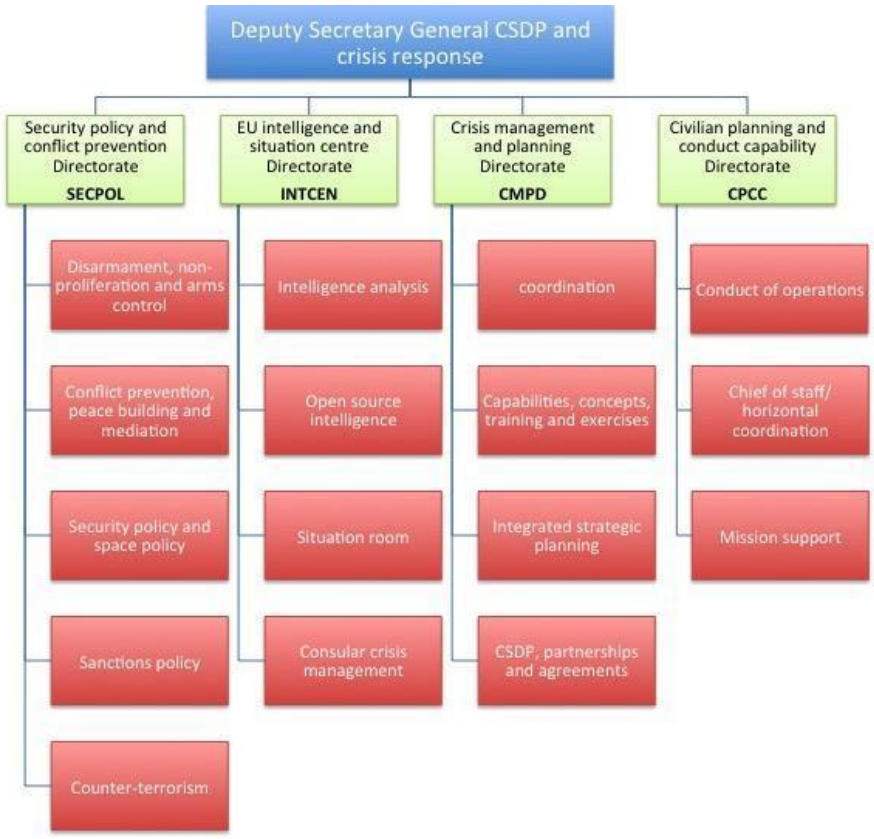

Figure 1 - Organisational Chart CSDP

The **CPCC** is the Brussels-based permanent headquarters devoted to the planning and conduct of civilian missions, thus the key body within the EEAS dealing with CSDP civilian crisis management (68 personnel in Brussels).[54] Created in 2007, the CPCC is headed by the Director and Civilian Operation Commander (CivOpCdr), who is essentially responsible for the operational planning, command and control of all the EU civilian missions. The Civilian Operations Commander is under the political control and strategic direction of the PSC and the overall authority of the HR/VP.[55] Among its main tasks, the CPCC: provides inputs to the crisis management concepts (CMC) for CSDP civilian missions including the development of Civilian Strategic Options (CSO); develops the legal framework for the different CSDP civilian missions; implements the "Force Generation Process" of the CSDP civilian missions; assists the Civilian Heads of mission in developing the Operation Plan (OPLAN) and the deployment plan of the mission; monitors and follows up and evaluates the CSDP civilian missions and

[54] Ibid.
[55] Ibid.

ensures adequate reporting; develops and maintains links with EUMS; and establishes and maintains links with member states, international organizations and relevant third states in order to channel the exchange of mission-specific information, and ensure co-ordination on operational issues with other actors in international crisis management. The CPCC comprises three divisions. The CPCC.1 ("Conduct of Operations Divisions") is in daily contact with the missions, and ensures that the political objectives of the missions' mandate are met. It is responsible for the revision of the OPLAN in line with CivCom and PSC recommendations. The CPCC.2 ("Chief of Staff/Horizontal Co-ordination Division") manages coordination of daily issues. It is divided into the Operational Capability Section, which provides guidance on lessons learned and operational guidelines, and the Operational Planning Section, which establishes Planning Teams to develop CONOPS and OPLAN. The CPCC.3 ("Mission Support Division") copes with the management of staff and the procurement, finance and legal elements of a mission.[56]

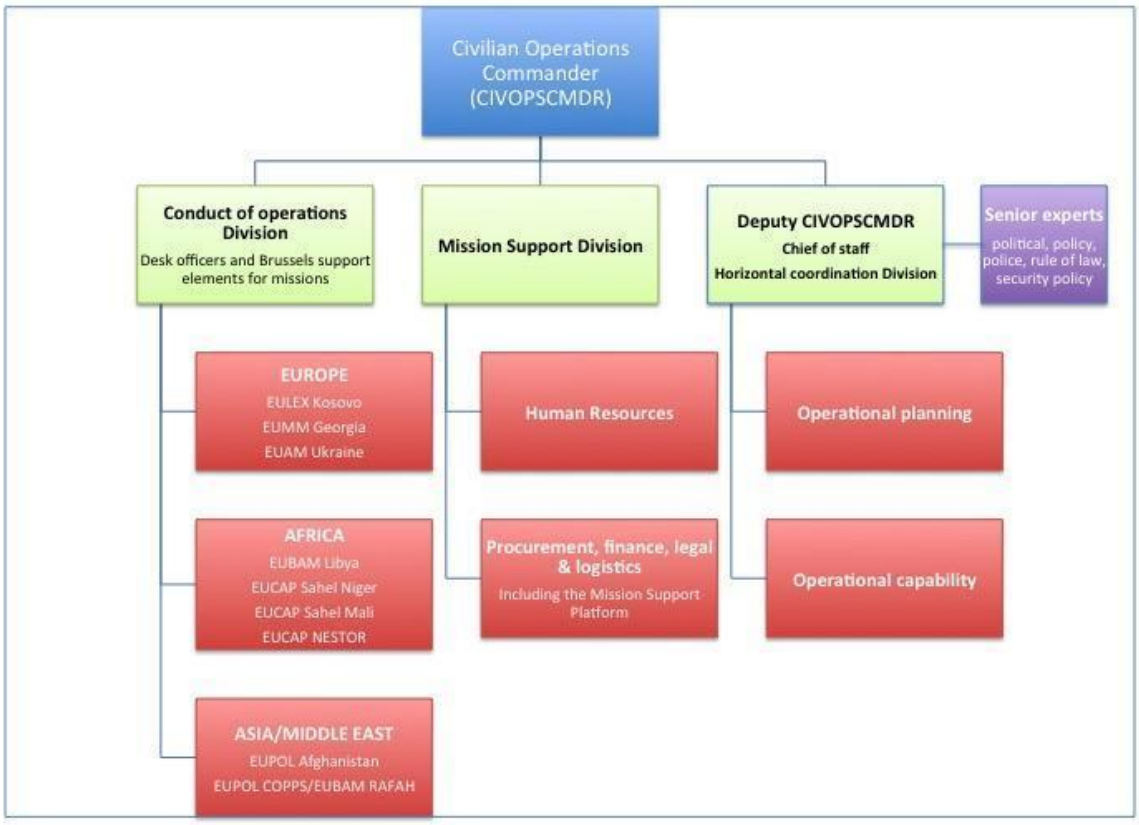

Figure 2 - Organisational Chart CPCC

The **CMPD** was created in 2009 and is the body in charge of the civilian–military integrated planning within EEAS. It works under the political authority of the PSC. The CMPD is tasked with the strategic planning of CSDP missions and operations, for which it produces the CMC, the foundation of operational planning and the conduct of the mission. It reviews extant missions (mandate, sustainability, objectives, size, etc.) in relation to the changing security

[56] Ibid.

environment. It develops partnership with international organizations (NATO, OSCE, UN, African Union, etc.) and third states. It oversees the development of civilian and military capabilities, seeking synergies between the civilian and the military sides.[57]

The **Security Policy and Conflict Prevention** (**SECPOL**) **Directorate** promotes the Comprehensive Approach in dealing with external threats. It has four focuses: disarmament, security policy, sanctions policy and conflict prevention, peacebuilding and mediation. The SECPOL.2 ("Conflict Prevention, Peace building and Mediation" division) runs the EU early warning system, which is a risk management/situational awareness tool with the goal of averting a conflict before it erupts.[58]

The **EU INTCEN**, the only civilian intelligence capacity of the EU, provides intelligence alongside its military counterpart (EUMS Intelligence Directorate) to CSDP bodies.[59] INTCEN's mission is to provide intelligence analysis, early warning and situational awareness. The body offers its services to the HR/VP, other EU decision-making institutions, and also to CSDP missions. It provides information based on member states' contribution as well as open-source information and is the single point of entry for classified information coming from member states' intelligence/security services.[60] It houses the EU Situation Room, a permanent body delivering worldwide monitoring 24/7, year round. It is the information hub that collects and spreads data collected by EU delegations, member states, EU CSDP missions and operations, EU Special Representative (EUSR) teams and international organizations. It is said to be the first point of contact for all crisis-related situations and it has a role also in the EU Integrated Political Crisis Response (IPCR), supporting coordination in complex crises.[61] In the same physical space as the SitRoom, one can also find the WKC which, despite its collocation, it is under the authority and part of the EUMS chain of command. As such, it is *de-facto* a hybrid unit with both military and civilian staff, which constitutes an information hub for all CSDP missions (see section 4.2). The WKC monitors all CSDP missions, alerts Brussels CSDP stakeholders in case of crisis and carries out information management (reports, tracking, archiving). In spite of the different chain of command, WKC and SitRoom are linked and share all relevant information.[62] According to the latest FAC conclusions, the WKC will be part of the newly established JSCC (see section 2.2).

[57] EEAS, CSDP structure, instruments, and agencies, Last reviewed 8 July 2016, http://eeas.europa.eu/csdp/structures-instruments-agencies/cmpd/index_en.htm#sp.
[58] EEAS, Conflict Prevention, Peace building and Mediation, Last reviewed 15 June 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/426/conflict-prevention-peace-building-and-mediation_en#Conflict+prevention.
[59] European Security and Defence College, Handbook for Decision Makers: The Common Security and Defence Policy of the European Union, 2014, http://eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/european-security-defence-college/pdf/handbook/handbook-for-decision-makers.pdf
[60] European Union Delegation to the United Nations – New York, Factsheet on EU Intelligence Analyses Center (INTCEN), http://eu-un.europa.eu/factsheet-on-eu-intelligence-analyses-center-intcen/
[61] EEAS, EU Crisis Response System, https://eeas.europa.eu/headquarters/headquarters-homepage/412/crisis-management-and-response_en#The+EU+Situation+Room.
[62] EEAS, Interviews, 20 October 2016.

There are **140 EU delegations** across the world, housing EEAS, EC and seconded national experts. In 2015, EU delegation staff numbered 5,438, of whom 36% came from EEAS and the remaining 64% from the EC. Security and defence experts/advisors were posted in 20 delegations in 2015, especially in Africa and the Middle East.[63] EU delegations have gained an important role in CSDP missions as they supply information on what is happening in the field and on all the stakeholders involved, which is paramount in the launch of a mission.[64] The Head of Delegation is in principle an important interlocutor for the Head of CSDP mission or operation in a specific country, but this collaboration relies heavily on personal relationships.

2.3.3 The European Commission

The European Commission has a direct role in civilian crisis management as it takes over responsibility for operational expenditure.

The Service for **Foreign Policy Instruments (FPI)** works under the authority of the HR/VP and ensures that CFSP operations correctly employ the budget at their disposal, and provide guidance to CSDP missions. After having prepared a budgetary impact assessment for each CSDP mission, it asks for endorsement from the RELEX Counsellors group. The FPI supports the missions in financial and budgetary matters and checks procurement processes; in addition, it represents the Commission within RELEX and CivCom.[65] The service is structured in units: FPI.2 IcSP, an EU instrument to support security initiatives and peace-building activities in partner countries through dedicated projects; FPI.1 is the office entitled to Budget, Finance and Relations with other Institutions; and FPI.3 is the Common Foreign and Security Policy Operations unit, which prepares a budgetary impact statement for each EUSR and CSDP mission and Non-Proliferation and Disarmament (NPD) projects.

Within the Commission, the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO), the Directorate-General for International Cooperation and Development (DG DEVCO), the Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) and the Directorate-General for Migration and Home Affairs (DG HOME) are four other important EU commission services that should be considered in the design and implementation of an OCP platform. These actors are important to mention as they often work side by side with CSDP missions personnel, with profound implications in terms of information sharing and situational awareness. In the light of the recent strategic and policy documents such as the EUGS and the Implementation Plan,

[63] European Union Institute for Security Studies, EUISS Yearbook of European Security (YES) 2016, 2015, http://www.iss.europa.eu/uploads/media/YES_2016.pdf.
[64] Azzoni A. and Pirozzi N., Civili in missione: l'esperienza italiana nelle missioni dell'Unione europea, Ibid.
[65] European Commission, Service for Foreign Policy Instrument (FPI), Last Update 12 January 2016 http://ec.europa.eu/dgs/fpi/about/index_en.htm.

a future information system will have to facilitate a more "joined-up" approach to strengthen the security–development nexus and facilitate between the relevant Commission services and CSDP actors.

DG ECHO is headquartered in Brussels and has a global network of field offices (48 field offices in 40 countries); it brings under one directorate-general two main instruments of EU crisis response: humanitarian aid and civil protection.[66] **DG DEVCO** designs and implements EU international cooperation and development policies with the objective of reducing poverty, ensuring growth and social and environmental development, and promoting democracy, the rule of law and good governance. EU development policy is framed within the EU's external action and is jointly defined by the EEAS and DEVCO.[67] Commission actors are located in EU delegations, where they manage and implement development and cooperation programmes.[68]

In addition to the development and humanitarian aid/civil protection services, other directorates within the Commission have assumed a greater role in EU external action, namely DG NEAR and HOME. **DG NEAR** works closely with EEAS to take forward the EU's neighbourhood and enlargement policies. It assists and supports reform and democratic consolidation of eastern and southern neighbours by implementing assistance actions. Based in Brussels, it has 1,650 staff deployed in Brussels or in EU delegations in partner countries.[69] **DG HOME** manages policies that aim at ensuring security to EU citizens, through supporting police and judicial cooperation, promoting dialogue and cooperation with non-EU countries and developing a balanced and comprehensive EU migration policy based on solidarity and responsibility. Furthermore, DG HOME funds the decentralized agencies mentioned below.[70]

2.3.4 European Union agencies in civilian crisis management

Finally, and also in light of recent policy development on the necessity to strengthen external and internal policies, other important actors should be taken into account: the European Police Office (Europol), European Border and Coast Guard Agency (Frontex), the European Asylum Support Office (EASO), the European Union's Judicial Cooperation Unit (Eurojust) and the EU SATCEN.

Europol is the EU's law enforcement agency with the goal to assist EU member states in the

[66] DG ECHO, Who we are, http://ec.europa.eu/echo/who/about-echo_en.
[67] DG DEVCO, About International Cooperation and Development - DG DEVCO, Last update 3 April 2017, http://ec.europa.eu/europeaid/general_en.
[68] DG DEVCO, Relations with the EEAS, EU institutions and Member States, Last update 3 April 2017, http://ec.europa.eu/europeaid/relations-eeas-eu-institutions-and-member-states_en.
[69] DG NEAR, Who we are, Last update 6 December 2016, https://ec.europa.eu/neighbourhood-enlargement/about/directorate-general_en.
[70] DG HOME, Who we are, Last update 3 April 2017, https://ec.europa.eu/home-affairs/who-we-are/about-us_en.

fight against serious international crime and terrorism.[71] As seen above in the document on "Strengthening ties between CSDP and FSJ Road Map", already in 2011 Europol was preparing to collaborate more closely with CSDP police missions, in order to promote law enforcement best practices in countries outside the EU, introduce intelligence policing techniques in CSDP missions, increase information exchange with police as well as civilian missions more generally and elaborate a working mechanism with INTCEN. Also in its 2016 Work Programme, Europol recognized "initiatives aimed at strengthening the ties between external (CSDP) and internal security (FSJ), which will provide the opportunity for Europol to enhance cooperation with the EEAS, its crisis management structures and CSDP missions and operations" as relevant factors to be considered in the definition of 2016 objectives.[72]

Frontex is the EU agency that coordinates and develops European border management. In addition to its analysis tasks, the Agency coordinates and organizes border interventions, supports search and rescue operations, deploys European Border and Coast Guard teams, fights organized crime and terrorism in cooperation with Europol and Eurojust, develops and uses information systems that allow information sharing concerning border management, while cooperating with the Commission, Union Bodies, offices and agencies.[73] An example of the increasing collaboration between the agency and CSDP is Operation Triton, in close collaboration with EUNAVFOR MED, which was launched in June 2015 to cope with the increasing flow of migrants coming from the Central Mediterranean Route.[74]

The main role of **EASO** is to foster cooperation with and between member states in the implementation of the Common European Asylum System. The agency also supports the work of Europol and Frontex in the field of migration, in direct or indirect coordination also with CSDP Missions (see EUNAVOR MED case study).[75]

Eurojust coordinates investigations and prosecutions between the competent authorities in the member states and improves the cooperation between these authorities, in particular by facilitating the execution of international mutual legal assistance agreements and the implementation of extradition requests. In relation to migration, the Agency has started to cooperate with CSDP Missions in the establishment of Joint Investigations Teams between Europol/Eurojust and CSDP missions. The feasibility of posting liaison officers and magistrates in third countries is still being considered.[76]

[71] Europol, About, https://www.europol.europa.eu/about-europol.
[72] Europol, Europol Work Programme 2016, EDOC # 736915v18A, The Hague, 3 February 2016, https://www.europol.europa.eu/publications-documents/europol-work-programme-2016.
[73] Frontex, Mission and Tasks, http://Frontex.europa.eu/about-Frontex/mission-and-tasks/
[74] Ministero della Difesa – Marina Militare, EUNAVFOR MED Operation Sophia - Situazione, http://www.marina.difesa.it/cosa-facciamo/operazioni-in-corso/Pagine/EUNAVFORMED.aspx.
[75] EASO, European Asylum Support Office: Who we are, https://www.easo.europa.eu/sites/default/files/EASO-Brochure-EN%20.pdf.
[76] EUROJUST, Mission and tasks, http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx.

The **EU SATCEN** supports the decision making of the EU in the field of CFSP, in particular CSDP, including EU crisis management missions and operations, by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite imagery and aerial imagery, and related services.[77]

2.4 The *decision-making process of CSDP civilian missions*

This section outlines the decision-making process that leads to the establishment of a CSDP civilian mission. It highlights and reinforces the argument that CSDP civilian missions take place in a wider CCM management environment with a convoluted decision-making and complex systems of interactions between EU Brussels-based actors. The implication is that a future OCP should be designed in accordance with taking into account such a decision-making process, connecting the various actors involved in it.

The planning and start of a CSDP civilian mission is a complex process in which many of the actors introduced above are involved. The process is developed around the drafting and approval of certain documents:

1) Crisis Management Concept (CMC)
2) Concept of Operations (CONOPS)
3) Operations Plan (OPLAN)
4) Council decision

Only after all four items are approved can the mission start.[78]

The EEAS Crisis Response & Operational Coordination Department activates the EEAS Crisis Response System (CRS), whose main goal is to ensure coherence in the management of a crisis. The Department is divided into three parts: 1) Crisis Response Planning and Operations; 2) the EU Situation Room; and 3) the Consular Crisis Management. Part of the CRS is the Crisis Platform, which is intended to provide clear political guidance in the management of a crisis. The Platform can assemble various EEAS departments (CMPD, CPCC, INTCEN), EUMS, EUMC and the relevant commission services (FPI, ECHO, DEVCO, etc.).[79]

[77] EU SATCEN, The Centre, https://www.satcen.europa.eu/about_the_eu_satcen/the_centre.
[78] EEAS, Interviews, 13 December 2016.
[79] EEAS, EU Crisis Response System, Last reviewed 15 June 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/412/crisis-management-and-response_en#Crisis+Response+System.

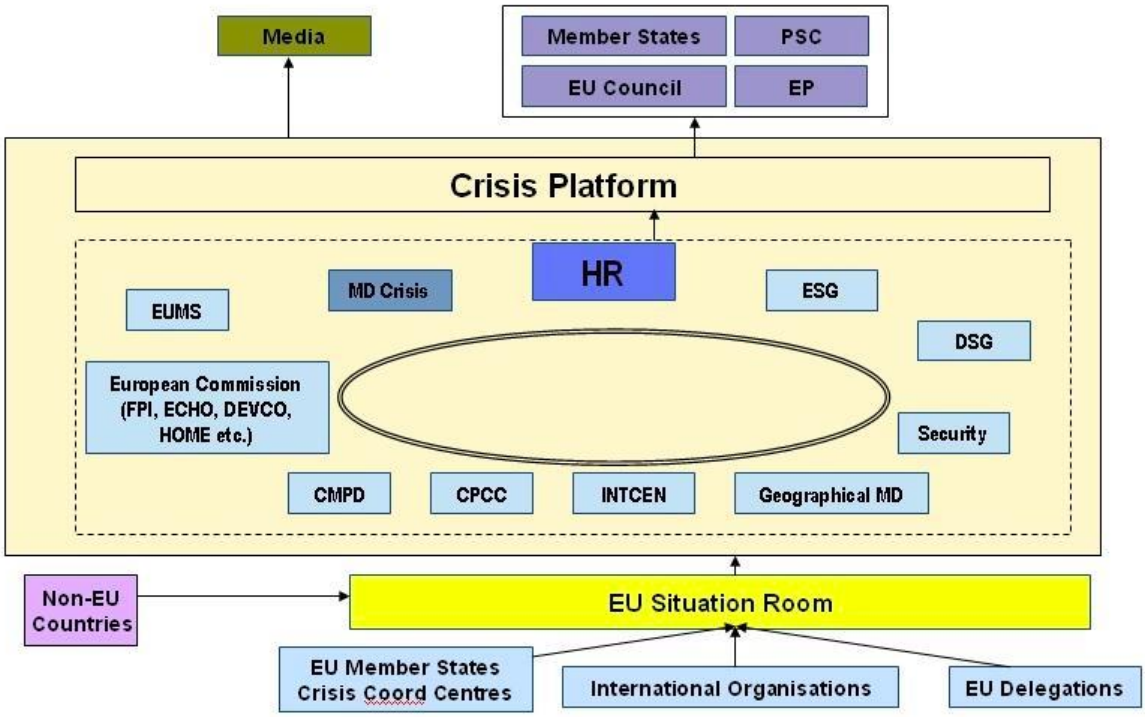

Figure 3 - EEAS Crisis Platform

If there is room for a CSDP mission, member states in the PSC invite the HR/VP and EEAS to redact a CMC, an EU restricted document that outlines the options for a CSDP activity, describes the phases of the mission, presents the possible risks and defines the potential Exit Strategy. In addition, the CMC deals with organizational aspects, providing guidance with respect to Command & Control (C2), coordination, resources, financing and communication strategy. The CMC is developed by the CMPD.[80]

The PSC has a debate on the CMC and asks for advice from the CivCom. After the PSC agrees on the CMC, it sends it with all the different options and specifics to the COREPER. After consensus is found in the COREPER, the Council generally adopts the CMC. On the basis of the CMC, the Council asks the PSC to develop strategic options for the mission.[81]

The PSC asks CivCom to produce some Police Strategic Options (PSO) and other CSO. CivCom then works out PSOs and CSOs with the support of CPCC and later sends them to the PSC, which evaluates these priorities and then sends a draft to the COREPER/Council.[82]

The Council decides on a Joint Action that requires the mandate, its objectives and financial requirements, and tasks the PSC to start the operational planning. The PSC asks the CPCC to provide operational planning on a range of police and civilian measures. The CPCC then

[80] EEAS, CSDP structure, instruments, and agencies, http://eeas.europa.eu/csdp/structures-instruments-agencies/cmpd/index_en.htm#sp; Azzoni and Pirozzi, Civili in missione: l'esperienza italiana nelle missioni dell'Unione europea, Ibid.
[81] EEAS, Interviews, 13 December 2016.
[82] Ibid.

submits a provisional CONOPS to the CivCom, which presents it to the PSC. After the PSC's approval, the Council has to approve the CONOPS and then asks the PSC to develop the final OPLAN.[83]

Since 2013, the CPCC Civilian Operations Commander is in charge of drafting the OPLAN with the support of the Head of Mission (HoM).[84] The OPLAN is then presented to the CivCom. In the meantime, the process of "force generation" starts. The CivCom then presents the OPLAN to the PSC, which has to agree on it and then send it to the Council.[85] It should be noted that in case of urgency the CONOPS and OPLAN can be merged in a single document (the so-called "CONOPS PLUS"), to speed up the process.[86]

After Council's approval of the OPLAN or CONOPS PLUS, the operation is ready to be launched.[87]

2.5 Institutional challenges for a future OCP platform: Findings from interviews in Brussels

The outlined institutional complexities, as well as the plethora of actors composing the EU civilian crisis management system, make information exchange, situational awareness and operational control in CSDP civilian missions not an easy task.

According to some interviewees, actors are so diverse that it would be too difficult to conceive a system able to connect them all. In this sense, although appealing, the notions of "civilian external action" or "civilian crisis management" that might result from the combined action of the aforementioned actors are artificial, as the actors that compose this ecosystem have quite different tasks, mandates and chains of command. In this sense, the interviewees considered that trying to link all them in a unique system would prove extremely challenging.

Nonetheless, improvements to better connect CSDP Brussels entities with missions in the field, as well as Brussels structures with the relevant European Commission services are possible. As expressed above, Commission services such as DEVCO and ECHO all have a strong operational dimension that needs to be addressed not only once a CSDP civilian mission is deployed, but also during the planning phase. In this sense, reconciling strategic planning between the CSDP and Commission structures had been difficult but seems

[83] Ibid.
[84] Ibid.
[85] EEAS, Interviews, 13 December 2016.
[86] Azzoni A. and Pirozzi N., Civili in missione: l'esperienza italiana nelle missioni dell'Unione europea, Roma, Ibid.
[87] EEAS, Interviews, 13 December 2016.

desirable also in light of the recent strategic/policy documents that encouraged a more "joined-up" EU external action.[88] Moreover, interviewees highlighted that connecting actors and entities such as the EU delegations, EC services and CSDP civilian missions, and possibly JHA actors, in the field should be treated as a matter of priority.[89]

Within EEAS, structural changes are occurring on how to improve situational awareness and to better conduct and manage operations through renewed institutional synergies. Recent developments at the strategic level have brought attention to communications and reporting. In this sense, the need to build bridges between EEAS and CSDP civilian missions has been expressed several times, so that CSDP missions should not be left isolated from Brussels.[90] It is important to highlight that, as of now, EEAS does not provide IT equipment to the missions, which all procure independently their own IT architecture and systems, as well as develop their own internal procedures. As a matter of fact, in EU CSDP civilian missions, IT management has not been yet standardized.[91] One interviewee suggested that EEAS should provide IT equipment to CSDP missions as well, as it does to the Delegations.[92] However, also within EEAS, there is at the moment no centralized IT system (and thus high fragmentation) and many interviewees have strongly suggested there should be rapid improvements in information exchange practices, interoperability and security awareness.[93]

An important role when it comes to CSDP missions and their IT systems is played by the Council, in particular the RELEX working group. Member states have an important role in influencing how the missions are financed, with the consequent impact of determining the availability of funding for information systems. One interviewee pointed out difficulties in obtaining the financial means to develop proper IT equipment. Reportedly, attempts to advocate for more funding to be spent on a more centralized CPCC IT system have been made, but without success.[94] One interviewee suggested that the Council has a great power in this area and that it heavily scrutinizes missions' expenditures, suggesting that this kind of scrutiny does not occur in many other policy areas.[95] At the Council level, CSDP-related information is usually accessed through the relevant CSDP bodies in Brussels and rarely from the mission directly, since the Council is mainly interested in strategic information that is relevant for its decision-making process rather than operational information.[96]

[88] EEAS, Interviews, 13 December 2016.
[89] EEAS, Interviews, 7 July 2016.
[90] EEAS, Interviews, EEAS, 6 December 2016.
[91] EEAS, Interviews, EEAS, 7 July 2016.
[92] Ibid.
[93] EEAS, Interviews, 6 December 2016.
[94] EEAS, Interviews, 7 July 2016.
[95] EEAS, Interviews, 23 August 2016.
[96] EEAS, Interviews, 6 September 2016.

3 Current state and evolution of CSDP civilian missions

> "*The Common Security and Defence Policy is best understood not in terms of institutions or of capacity, but in terms of what it does. Between January 2003 and late 2013, […] the EU launched no fewer than 32 overseas 'crisis management' missions. That is what CSDP does, and ipso facto, what it is*."[97]

Notwithstanding the idea of thinking globally expressed in the European Security Strategy (2003), it is clear that of the 21 civilian missions deployed so far, only a few were outside the European neighbourhood.[98] Currently, 10 out of 16 CSDP missions are civilian.[99] Most of them deal with capacity building and reinforcement of the rule of law, while others are about SSR and good governance, or have a security dimension with a focus on the fight against organized crime and terrorism, border and illegal immigration management or, finally, anti-piracy and maritime capacity.[100]

This chapter presents a general overview of CSDP civilian missions once they are deployed in the field. The scope of this exercise is to highlight missions' tasks and related needs in terms of situational awareness, information exchange and operational control and to shed light on

[97] Howorth J., Security and defence policy in the European Union, Ibid.
[98] In addition to these 21 civilian missions, 12 other military missions have been launched since 2003.
[99] The current military missions are: EUTM RCA Central African Republic (2016 -); EUNAFOR MED Mediterranean (2015 -); EUTM Mali (2013 -); EUTM Somalia (2010 -); EU NAVFOR ATALANTA Somalia (2008 -); EUFOR ALTHEA Bosnia Herzegovina (2004 -).
[100] Tardy T., Recasting EU civilian crisis management, EUISS Report, N.31, 01 March 2017, http://www.iss.europa.eu/uploads/media/Report_31.pdf.

their potential evolution after the release of the EUGS and the Implementation Plan on Security and Defence. In doing so, section 3.1 broadly outlines the current CSDP civilian missions and, also with the help of the "List of generic civilian CSDP tasks," identifies their related tasks; section 3.2 takes a deeper look at missions' tasks and needs by delving into selected case studies; finally, section 3.3 reflects on how the recent policy changes spurred by the EUGS and the Implementation Plan might effect civilian crisis management in the years to come.

3.1 The current state of CSDP civilian missions: mandates, objectives and tasks

This section describes the current civilian mandates and tasks, with the objective to broadly define the activities and goals a future OCP platform should support. Mandates and tasks are the basis according to which the CIVILEX project will derive requirements (D.3.1), foresee technical options (D4.1) and present recommendations (D5.3).

As said above, 10 of the current 16 CSDP missions are civilian. These missions are:

Name of the Mission	Start	Mandate and Objectives
1) EUAM Ukraine[101]	2014	To assist Ukrainian authorities in the reform of the civilian security sector
2) EUCAP Sahel Mali[102]	2014	To provide assistance and advice to the national police, the national gendarmerie and the national guard in the implementation of the security reform
3) EUBAM Libya[103]	2013	To support Libyan authorities in border management and security
4) EUCAP Nestor	2012	To assist host countries (now mainly Somalia) to develop capacity to improve maritime security, including anti-piracy and maritime governance; to reinforce coast guard functions; and to strengthen rule of law and judiciary
5) EUCAP Sahel Niger[104]	2012	To advice and train Niger's authorities to reinforce their security capability in the fight against terrorism and organized crime

[101] EUAM Ukraine, Our Mission, http://www.euam-ukraine.eu/en/what-we-do/our-mission
[102] EEAS, The EUCAP Sahel Mali civilian mission, Updated: June 2016, http://eeas.europa.eu/csdp/missions-and-operations/eucap-sahel-mali/docs/factsheet_eucap_sahel_mali_en.pdf
[103] EUBAM Libya, Factsheet, https://eeas.europa.eu/csdp/missions-and-operations/eubam-libya/pdf/factsheet_eubam_libya_en.pdf.
[104] EEAS, The EUCAP Sahel mission, Updated April 2016, ibid.

6) EUMM Georgia[105]	2008	To ensure no return of hostilities (stabilization) on the border between Georgia, South Ossetia and Abkhazia (normalization), to build confidence among warring parties and to advise EU policy in Georgia
7) EULEX Kosovo[106]	2008	To monitor, mentor and advise Kosovo's rule of law institutions and ensure rule of law is provided until Kosovo's institutions assume full responsibility
8) EUPOL Afghanistan	2007	To support the Afghan government to build civilian police in the context of improved rule of law and respect of human rights; reform of the Ministry of Interior and the Afghan National Police (local training capacity and institutions)
9) EUPOL COPPS Palestinian Territories[107]	2006	To support the Palestinian civil police reform and development, and the criminal justice system, to improve prosecution–police interaction
10) EUBAM Rafah Palestinian Territories[108]	2005	To provide a third-party presence on the Rafah Crossing Point and to build confidence between the Israeli government and the Palestinian Authority

Table 1 - Overwiew of current CSDP civilian missions

Based on these current and past operational experiences, as well as CHG 2008 and 2010, a "List of generic civilian CSDP tasks" was developed to detail a series of tasks that can be expected to be performed in CSDP civilian missions regardless of their mandate. With reference to situational awareness, information exchange and operational control, the Generic List provides useful information on what a mission is supposed to do:

1) Command & Control ("initiating, conceiving, enabling, monitoring and directing missions across the chain of command"): undertake political-strategic planning through the redaction of the CMC; undertake operation planning through the translation of the CMC in CONOPS, OPLAN and the Mission Implementation Plan (MIP), which details the activities of the mission; preparing the budget; execution and control of the mission through reporting, analysis and direction to the mission; process lessons and best practices; and, finally, evaluate;
2) Engage & Implement (mandate delivery, engagement with local authorities and other

[105] EUMM Georgia, Our Mandate, https://eumm.eu/en/about_eumm/mandate.
[106] EULEX Kosovo, EULEX implements its mandate through two operational objectives, http://www.eulex-kosovo.eu/?page=2,44.
[107] EUPOL COPPS, Mandate: "EUPOL COPPS is the European Union Co-ordinating Office for Palestinian Police Support", http://eupolcopps.eu/en/content/what-eupol-copps.
[108] EU Council, EU Border Assistance Mission at Rafah Crossing Point (EUBAM RAFAH), Updated: March 2009, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/wgme/dv/13_factsheeteubamrafahversion10_/13_factsheeteubamrafahversion10_en.pdf.

stakeholders): plan and undertake the activities agreed in the MIP; coordination and cooperation with other stakeholders (EU actors, international organizations, civil society);

3) Inform ("gathering, analysing and transmitting information"): provide situational awareness through the assessment of the situation in the field;
4) Set Up & Sustain ("enabling a civilian CSDP"): conduct deployment planning; manage human resources, finances, procurement and logistic support; develop communication and information systems through organization of command and control system, command and control communication system, command and control information systems (EUCCIS), directing configuration management.

3.2 "From mandates to action: selected CSDP missions case studies"

Despite the common general tasks described above, missions can be very heterogeneous in terms of objectives, length, personnel deployed, capabilities, quantity of data to be exchanged, stored and retrieved. For these reasons, the CIVILEX project decided to analyse five case studies in order to gain a deeper understanding of how missions are run and how info management and communication issues are addressed. The five case studies are: 1) EUCAP Nestor,[109] 2) EUNAVFOR Atalanta 3) EUCAP Sahel Mali and Niger, 4) EULEX Kosovo, and finally 5) EUNAVFOR MED Operation SOPHIA. These operations and missions were chosen because of several factors: EUCAP Nestor as a civilian mission in a complex security environment interacting, under the coordination of the EU Operations Centre (EU OPCEN), with two EU military missions such as EUNAVFOR Atalanta and EUTM Somalia; EUCAP Sahel Mali and Niger as two civilian missions interacting with an EU military mission (EUTM Mali), under the coordination of the EU OPCEN after 2014; EULEX Kosovo as the most extensive EU civilian mission, with executive powers, ever to be deployed in EU CSDP history; and finally, EUNAVFOR MED as a military mission being deployed in the policy context of the EU internal–external security nexus, where a previous civilian mission was already operating (EUBAM Libya).

Launched in 2012, **EUCAP Nestor** is a civilian maritime capacity-building operation with initial activities in five states of the Horn of Africa and Western Indian Ocean (Djibouti, Somalia, Seychelles, Kenya and Tanzania).[110] EUCAP Nestor initially aimed at "[assisting] the development in the Horn of Africa and the Western Indian Ocean States of a self-sustainable capacity for continued enhancement of their maritime security including counter-piracy, and

[109] The complete "EUCAP Nestor case study" is the subject of D2.2. For the purpose of D2.1, here follows a brief overview.
[110] Council of the EU, Council Conclusions on the Mission Support Platform, 18 April 2016. http://www.consilium.europa.eu/en/press/press-releases/2016/04/18-fac-mission-support/

maritime governance."[111] In 2015, following a strategic review, it was decided to gradually phase out activities in the broader Horn of Africa to focus exclusively on Somalia, leading therefore to a relocation of the Mission Headquarters (MHQ) from Djibouti to Mogadishu.[112] An unarmed civilian mission with no executive powers, EUCAP Nestor's tasks include strategic and operational advice, law drafting support and mentoring for the Somali Coast Guard.[113] Since the review of its mandate in 2015, the mission has scaled up its engagement in Somalia and now also provides support in the implementation of legislation as well as capacity-building activities for the country's judicial and prosecution actors, particularly those responsible for investigation and prosecution of suspect pirates.[114]

In total, EUCAP Nestor has a planned capacity of 176 staff members (137 international and 39 national staff).[115] The HoM and the Head of Operations are based in the MHQ in Mogadishu. The mission currently has personnel deployed in Mogadishu (which also functions as a field office) as well as in the field office in Hargeisa (Somaliland), from which operational activities are executed by the mission's maritime, legal and police experts.

Two other CSDP operations are active in Somalia: EU Naval Force (EUNAVFOR) Somalia-operation Atalanta and the EUTM in Somalia. In light of implementing the EU's Horn of Africa Strategy, the diversity of actors, including both civilian and military, each with their own mandates, organizational structures and lines of command, brings specific needs and challenges for coordination and information exchange in order to implement a coherent EU-wide response to the situation in Somalia. To coordinate these efforts, the Strategy called for the appointment of a EUSR for the Horn of Africa.

In addition to EU actors, there are a number of international organizations active in the region, which pose additional coordination challenges. These notably include the African Union Mission in Somalia (AMISOM), the United Nations Assistance Mission in Somalia (UNSOM) and the NATO maritime anti-piracy operation Ocean Shield.

Most of the information exchange both inside the EUCAP Nestor mission and between the mission, the Brussels level and other partners, happens via email and attachments. Large

[111] Council Decision 2012/389/CFSP of 16 July 2012 on the European Union Mission on Regional Maritime Capacity Building in the Horn of Africa (EUCAP NESTOR), Official Journal of the European Union, L 187/40, Art. 2., 17 July 2012, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede121112cd389_/sede121112cd389_en.pdf

[112] Council Decision 2012/389/CFSP of 16 July 2012 on the European Union Mission on Regional Maritime Capacity Building in the Horn of Africa (EUCAP NESTOR) (OJ L 187, 17.7.2012, p. 40), 7 December 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02012D0389-20151207&qid=1473075547345&from=EN

[113] Ibid.

[114] Ibid.

[115] EUCAP Nestor, EU Maritime Security Capacity Building Mission in Somalia (EUCAP Nestor), https://www.eucap-nestor.eu/data/file/1427/EUCAP NESTOR_Factsheet_November_2016.qF1oOOwtvM.pdf.

files are also exchanged with USB sticks. To provide an email service, a Microsoft Exchange Server has been set up. Standard office software for data processing and storage, in particular MS Word, MS PowerPoint, MS Excel, MS Access and MS Outlook. Additionally, Microsoft Navision, an enterprise resource planning software, is provided for logistics and other administrative purposes. MS Access serves to set up local databases, among them a database for archiving incoming and outgoing unclassified documents. This database is accessible from Nairobi, Mogadishu and Hargeisa. Citrix Go2Meet is in use for online video conferences and the Voice over Internet Protocol (VoIP) App Zoiper is provided for messaging. WhatsApp is officially only used for security alerts. EUCAP Nestor also relies on hardcopy documents and physical storage, due to expensive and unreliable Internet connection in Somalia.

Information exchange between the EUCAP Nestor mission and the Brussels level was found to be particularly burdensome because of complex administrative procedures the mission has to comply to, which were found to be not always adapted to the field situation. In a volatile security environment with a lack of infrastructure, a significant amount of time is spent on meeting the requirements set from CPCC/FPI, for example because Somali banks are not connected to the international payment systems. The fact that EUCAP Nestor operates from different countries and quasi-autonomous states further adds to the regulatory complexity, as well as to very practical challenges due to the absence of functional IT and banking infrastructures in Somalia.

Exchanges with EUNAVFOR - Atalanta are done through a system of liaison officers, which contributes to wider situational awareness across CSDP entities. Still, the more restrictive classification habits in the military sphere were found to lead to asymmetries in the information flows between both CSDP operations. As regards interaction with the EU Delegation to Somalia, there is no systematic information exchange through a shared network, making information exchange largely reliant on good personal relations between staff members, with implications for business continuity in an environment that faces high staff turnover. However, regular “comprehensive approach meetings”, chaired by the EU Delegation and held via an unclassified Video Telephone Conference (VTC) link, offer a useful opportunity to exchange information on political and security issues among EU actors involved in Somalia.

Data security is a further issue for EUCAP Nestor: for horizontal communication with other EU actors, the mission does not have access to ECAS for exchanging encrypted information. As a consequence, encrypted files sent by the EU Delegation cannot be easily opened. Instead, mission staff has to rely on the ACID system to exchange encrypted information. This is, however, cumbersome, as one needs to manually encrypt and decrypt, which leads to workarounds. ACMN terminals are used for email and file exchange with EUNAVFOR Atalanta, but the processes to get this system working seem to be cumbersome as well.

EUNVAVFOR has set up a Sharepoint for sharing basic documentation, but this is not possible to access from Mogadishu.

The **EUNAVFOR Somalia Operation Atalanta** is a EU military operation launched in 2008 to contribute to the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast.[116] The operation is not strategically "self-standing" as such, as it is part of a regional approach for the Horn of Africa. Atalanta is also part of a wider international engagement to counter maritime piracy:

- UN Contact Group on Piracy[117] to ensure safe trade in the Gulf of Aden;
- the Indian Ocean SHADE[118] coordination and de-confliction mechanism;
- US-led maritime coalitions as well as NATO maritime engagement.

According to some interviewees, SHADE (as an international coordination mechanism) has inspired similar arrangements by EUNAVFOR SOPHIA in the Mediterranean. In this respect Atalanta could serve as a model in the broader CSDP context.

The Operation Headquarter (OHQ) is located at the military base of Northwood, near London, which also hosts the NATO UK headquarters and other British military facilities.[119]

[116] Council Joint Action 2008/851/CFSP of 10 November 2008 on a European Union military operation to contribute to the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast, Official Journal of the European Union, L 301/33, 12 November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:301:0033:0037:EN:PDF

[117] The Contact Group on Piracy off the Coast of Somalia was created on 14 January 2009 pursuant to UN Security Council Resolution 1851. This voluntary ad hoc international forum brings together over 80 countries, organizations and industry groups with a shared interest in combating piracy. It is composed of five working groups. EEAS, EU 2014 Chairmanship Contact Group on Piracy off the Coast of Somalia, 14 May 2014, http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2014/140514_piracy-contact-group_en.htm.

[118] The Shared Awareness and Deconfliction (SHADE) initiative began in 2008 as a mechanism of meetings aimed at coordinating and de-conflicting activities between the countries and coalitions involved in military counter-piracy operations in the Gulf of Aden and the western Indian Ocean. The meetings are held in Bahrain at regular intervals and are co-chaired on a rotational basis by the Combined Maritime Forces (CMF), NATO, and EUNAVFOR. Since the beginning in 2008. Oceans Beyond Piracy, Shared Awareness and Deconfliction (SHADE), http://oceansbeyondpiracy.org/matrix/shared-awareness-and-deconfliction-shade.

[119] The OHQ is the location where the Operation Commander and his team are based. The Operation Command (or the Command) is the team leading the operation, serving the Operation Commander. The chain of command is the hierarchical chain going from the Operation Commander down to soldiers on ships and on the ground. "An OHQ is led by an Operation Commander (OpCdr) and is organized under a Chief of Staff (COS) from J1 (personnel) through J2 (intelligence), J3 (current operations), J4 (split in logistics, movement and medical), J5 (plans), J6 (CIS), J7 (training and lessons) J8 (finances), to J9 (civil-military relations, CIMIC). The number of officers assigned to each of the cells is time and mission dependent. Additionally, the OpCdr has a number of personal advisors; legal, political, medical, cultural, gender etc." Simon L., Command and control? Planning for EU military operations, EUISS, Occasional Paper 81, January 2010,

The Field Headquarters (FHQ) is aboard one leading military vessel in the Area of Operation (AOO). Hence, the FHQ is mobile and moving by default. The operation has an outpost in Djibouti and a number of Liaison officers (LNO)[120] deployed in the region including at EUDEL Nairobi, EUCAP Nestor and EUTM Somalia.

In 2016, only two EU vessels were under Atalanta's command. A new strategic review is being prepared with a view to managing a transition towards a possible closure of the operation. This casts doubts on the future of the communication tools that were created by and for the operation, in particular the MSCHoA (Maritime Security Centre for the Horn of Africa). The MSCHoA is a unique information exchange tool in CSDP. It is a virtual information exchange platform that was created simultaneously with the first CSDP maritime operation, EUNAVFOR Atalanta. It is not a classified information system but it is secured. The purpose of MSCHoA has been to serve as a hub towards which a variety of information flows from the civilian and military worlds converge. Technically, it is structured as a web portal with multiple components: several newsrooms on specific topics (risk alerts for various types of vessels: Fairplay for merchant vessels, specific guidance for yachting, Best Management Practice (BMP) guidelines for safety aboard merchant or fishery vessels, EUNAVFOR Atalanta's press releases); a database registration system for merchant vessels; normal email boxes to receive and send messages; and a military navy real time chat system (Mercury). The MSCHoA website is a standalone tool separated from Atalanta's classified Mission network (ACMN). ACMN includes the following functions: phone, video, email, chat and MS Office applications. In 2016, the CivOpCdr uses ACMN to a limited extent since his main assignment is a national one (Commander of the UK Royal Marine). As a consequence, the main communication channels used by the Operation Commander (OpCdr / OpsCmdr) for classified information are national channels and assets. Situational awareness, in the case of Atalanta, is a mix of information on developments at sea (maritime awareness) and on land. The function of the MSCHoA is, among other things, to contribute to providing a comprehensive maritime picture. Against this background, both ACMN and the MSCHoA contribute to coordination through information exchange.

Communication and coordination with non-EU actors has largely focused on military coordination. With NATO, OHQs are so close, next door, that EUNAVFOR simply visits them. For instance, some staff have lunch daily with NATO staff, even more so when they are from the contributing nation. The so-called "Big 3" (NATO, US, EU) have weekly meetings via VTC. For these VTCs, NATO means (classified or unclassified depending on the level of the meeting) are used. Practically, this means that EUNAVFOR staff go to a NATO room in the

http://www.iss.europa.eu/uploads/media/Planning_for_EU_military_operations.pdf.

[120] LNO is used by Atalanta staff (they did during the whole day I was in Northwood). I presume the N is for Naval, but I did not find confirmation of this. However there is evidence that LNO is used in public documents. All Liaison officers of a given operation are under the command of that operation: Atalanta's LNOs are all under the command of Atalanta.

same Northwood building or in a neighbouring building.

Non-EU states contributing to Atalanta might also receive ACMN SUS or MUS based on an ad-hoc agreement. For instance, the operation is currently working on an agreement between South Korea and the EU, as South Korea wants to contribute to the mission.

Since its inception, Atalanta has had a strong civil–military dimension in its design. Because its creation was partly the result of pressure from the shipping (and insurance) industry to receive security provision from governments, industry has had an association with Atalanta's work from day one. This joint engagement took the shape of the MSCHoA.

Atalanta is also exchanging information intensively with the justice sector. While the operation has the authority to arrest suspected pirates, their prosecution has been carried out by the civilian jurisdictions in various countries (depending on the nature of the case). This has resulted in quite intensive *civ-mil* cooperation on the legal aspects of the arrest–prosecute–sentence chain, especially at the peak of the military operation when attacks and arrests were frequent.

As for CSDP civilian missions, strong links have been developed with EUTM Somalia in terms of information exchange and situational awareness—as well as, since its creation, EUCAP Nestor, which is viewed as the prolongation of Atalanta's work in a long-term, preventive manner.

Information exchange and cooperation with humanitarian aid organizations (in particular World Food Programme (WFP) convoys to AMISOM) in Somalia have also played an important role in situation awareness and efforts to disrupt the pirates' business model (including organized crime networks on land, the involvement of Somali diasporas and money laundering practices).

Beyond CSDP, EUNAVFOR Atalanta has interacted with civilians working in Somalia and the region of the Horn of Africa and the Indian Ocean in a variety of sectors: maritime security policy (ports, border and coast guards), development cooperation (capacity building, alternative livelihoods), diplomacy and humanitarian aid.

Regarding data protection there is a debate between the Council of the EU and the UK government on which legal framework should apply to data protection and data usage within the remit of the operation. The UK position is to apply UK law while the Council considers that EU law should apply. EUNAVFOR and MSCHoA received requests to increase data protection standards in 2015. However, in practice, while the operation is not supposed to store personal data records, it actually holds and circulates some records about suspected pirates as well as the operation's staff. According to MSCHoA staff, there is no personal data

transmitted to MSCHoA, which means there is no issue of individual data protection. All the data going to MSCHoA (commercial data on vessels, the composition of their crew, the level of BMP, etc.) is backed up on servers.

The **EUCAP Sahel Mali and Niger** were initially designed as part of the EU regional strategy for the Sahel (adopted in 2011 by the member states). Following the French military intervention in early 2013, Europeans stepped up their engagement in Mali and in the region and widened the mandate of CSDP missions. The EU Sahel strategy was revised in 2014 and its action plan adopted in 2015.[121] As of 2016, three CSDP missions are operating in the region:

- EUCAP Sahel Niger (2012 - ongoing) is a security cooperation and assistance civilian mission with HQ in Niamey to contribute to the strengthening of the Niger security sector. The mission's objectives respond to several challenges in the Sahel: inability of national security forces to effectively tackle regional threats; organized crime networks; Jihadist terrorism; and uncontrolled migration flows crossing the Sahel towards North Africa and Europe.
- EUTM Mali (2013 - ongoing) is a CSDP military operation set up in February 2013 to train Malian forces and support their redeployment in the North of the country.[122]
- EUCAP Sahel Mali (2104 - ongoing) is a civilian SSR operation based in Bamako to assist Malian authorities in the modernization of their internal security forces. The mission assists and advises the police, gendarmerie and the National Guard in order to: implement the national security reform; strengthen the effectiveness of internal security forces; and support their deployment in the North of the country.

The two civilian EUCAP missions in Niger and Mali operate in a wider regional security environment with which they interact. The crisis in Mali led to the creation of an integrated multidimensional UN stabilization mission, MINUSMA. In the Lake Chad Basin, a multinational counter-terrorism joint task force has been operating since 2014 against Boko Haram.[123] France maintains troops in Chad in the framework of a bilateral military cooperation agreement. The US has also been engaged in counter-terrorism and in the field of development.

[121] EEAS, Factsheet: EU relations with Sahel countries - Burkina Faso, Chad, Mali, Mauritania, Niger, 17 June 2016, http://eeas.europa.eu/archives/docs/factsheets/docs/sahel-european-union-factsheet_en.pdf

[122] Council Decision 2013/87/CFSP of 18 February 2013 on the launch of a European Union military mission to contribute to the training of the Malian Armed Forces (EUTM Mali), Official Journal of the European Union, L 46/27, 19 February 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:046:0027:0027:EN:PDF.

[123] William A., Jeannine E. A. A. and Wendyam A. S., West Africa Report Assessing the Multinational Joint Task Force against Boko Haram, Institute for Security Studies, Issue 19, September 2016, https://issafrica.s3.amazonaws.com/site/uploads/war19.pdf

The missions' mandates have evolved over time. EUCAP Sahel Mali initially had a one-year mandate, which was twice extended for two years. Its mandate now runs until 2019 and has been expanded.[124] The budget of the mission increased from an initial €5.5 million in 2014 to around €30 million in 2017.

Information exchange with the European Commission takes place regularly (if not daily) in the framework of the Sahel task force chaired by the EU Special Representative for the Sahel, guided by the Sahel action plan and using the "comprehensive approach" to crises. However, one interviewee working in CSDP noted that "having a focal contact point" in the European Commission would be helpful.[125]

Information exchange on security and intelligence aspects is done through INTCEN in Brussels. Missions and member states feed INTCEN with security information which INTCEN can then share with member states and other missions.

Heads of Missions and mission staff come regularly to Brussels for briefings and seminars as well as sessions of the PSC to brief member states and EU HQ on the mission. Bi-weekly VTCs are organized between CPCC and each mission. In 2017, interviewees reported that triangular VTCs were starting to be organized between CPCC, EUCAP Sahel Mali and EUCAP Sahel Niger.[126] In that sense, as put by an interviewee, "horizontal information exchange is becoming institutionalized."

Information exchange between CSDP missions and EU Delegations takes place on a daily basis. EU Delegations are in charge of ensuring that the comprehensive approach is applied, while missions focus on technical training and assistance as well as projects' cell aspects.

The specificities of both missions in terms of information exchange are:

- Concentration of EU staff in the capital HQ with limited field offices, implying:
  a) a high degree of informal oral exchanges between staff and between the mission staff and other EU actors in the capital HQ;
  b) a challenge in terms of horizontal coordination as well as coordination with other international agencies in the capital; and
  c) specific requirements to manage information exchange with mission staff moving in the country or being based in field offices.
- A regionalization trend in the work of CSDP missions in the Sahel, consisting of:

[124] Council Decision (CFSP) 2017/50 of 11 January 2017 amending Decision 2014/219/CFSP on the European Union CSDP Mission in Mali (EUCAP Sahel Mali), Official Journal of the European Union, L 7/18, 12 January 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0050&from=EN.
[125] Cooperation with EUTM is taking place in the field. This case study however focuses on the civilian aspects.
[126] It was reported to the CIVILEX team that for technical reasons, the two CSDP missions could not hold direct VTCs and had to include CPCC in order to make the technology work. Interviewed staff admitted they were unable to explain this phenomenon.

a) cross-border and regional cooperation and coordination with local authorities; and
b) intelligence coordination and management on various security presence issues and threats (civilian–military, trade, trafficking, terrorist groups, migrants, etc.) in a given area.

In the case of EUCAP Sahel Mali, there are daily contacts with the EUTM Mali mission. International security coordination meetings are held in Bamako and Niamey on a very regular basis. They gather local authorities, major powers present in the country, EU actors, UN agencies, and humanitarian and development NGO communities when relevant. Information exchange on security with the US and France are deemed particularly important.

Tools and mechanisms used for information exchange within the operations, and between the operations and the outside world have been designed along procedures that were already in place for CSDP missions. However, each mission has developed these individually and the toolboxes they use are at times quite decentralized and ad hoc. EUCAP Sahel Mali uses a website managed by a private operator in Brussels. The mission staff email inboxes and addresses are hosted by the website. This system is not classified. It is often used to exchange drafts of missions reports that are then sent through a classified system. The mission uses classified systems (up to EU Restricted) to send its monthly and six-monthly reports, as well as CONOPS and OPLAN. Exchanges on CONOPS and OPLAN with the CMPD are done with the ACID encryption system. Reports from other CSDP missions in the region (EUCAP Sahel Niger, EUBAM Libya) as well as weekly information from the WKC are received by EUCAP Sahel Mali through the CPCC and under the ACID system. Experience from EUCAP Sahel Niger (2013–2015) is quite similar. Regular mission reports (weekly, bi-weekly, monthly and six-monthly) were sent via ACID to the CPCC. Exchanges on draft reports amongst staff circulated via unclassified email.[127] For unclassified information, both missions use phones (local phone operator), VTC, email and other basic software for communication that is not classified. EUCAP Sahel Niger at its inception had two satellite phones, but hardly used them. In the first few months, staff based in a hotel were using the hotel Wi-Fi network.

Situational awareness, in the case of CSDP civilian operations in the Sahel, remains quite fragmented. Mission security, MAC products and for instance the work of the political advisor contribute, albeit not systematically, to the situational awareness of senior staff and the chain of command. Interviewees expressed the need for a more coherent tool to produce and process situational awareness in the region. At the moment, a mission's situational awareness is a mix of information on developments in the capital (governance and international cooperation awareness) and in areas where security threats are

[127] This information was given only for the period 2012–2015.

considered the most acute.

In addition to the information contributing to situational awareness, regular exchange takes place between CSDP Sahel civilian missions and a number of institutions and actors. Information exchange takes place primarily via email, phone and face-to-face meetings. The WKC plays an important role in the case of Sahel CSDP missions, since it is through the WKC that the missions send their encrypted reports to CPCC via the ACID system. As one interviewee put it, "actually, watchkeepers help us to get around the question of encryption". CSDP missions hold bi-weekly VTCs with CPCC. In CPCC, there are two desk officers for each CSDP Sahel civilian mission. Two more will be in charge of regionalization in the first half of 2017. Heads of Mission and other staff visit Brussels regularly and have informal exchanges with Brussels institutions as well as their member states' permanent representations. In that respect, national channels of information exchange do matter. Information exchange between CSDP missions and EU Delegations largely depends on the quality of the relationship created by the Head of Delegation and the HoM. It also depends on their personalities. In general, both communicate by email very regularly and by phone almost daily.

In Mali, exchanges with EUTM have remained quite limited. Recent interviews show that some informal thinking is being given to closer cooperation in the field of external communications, although there are no clear plans yet to further institutionalize strategic communications.

Regionalization prospects will certainly create new needs and challenges for information exchange between CSDP missions. EUCAP Sahel Niger and Mali are already working on a joint action plan on border activity. They have organized cross-visits of their staff. The creation of a coordination platform in that respect could be a test case for the mutualisation of situation awareness. However, several interviewees underlined certain risks linked to a joint platform: 1) the risk of mutualizing all EU reporting into one single EU reporting channel to Brussels, thereby losing the specificity of each mission's mandate and added value; and 2) the risk of depersonalizing information exchange through technical tools that are too complex and not user-friendly.

Since 2015, CSDP missions in the Sahel have operated in closer cooperation with Frontex. The mandate of EUCAP Sahel Niger was extended to assistance in the field of migration and border management and control. As for EUCAP Sahel Mali, its 2017 mandate includes formalized exchange of classified information with Frontex.[128]

The operational control exercised from the CivOpCdr down the chain of command uses

[128] Council Decision (CFSP) 2017/50 of 11 January 2017 amending Decision 2014/219/CFSP on the European Union CSDP Mission in Mali (EUCAP Sahel Mali), Ibid.

encrypted reporting (ACID) for classified documents. Otherwise, unclassified assets are used. Operational control is exerted by the CPCC and the HoM. At critical junctures (mandate renewal, incidents or crisis in the country), the HoM refers to the CPCC but also to key member states in the PSC. This can also be done via national ambassadors or PSC ambassadors.

The **European Union Rule of Law Mission** (EULEX) Kosovo is the largest CSDP civilian mission to date. Planning started in 2006 as the negotiations about the final status of the province of Kosovo gained momentum. In the wake of Kosovo's unilateral declaration of independence (UDI) in February 2008 the mission was launched to ensure that the rule of law would be upheld by the Kosovo authorities. The mission carries out strengthening activities in the broader area of rule of law (police, customs, justice, etc.) as well as executive functions in the judiciary. So far, it has been the only civilian CSDP operation with a substitution mandate. EULEX Kosovo is part of the EU´s comprehensive approach in the Western Balkans aiming to promote peace, stability and economic development, with the long-term goal of EU membership for all Western Balkans countries. As part of its CSDP, the EU presently runs two missions in the area: EUFOR Althea in Bosnia and Herzegovina (BiH) and EULEX.
For communication purposes, mainly standard applications and tools have been deployed since the inception of the mission:

- telephone (landline, GSM and VoIP)
- email (desktop and mobile computers, server architecture)
- MS office suites
- bookkeeping and project management programmes.

The exact requirements are defined in the EULEX OPLAN and, due to the mission's longstanding deployment (more than ten years) and subsequent downsizing, the mission has no difficulties in equipping personnel with basic communication and IT tools.
Information exchange takes mostly place through open, not secured channels. As a reason for this, interviewees cited the lack of technology and practicality of tools to ensure secure information exchange. After ten years of mission deployment, the main issue relating to information has to do with internal and intra-EU exchange. A further concern that was raised is the lack of personnel in charge of information management. By default, this responsibility rests with the Heads of Missions. Another interviewee highlighted that there is no secure platform for a broad exchange of information between CPCC, EEAS and the mission. Between CPCC and EULEX, efforts to improve communication have not produced satisfactory results.

For restricted information, EULEX uses the ACID technology deployed to all civilian CSDP operations. Information exchange at the level EU SECRET and higher is not provided for or within EULEX.

In the area of non-classified information, the EEAS email system offers "SECEM" providing the possibility to "secure" mail communication. In EULEX only the HoM has access to the technology as the HoM is also an EEAS official and as such is provided with an @eeas.europa.eu email account and remote access to the server. No other mission members can secure communication in this manner.

Information exchange between ordinary mission members and communication between them and CPCC staff member also takes places through publicly available messenger services such as Signal, WhatsApp and Threema.

EUNAVFOR MED is the first EU mission in the Mediterranean region to bring closer the internal and external dimensions of EU security, whereby an internal issue (the vast number of migrants arriving on EU shores) is addressed with an external action. EUNAVFOR MED was launched on 22 June 2015 "to undertake systematic efforts to identify, capture and dispose of vessels and enabling assets used or suspected of being used by migrant smugglers or traffickers, in order to contribute to wider EU efforts to disrupt the business model of human smuggling and trafficking networks in the Southern Central Mediterranean and prevent the further loss of life at sea."[129]

The main initiative implemented by EUNAVFOR MED for information exchange and situational awareness is Shared Awareness and De-confliction in the Mediterranean (SHADE MED), a forum where 145 representatives from 74 nations and organizations interested in or impacted by the migratory phenomenon in the Mediterranean basin can meet to coordinate their Maritime Security Operations (MSO) by sharing situational awareness, assessment of the evolution of trends and best practices.[130]

SHADE MED brought the introduction of an improved Service-oriented infrastructure for MARitime Traffic (SMART) platform, an important cornerstone in establishing and sharing maritime situational awareness. The common desired goal of SHADE Working Group 2 is to define minimum required standards for the establishment of a Maritime Security Capacity (MSC) and possibilities for the commercial shipping community to contribute to enhancement of maritime situational awareness. This system is designed to enable information sharing between EUNAVFOR MED, NATO, Frontex, national organizations and maritime shipping industries in order to enhance situational awareness, de-confliction and coordination as well as to improve rescue operations in terms of aviation safety and

[129] EEAS, European Union Naval Force – Mediterranean Operation Sophia, Update: 30 September 2016, http://eeas.europa.eu/csdp/missions-and-operations/eunavfor-med/pdf/factsheet_eunavfor_med_en.pdf.
[130] Difesaonline, Intervista al comandante dell'OperazioneEUNAVFOR MED SOPHIA, Amm. Enrico Credendino, 3 August 2016, http://www.difesaonline.it/evidenza/interviste/intervista-al-comandante-delloperazione-eunavfor-med-sophia-amm-enrico.

effectiveness in rescue activities by usage of commercial secure services.

The Operation has a robust, flexible and accredited Communication and Information System (CIS) infrastructure. The CIS architecture follows the ''higher to lower'' principle, in accordance with EU concepts, whereby any higher authority or organization in the chain of command is responsible for providing the CIS at that level and links down to its subordinate level. The mission system, and primary means of communication, is the EUNAVFOR MED Classified Mission Network (MED CMN), capable of timely and efficient exchange of classified information (up to Secret). The tactical communication links have been established using military as well as commercial assets.

The lack of coordination with other CSDP missions, such as EUBAM Libya, may derive from political reasons and from the absence of a common communication platform. EUNAVFOR MED would welcome a link with other CSDP missions such as EUBAM Libya and EUCAP Sahel Mali.[131]

The operational Standard Operating Procedures (SOP) signed between EUNAVFOR MED and Frontex is crucial for the deployment of liaison officers/working visitors and for sharing of information between the two actors.

It must be noted that data protection plays a key role in the exchange of information. Interviewees both from EUNAVFOR MED and Frontex suggested that a common framework would improve communication of data related to persons. At the moment, EUNAVFOR MED shares personal data directly with the Italian authorities, while Frontex passes through the European authorities. Only after this process is completed can the personal data be shared between the two institutions, which causes delays that may hamper operations in the field.
Issues concerning classification of information were raised mainly by Frontex and Europol officers. It is rare that information is classified by EUNAVFOR MED, but when this happens the procedures generate operational complications.

The brief overview of the case studies underlines several important features that should be taken into account in the design of a future platform. Over the years, CSDP civilian missions have seen their mandates and tasks changing, so that a future platform should be “flexible” enough to support a variety of actors and actions. Missions have been differing in size and length, changing inevitably the quantity of data exchanged, stored and retrieved. CSDP civilian mission have been strengthening ties with their military and FSJ colleagues, therefore suggesting that a future platform should be able to connect actors that are not necessarily representatives of their institutional family (EEAS VS Commission VS EU agencies) and have different chains of commands and budget line to respond to. This closer relationship between these actors stem from the concept that security challenges will be tackled along

[131] EUNAFVOR MED staff and in OHQ, Interviews, 09 January 2017 – 13 February 2017.

the internal-external security continuum. Better links with EU delegations, but also easiness in communicating with main international actors such as NATO, UN, OSCE, AU will have to be pursued. Finally, security of networks and information, as well as data protection rules, will have to be seriously considered to allow swift and fast exchange of information, while ensuring that the data are secured properly.

Institutional and political lesson learned are expanded in chapter 5.

3.3 The future of CSDP civilian missions: hints for a prospective OCP platform

The analysis of the evolution of CDSP civilian action (sections 2.1 and 2.2), as well as the evaluation of current missions and case studies (sections 3.1 and 3.2) show that CSDP missions are an evolving endeavour, and that they might be influenced by new strategic drivers and policy initiatives. The release of the EUGS, the Implementation Plan and the subsequent Council are certainly among them. Their full implications are difficult to foresee as of now, but they will have to be fully taken into account when imagining the future of civilian missions, and, as a consequence, the design of a possible future OCP platform to support them.

In particular, the 14 November Council conclusions invited the HR/VP to make proposals on a review of the priority areas of CSDP civilian missions by spring 2017. The Council conclusions of 6 March reiterated the need for such a review, while postponing it until later in the year. Moreover, the Implementation Plan and the November's Council conclusions affirmed the need to identify the required capabilities stemming from the list of generic civilian CSDP tasks and to revise the CCDP to meet the new security challenges and threats. These driving factors, which all have the potential to modify needs and technical requirements, will have to be fully accounted for in the design of a future OCP platform.

In addition to this changing policy landscape, civilian missions seem to be in the midst of a paradigm shift that is going to influence how missions will be run in the years to come. According to some analysts, CCM has been transformed in at least two interrelated ways:[132] first, it has become a broad-ranging activity that cuts across EU external but also internal security, encompassing a wide spectrum of activities and tasks; second, institutions and bodies that now play a role in CCM are not only CSDP and EC actors, but also JHA institutions and agencies. More recently, these agencies have been involved "at the very frontiers of home affairs," in response to an increasing need to deal with external issues with a clear repercussion on EU internal security, like international terrorism and strong migration waves. Clear examples of these shifts are Frontex cooperating with EUNAVFOR MED, or Europol partnering with EULEX in Kosovo. Therefore, the direct consequence of new policies

[132] Thierry T., Recasting EU civilian crisis management, Ibid.

at the nexus between security and development, paired with the blurring distinction between internal and external security, has made EU civilian crisis management "a three-pillar endeavour that brings together CSDP, European Commission-led and JHA-led activities."[133]

How this evolving configuration of CCM actors and actions will develop is still hard to foresee. However, at least three elements need to be considered: operational coordination, respective agendas and possible political challenges. Operationally, and in spite of recent agreements on information exchange and regular consultations, CSDP and JHA worlds remain different in terms of institutions involved and type of operations. Moreover, partial overlapping between actors that have conducted operations on their own is likely to raise questions that are now difficult to answer, for instance those related to funding or the degree of control exercised by member states.[134]

More generally, it seems that all these considerations are placed in a context of a revaluation of CSDP civilian missions. Three main questions will have to be answered: 1) What will be civilian CSDP added value in contribution to the "security of the Union" in this changing security environment, and how will the EU and member states articulate and coordinate civilian CSDP action with other actors that are now part of CCM? In other words, what should be the nature of CSDP civilian missions, taking also into account that long-term policies addressed by civilian CSDP issues do not necessarily pertain to "crisis management" stricto sensu? 2) What is CSDP civilian relevance in the context of blurring lines between external and internal security, especially vis-à-vis JHA actors? 3) What resources are required in terms of expertise and force generation?[135]

[133] Ibid.
[134] Ibid.
[135] Ibid.

4 Envisaging information exchange, situational awareness and operational control in civilian CSDP

In the following chapter information exchange, situational awareness and operational control are envisaged from three interlocking perspectives:

- the institutional-administrative dynamics of the operational life-cycle of civilian CSDP operations, and how information exchange, situational awareness and operational control issues impact on the phasing-in, implementation and phasing-out of CSDP operations (section 4.1);
- the institutional-technological landscape in which missions are conceived and which form the backdrop of the recommendations for developing an OCP; since the emergence of CSDP approximately 15 years ago and the EEAS almost seven year ago a number of initiatives, mechanisms and technological solutions have been developed in the field of civilian external action which also aim at improving their effectiveness and which have an impact on the conceptualisation of a future OCP (section 4.2);
- the management of sensitive data and EUCI; a field that has seen considerable development with the growth of the CFSP and CSDP as well as the evolution of Community legislation in the area of data protection and information security (section 4.3).

All three perspectives, while analysed here distinctively, are interlocking as the institutional-administrative mission life-cycle management is confronted with legacy technology and communication solutions as well as the thickening web of data management regulations and legislation. In order to approach the substantial elements of the OCP it is therefore also to delineate the key terms in the context of civilian CSDP against the background of the three perspectives taken in this chapter.

4.1 Aspects of information exchange, situational awareness and operational control

In the civilian CSDP operational context, this research envisages information exchange, situational awareness and operational control as follows.

Information exchange is essential in civilian CSDP operations. Simply put, given the primarily 'capacity development' nature of the operations, without information exchange there is no operation. Information exchange has two dimensions: internal and external. Internally, there

are first the formal exchanges that follow predefined pathways, as described in the relevant constituent documents setting up the operation. CSDP operations send and receive information through the chain of command as well as other reporting and information exchange mechanisms agreed upon by EU member states when they set the operation's mandate. Second, there are information exchanges that emerge within the mission organization, and that help to shape its course of action. Information exchange is required on the one hand in the theatre of operations, within the mission and its constituent elements, and on the other hand with the EU family—including other CSDP operations (civilian and military) and other organizations active in the area of intervention of the civilian CSDP operation. External information exchange thus takes place with trusted parties but also with the general public (public information). CSDP operations develop, contribute to and maintain public information initiatives, which provide the media as well as the general public with information about the activities performed in their framework. Hence, information exchange in the broadest sense happens at the strategic/political level in formalized external action structures as well as informally among member states. It fuels the decision-making and once an operation is set up, the exchange from the operational level adds and contributes to the existing mechanisms. Information exchange therefore is a prerequisite to operational control and communication.

Differently from the descriptive notion of information exchange, the term **situational awareness** denotes the outcome of a cognitive human (operational) process whereby information, data and observations are analysed and contribute to comprehending how these environmental elements relate and what they mean. Situational awareness is required for a number of purposes in a civilian CSDP context. The Heads of Mission and mission senior leadership as well as the Civilian Operations Commander and the CPCC require situational awareness for implementing the mandate of the mission but also for the safety and security of the mission's personnel. Situational awareness is also required for political control and strategic direction of civilian CSDP operations, which is exercised by the HR/VP and the PSC.[136] The CMPD also identifies situational awareness beyond the EEAS remit to which CSDP should contribute in conjunction with civilian FSJ actors.[137] Hence, situational awareness is generated for actors to operate in the theatre of operations and should be harmonized across CCM. While it contributes to the initial deployment planning, the depth and rhythm of feeding back elements for situational awareness at the operational and strategic/political level has to be adapted as CSDP missions evolve.

Operational control is described as "a continuous sense, assess, decide and act cycle

[136] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art. 38 and 43, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M021.

[137] EEAS, CMPD Food for Thought Paper: From strengthening ties between CSDP/FSJ actors towards more security in Europe, Ibid.

executed in order to accomplish an assigned mission."[138] Operational control includes therefore the need for "information exchange" (to sense), the generation and use of "situational awareness" (to assess), as well as rules (to decide) and tools (to act). Operational control is possible thanks to the "downstream" and "upstream" of communication and action related to the theatre of operations and the implementation of the mandate in the chain of command and the policy-making cycle. It includes the beginning of the CSDP planning cycle, from the level of the Council (PSC, CivCom) and the EEAS structures (CPCC) to the "planning team" and the operation. This includes operational tasks undertaken within missions, e.g., by teams in specific locations and at specific times, which all has to be coordinated, as well as information available for HQ in the field and possibly in Brussels.

While the CPCC is a permanent Brussels-based structure established to plan and conduct civilian CSDP operations, the individual CSDP civilian operations are purely temporary. Yet, operating expenditure is charged to the Union's budget, which is administered by the Commission service for FPI. This has implications for the environment in which information exchange, situational awareness and operational control have developed over time. With the establishment of the EEAS, CPCC has become part of this novel administrative structure, while the civilian CSDP operations remain distinct entities, which have gained "legal personality" since 2012.[139] In this respect, CSDP civilian missions follow a project management (or project steering) communication approach, adapted to the specific environment and tasks they are set up for. On the other hand, the CPCC and EEAS separate the civilian CSDP operations from their internal (Brussels or Delegation-based) administrative–institutional communication systems. To bridge this divide, a MSP was established to facilitate coordination and thereby information exchange between the Commission and the EEAS:

> "The MSP will be established in coordination between the Commission and the EEAS to provide support and bring forward greater efficiencies, flexibility and economies of scale to CSDP civilian missions. The Council emphasises that the establishment of the MSP is a part of an effort to take forward a Shared Services Centre concept. The results that the MSP is expected to deliver shall be presented to the Council through regular reports on the impact of the MSP on improving the effectiveness of CSDP missions and financial benefits for the CFSP budget."[140]

The information technology infrastructure of the CSDP civilian missions varies considerably as missions have purchased and are utilizing different types of hardware and software. More

[138] Council of the EU, Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management, Ibid.
[139] European Commission, 2012 Annual Activity Report Service for Foreign Policy Instruments (FPI) http://ec.europa.eu/dgs/fpi/documents/fpi_activity_report_2012_en.pdf.
[140] Council of the EU, Council Conclusions on the Mission Support Platform, 18 April 2016. http://www.consilium.europa.eu/en/press/press-releases/2016/04/18-fac-mission-support/.

harmonization in the area is expected after the establishment of a more harmonized mission support structure (including the MSP), yet those structures will not be able to replace a more strategic decision on technical standards and the adaptation to newer information technology development such as cloud computing, collaborative working and social media application. However, the MSP is also aiming to streamline communication technology aspects; this is necessary since institutional developments at the Brussels level as well as the experimental growth and development of civilian missions and their financing have led to a great variety of communication technology and data processing approaches within missions. Yet, a comprehensive approach would require envisaging a more integrated approach for civilian CSDP operations which would enable them to fully exchange information with all CFSP actors, contribute to and benefit from situational awareness, and allow for an integrated approach to operational control. To date, communication streams throughout the civilian CSDP system, and with the institutions and bodies governing it, remain fragmented.

4.1.1 The needs for information exchange, situational awareness and operational control throughout the CSDP operational cycle

From an institutional perspective, unpacking the evolution of civilian CSDP operations helps to identify the shortcoming and possible gaps in the process of information exchange, in the generation of situational awareness and in operational control. Civilian CSDP contributes to strengthening EU activities aimed at capacity development in the theatre of operation. This requires knowledge of other past and ongoing activities and actors, especially concerning EU institutions and member states. CSDP missions are established based on previously generated situational awareness that derives from other EU external actions as well as information exchange among EU external action actors and third parties. CSDP missions and operations often unravel as an element in the "transition" or reconfiguration of different forms of EU civilian external action in a specific theatre, even if the use of CSDP is connected to a situation of crisis, crisis management and/or post-crisis intervention. So far, every single CSDP mission has been established in a theatre where other EU instruments (development, humanitarian assistance, CFSP instruments) were already present. In this sense, it is never fully "uncharted territory" for EU CSDP. Nonetheless, while at times drawing on existing knowledge and structures, missions and their communication are set up as formally ex-novo, with the related opportunities.

This section is organized in three parts structured along the stages of the CSDP operation life-cycle (before, during and after), described as phasing-in, task implementation and phasing-out stages of CSDP.

Phasing-in stage of CSDP operations

Operational control and communication includes the beginning of the CSDP planning cycle, from the level of the Council (PSC, CivCom), the EEAS structures (CPCC), to the "planning

team" and the operation. This includes operational tasks undertaken within missions, and information available for HQ in the field and possibly in Brussels. The Council decision sets up the formal operational control structure, while the planning phase is governed by the hierarchy of the EEAS. Hence, access to the knowledge generated by previous EU actions should in principle become easier through the EEAS, and yet it has not. Access to information and data during the stage of phasing-in the CSDP instrument is an important aspect of establishing situational awareness for the three steps of phasing-in:

- planning,
- deployment and
- initial operational capability.

Access to information and data related to the theatre of operations, and to past as well as ongoing activities of the EU, is not systematically accessible to the CPCC, which is the main driver behind the phasing-in stage at the operational level in the EEAS.

At the political-strategic level — with important roles for the PSC and CivCom — the Commission's representative who participates in the sessions is in a position to provide the necessary input and contribute to these aspects of situational awareness. Yet, such systematic analysis and review of "political background" or "archival" information is not being made available during the phasing-in stage of the operation. Information may become available due to the continuity of personnel and through informal channels. However, such information is not stored and retrievable in a systematic manner. The random documentation practices and the random use/transfer of such information do not contribute to increasing the strategic analysis capacity to support CSDP.

Up-to-date situational awareness during the phasing-in stage should be generated by the EEAS INTCEN, for the use of the CSDP chain of command as well as the mission/operation. The Commission and other EU bodies and agencies are key providers of information in this process. Member states could also provide information through INTCEN as well as non-formalized channels and personal interaction with the planners of CSDP operations.

Implementation stage of CSDP operations

When CSDP operations have reached "initial operational capability" they become active participants in information exchange, and users and producers of situational awareness products. Nevertheless, such information emanating from the missions is not processed through a single platform, either institutionally or technically.

Operational control and communication in a CSDP operation follows formal rules set out in the C2 arrangement of the individual civilian mission. Those can be found in the Council Decision, the CONOPS and OPLAN, as well as operational instructions issued by the CivOpsCmdr and the HoM. C2 is exercised by the CivOpsCmdr through the HoM and over

personnel seconded by member states or by participating third states or EU institutions or agencies, together with contracted staff (international, national and local). Information exchange, situational awareness and operational control processes are key requirements for the CSDP operation in the interplay with other CFSP and CSDP actors, the EEAS and the Commission during the implementation stage, as they are supporting:

- task implementation and achieving mandated objectives of the operation, including exchange with stakeholders;
- reporting through the chain of command and provide political-strategic guidance;
- operational security.

Implementation happens through direct and indirect interpersonal interaction of CSDP personnel with counterparts and host country authorities as well as other actors (governmental and non-governmental), other EU actions, member state officials, civil society and media, depending on the mandate. Through "monitoring" and also as a side product of "mentoring and advising", the CSDP operation gathers insight and information contributing to situational awareness. Furthermore, CSDP operations may have at their disposal automated tools of data analysis as well as audio-visual aids and imagery produced by the private sector and other parties, such as the EU SATCEN. The process of creating "situational awareness" seems not be carried out in such a manner that CPCC and CSDP operation staff can easily describe the method used. It seems not to be aided significantly by the use of analytical software. Some experimentation has taken place with the establishment of a Mission Analytical Capability (MAC).[141]

The Civilian Operations Commander regularly issues instructions and guidance with regard to the structure, contents and periodicity of the information required. Transmission between the operations and the CPCC is channelled in most cases through the EUMS's Watchkeeping facility. However, over time CSDP operations tend to create different structures to process information. While standardization of mission planning remains an objective, including through the Operational Planning section within the CPCC, situational awareness has remained an area of experimentation within the operations as well as in communication with the CPCC. The link to the WKC has been formalised, however, possibly providing a hook for further development of an integrated approach to situational awareness.

[141] "CivCom supported in general the need for a Mission Analytical Capability (MAC) as a complementary tool to closely cooperate with existing mission functions, which will contribute to enhance continuous monitoring and analysis of the crisis environment necessary to satisfy decision making requirements in the pursuit of Mission objectives. Where considered beneficial and based on a thorough need assessment, the MAC will be established in Missions through OPLAN as deemed appropriate, bearing in mind that the MAC will not engage in intelligence activities on the ground. 4. CivCom noted that the MAC could also support the Heads of Mission by improving information management, enhancing situational awareness, and aiding their decision making, as well as underpinning organisational memory." See CivCom advice on the introduction of the overarching principles for a mission analytical capability in a civilian crisis management operations, Council document 15883/09, 13 November 2009.

Information security procedures are currently in place, but they seem to differ or are in the process of review. The EU document classification is being used for certain types of documents (e.g., CONOPS and OPLAN), with regular reports being classified "EU Restricted". For transmission, encryption systems are being used (i.e. ACID). So far, data protection issues have not been seen as a major complicating factor, although at the field level a lack of preparedness to deal with the requirements was observed. Secure (mostly mobile/satellite) telephone lines (up to the "confidential" level) have been created for communication between the CPCC and the mission HQs. For the entire implementation phase of a CSDP mission, operation information sharing requirements are prescribed in the OPLAN and its annexes. The OPLAN regulates the available technical infrastructure and the regular information processes that have to be followed by the operation but the information transmission infrastructure does not always meet the expectations of those who have to use it. This leads to circumventing certain procedures, as the information can more easily be shared through means other than those officially prescribed. Furthermore, the periodic reporting systems which form the backbone of the information-sharing architecture do not lend themselves to a dynamic flow and accessibility of information throughout the CSDP operations system. A number of gate-watching functions and dissemination through email distribution lists (or shadow software applications such as WhatsApp) do not sufficiently contribute to a collaborative information sharing environment.

In turn, situational awareness during the implementation stage depends on a dynamic information sharing environment that is not controlled by the mission and the CSDP structures. Hence, a more comprehensive integration of various types of information is required in the operational conduct of operations. In particular, open-source web-based information and media, privileged exchanges with international and non-governmental organizations, diplomatic information from EU and member state delegations and embassies, and reporting from within the missions, including civil–military exchange, are not systematically integrated in the information exchange. Some experimentation has taken place with the establishment of what is being referred to as a "wiki" for the use of mission personnel—a database which is, however, not interactive. This "wiki" use indicates that at the CPCC and operational level, the technical functionalities of information management software—e.g., of MS Outlook (most commonly used) and other platforms—are not being fully used, including for gathering information on activities of personnel. Neither are they fully utilized to allow also for mission-internal peer-to-peer automated information exchange and knowledge sharing.

With the establishment of the EEAS, a more streamlined system for management of EU civilian external action is emerging. However, so far no comprehensive "information plan" has been developed for various theatres of operation in conjunction with all EU external actors that would identify common information needs, not least benefiting the more

transitional and temporary character of the CSDP operations. Such an information plan would rationalize the information efforts and maximize the effectiveness of EU external action during the period when the "additional" CSDP assets are active in a particular theatre of operation.

A variety of CSDP mission "information products" are exchanged, containing situational awareness relevant for an ongoing CSDP mission and potentially of use for the wider EU environment, and are used by the chain of command for operational control. These include, among others:

- regular reports issued by the mission (weekly, monthly and six-month reviews; spot and special reports)
- updates by the WKC
- INTCEN products
- open-source communication
- media monitoring
- missions websites, social media

Information and intelligence in a civilian CSDP environment
A mix of sources may be used when creating situational awareness: they contain open information but also at times "intelligence". Those terms may also become mixed up as they are subject to different use, and interpretations vary from member state to member state. In an early CSDP context the following definition was used: "information is taken to include information deriving from a range of sources, e.g. diplomatic, open, for which no special clandestine or intelligence methods are used. Intelligence is taken to include just that information where special methods are used."[142] The terminology problems persist, and have impact on issues like classification and secure transmission. Nevertheless, the most significant issues are those related to the processing and storing of information products at the levels of CSDP operation and CPCC (in Brussels), rather than the nature of the information itself. So far situational awareness products remain stored in different databases and without consistent archival standards. Information is often stored randomly in email systems, leading to accessibility problems and multiple storage. Business continuity in case of change of personnel and deployment is thus not guaranteed. No system exists at the operational level to follow how and which information has been processed by whom.

Table 2 - Information and intelligence in a civilian CSDP environment

[142] Council of the EU, Civil-military Co-Ordination: Possible Solutions for the Management of EU Crisis Management Operations: Better Sharing of Information in Theatre", 13218/5/06, REV 5, Brussels, 31 October 2006, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260410cmcoinformationsharing_/sede260410cmcoinformationsharing_en.pdf.

Phasing-out CSDP and handing over to other instruments of EU external action

Through ongoing experimentation and continuous adaptation to an ever-evolving institutional environment since the inception of operational CSDP after 2001, elements of a communicative and information management practice for situational awareness have been established for the **phasing-in** and task implementation stages of civilian CSDP. However, the archiving of "situational awareness" products which would transform them into "information" for future use is not taking place during the phasing-out stage of CSDP operations and handing over to other instruments of EU external action. The phasing-out of CSDP operations has so far not resulted in a standard practice of information and archive storage for the benefit of the continuing EU civilian external action. For the concluded operations almost no situational, mandate-related and mission implementation information is easily accessible, differently from the access provided to information related to the execution of the Community budget. The data generated by civilian CSDP operations is thus not readily available for reference and use by follow-on and future EU civilian external action. Recently in 2016, the Civilian Operations Commander issued guidelines on the management of certain archival material in the EEAS.[143]

It would seem that information management during the phasing-out and post-mission phase would also benefit mission implementation (as experience is recorded for later beneficiaries). Thereby it would contribute to overall operational capacity of the EEAS and the EU, and contribute to the situational awareness and security of future EEAS and other European civilian external action deployments. In this respect, issues remain pertinent beyond the directly concerned CPCC and the mission. In particular, through the EEAS and the HR/VP the linking of a phased-out CSDP mission to the network of EU Delegations, the EUSRs, Commission bodies and EU agencies active in external action needs to be ensured, as the data and knowledge produced by CSDP civilian missions might be the necessary basis for future deployments, in particular at the nexus of internal and external security.

4.2. Scoping of past initiatives

To respond to the communication and information exchange needs of CSDP missions, as outlined above, several tools, mechanisms and practices have been created or are currently being developed. Some of the past and current initiatives have been successful in contributing to more effective communication and information exchange, and a future OCP will need to build on them and take into account their good practices. Other initiatives have been more limited in their added value, and therefore provide useful sources for lessons learned. Therefore, this section provides a scoping of past initiatives in the CSDP context to

[143] EEAS, Civilian Operations Commander Instructions VII: Guidelines on document management and procedures for the transfer of closed archives to EEAS HQ, EEAS/CPCC/A2/UK (2016), 23 March 2016.

harmonize, standardize and improve communication and information exchange, and strengthen situational awareness and operational control. It also aims to present and discuss institutional implications and lessons learned. It highlights success cases, while also identifying lessons learned to be taken into account in the design of future systems. Section 4.2.1 gives an overview of centrally-led initiatives (EEAS or cross-EU at HQ level), whereas section 4.2.2 presents observations with regards to communication and information exchange practices at the field level.

4.2.1 Centrally led initiatives

- **Integrated Political Crisis Response Arrangements (IPCR)**: The IPCR arrangements, established in June 2013 by the Council, are an instrument to facilitate a coordinated response to major crises in or outside the EU among relevant EU bodies and member states at the highest political level. Not a CSDP-specific tool, the IPCR could be used for any crisis situation deemed relevant by the Council Presidency (ranging from global health crises to refugees and migration or crises in diplomatic relations).[144] IPCR arrangements are built around a restricted web platform, managed by the General Secretariat of the Council, where monitoring pages can be created to share regular information updates between users. As the platform is Internet-based, it only allows for information-sharing up to the 'restricted' level. The Council Presidency can decide to activate the IPCR arrangements either in *information-sharing* mode or in *full* mode. Activation of the IPCR triggers the weekly Integrated Situational Awareness and Analysis (ISAA) reports. These crisis-specific reports are compiled via the IPCR web platform and integrate information and intelligence from all IPCR users to provide a common picture of situations and support the political decision-making process. Depending on the nature of the crisis, either the EEAS or the Commission is in the lead for developing the ISAA reports. Activation in *full* mode offers the possibility to convene informal roundtables at the technical, ambassadorial or ministerial level. Where relevant, such roundtables may also include CSDP mission representatives. The IPCR arrangements have only been activated once in full mode, by the Luxembourgian presidency in response to the immigration and refugee crisis. Capacities for the Council General Secretariat to manage the IPCR are relatively limited and would likely allow it to deal with one or two more crises.[145] Concerns have also been expressed over whether the IPCR arrangements merely add another layer of complexity rather than contributing to synchronization of an inter-institutional crisis response.[146] Moreover, the full activation of the IPCR arrangements has also proven to be politically sensitive.[147]

[144] EEAS and EU Council, Interviews, 10 May 2016; 6 September 2016.
[145] EU Council, Interviews, 25 October 2016.
[146] Minard, P. The IPCR Arrangements: A Joined-Up Approach in Crisis Response?, EUISS, Brief Issue 38, December 2015, http://www.iss.europa.eu/uploads/media/Brief_38_IPCR.pdf.
[147] Ibid.

- **EEAS CRS:**[148] The EEAS CRS is managed by the EEAS Crisis Response & Operational Coordination Department and aims to ensure timely and coherent mobilization of all EU actors and instruments across the EU system throughout the different stages of the crisis cycle (ranging from prevention and preparedness to response and recovery), including in the security, political, diplomatic, humanitarian and developmental fields. Within the EEAS CRS, a key component is the **EU Situation Room**. The Situation Room provides 24/7 situational awareness on worldwide events. As such, it acts as the first point of contact for EU institutions and bodies on crisis-related information. It produces situation reports and flash reports with crisis-related information provided by different sources such as EU Delegations and CSDP missions and operations. The EU Situation Room also plays a role in the IPCR arrangements insofar as it supports political coordination and decision-making in major, complex crises. The EU Situation Room liaises with CSDP missions and operations through the **WKC**. The WKC functions as a hub for information exchange and situational awareness between all CSDP missions and operations in the field and at the HQ level. While the WKC is housed within the EUMS, it is in fact a hybrid civilian–military unit and closely cooperates with the EU Situation Room, which is collocated in the same room. It monitors all CSDP missions and operations and hosts two-weekly classified briefings for EEAS staff on mission-related operational matters. While it contributes to situational awareness across relevant EEAS units on operational matters from CSDP missions, the WKC is not directly involved in mission planning, an aspect which is identified as a weakness.[149] Another element of the EEAS CRS is the **Crisis Platform**, which comprises different EU bodies and services involved in crisis response. Crisis Platform meetings are chaired by the HR/VP or a substitute and can be convened on an ad-hoc basis to coordinate across the EU system in the event of an external crisis. The platform aims to provide the EEAS and the Commission with clear political and strategic guidance.

- **OPCEN and Scope HoA:** The EU Operations Centre (OPCEN) is one of the three command options for military CSDP operations,[150] but has in practice never been used in that capacity. Instead, the OPCEN has been activated by the Council as a coordination body to support CSDP missions and operations in the Horn of Africa (since 2012) and in the Sahel (since 2014) in the field of operational planning and conduct, aiming to facilitate information exchange and strengthen civil–military synergies in both regions.[151] This includes support to the CivOpCdr, the military commanders and CMPD, and facilitation of

[148] EEAS, Crisis Platform, https://eeas.europa.eu/headquarters/headquarters-homepage/412/crisis-management-and-response_en#Crisis+Platform.
[149] EU, Interviews, 20 October 2016.
[150] The other two options are using either NATO or member state command structures.
[151] Council Decision 2014/860/CFSP of 1 December 2014 amending and extending Decision 2012/173/CFSP on the activation of the EU Operations Centre for the Common Security and Defence Policy missions and operation in the Horn of Africa, Official Journal of the European Union, L 346/32, 2 December 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0860&from=EN.

interaction between CSDP missions and operations in the region and with the Brussels-based structures, in liaison with the respective EUSRs.[152] To implement its mandate, OPCEN developed the **SCOPE** (Synergies and Coordination Portal). SCOPE is a protected web portal that allows the sharing of information on EU strategic objectives in the region and the coordination of activities.[153] It also provides users access to detailed information about different EU-funded activities in fields such as security, development, humanitarian aid or anti-piracy. In practice, both Brussels-based staff and CSDP staff in the field have expressed reservations over the usefulness of the portal, arguing that its purpose is not clear or that the information is usually already channelled through other means.[154] In addition, the OPCEN also ran two closed Twitter accounts to share updates across users in the Sahel region and the Horn of Africa, respectively. The aim was to give users timely and reliable information on, for instance, crises or emergencies. The mandate of the OPCEN expired in 2016 and has not been renewed. This also provides an opportunity for sharing lessons learned. In light of this, several interviewees in Brussels and in the field have questioned the added value of the OPCEN, arguing that it failed to find its own niche to support missions at the strategic, tactical or operational level.[155] Some have also argued that the EU Delegation on the ground should play a bigger role in coordinating EU actors.[156]

- **EUCCIS:** The EUCCIS was developed by OPCEN, and is owned by the EEAS. The aim of the EUCCIS is to enable an Operation Commander to efficiently plan, monitor and conduct an EU-led crisis management operation and support staff during routine activities. The EUCCIS contains the following functionalities: a Viewer that provides geospatial information to support planning and developing a Common Operational Picture; and Operational Planning Process Functional Area Service that enables collaborative work within the Operational Planning Process; a portal for OHQ staff and branches to keep track of all documents and information, including through a document management functionality and a function to keep personnel informed on developments and activities; and a Civilian Functional Area Service, supporting the operational planning process for CSDP civilian missions, including through an online collaboration tool and documentation record.[157] The EUCCIS contains a dedicated functionality for civilian missions. So far, it has not been used for civilian missions, although the EEAS Secure Communications Operations team have set up a server room for the use of the EUCCIS by CSDP civilian missions (initially intended for the use of EUMM Georgia, mainly for reporting and e-

[152] EEAS, EU Operations Centre Horn of Africa & Sahel (EU OPCEN), Updated: June 2015, http://eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-operations-centre/docs/factsheet_eu_opcen_23_06_2015.pdf.
[153] Benmansour A., Sorensen A., Cannarozzi N., Feasibility Study: Centralised and Integrated Resource Management System for CSDP Missions and Headquarters, Brussels: CPCC, December 2014.
[154] EUCAP Nestor, Interview with staff member, 28 November 2016; EEAS, 10 October 2016.
[155] EU, Interview, 23 August 2016 and 24 November 2016.
[156] EU, Interview 29 September 2016.
[157] Leaflet on EUCCIS and interview with EU official, 23 August 2016.

maps).

- **CPCC Wiki**: This Wiki is an online repository developed within CPCC to gather and keep information. Initially designed for human resources management, it is now used to share information of a general nature (e.g., SOPs, guidelines, instructions), but not for purposes of situational awareness. The Wiki is organised around clusters, project cells and thematic libraries (e.g., on human rights and gender). There is also an option for discussion fora. The Wiki has an option to encrypt and decrypt information, but it is not used for classified content. Access to the Wiki is centrally managed by CPCC, and missions can request access as well. While designed as a collaborative system, it is in practice used as an archiving tool.[158]

- **SOLAN, ACID** and **EC3IS**: SOLAN is the current system managed by the EEAS to enable exchange of confidential and secret information in Brussels. It is a legacy system used mainly within the Council General Secretariat and remaining in use today primarily in the EEAS. The Council General Secretariat has two terminals still available to receive information from the EEAS (CMPD and EUMS). CPCC hardly uses the SOLAN, as most of the information it shares is restricted, for which other systems are available. The main encryption product used for CSDP civilian missions and the CPCC is ACID. The EEAS is currently in the process of planning procurement of the EEAS Corporate Classified Communication and Information System (EC3IS). The EC3IS will replace the SOLAN and aims to be a wide-area network, also linking to the military headquarters in Europe. According to an interviewee, CSDP missions are currently not foreseen as users, as the system would focus on communication at the HQ level.[159]

- **ARGUS** and the **CCC:** ARGUS is a general European rapid alert system launched by the European Commission in 2005 that aims to contribute to a more coordinated emergency management in the domains of the Commission's competencies (taking into account the principle of subsidiarity). ARGUS allows each Commission Directorate-General to inform other DGs and services of a multisector risk or emerging crisis via an alert exchange, and provides a coordinated process that can be activated in case of crisis (the crisis coordination committee). It also provides a common source of information for the Commission to communicate coherently with EU citizens. ARGUS is an EU internal network, although member states and external bodies can be connected through sector-specific rapid alert systems. In the event of a crisis, the Secretariat-General of the Commission can also activate the Central Crisis Centre (CCC), which assesses and monitors the development of the situation, identifies issues and option for action, ensures their implementation and ensures coherence and consistency of the Commission's response.

[158] EU, Interview, 27 July 2016.
[159] EU, Interview, 6 September 2016.

- **MSP** and **CIMA:** Established by the Council in 2016,[160] the MSP builds on the concept of a "Shared Service Centre", planned as a centralized structure for support to missions in the domains of IT, human resources, procurement and others. In its current form, the MSP aims to improve management, deployment and conduct of CSDP civilian missions. As such, it should address the existing practice among missions of relying on systems developed and used by other missions, which often results in inter-mission dependencies, limited control and use of systems not tailored to the specific needs of a mission. The MSP currently consists of an IT unit, a logistics unit and one human resources person. A procurement unit is being set up. The team is currently developing a web-based platform named

- **CIMA** (Centralized Information Management Application). CIMA will be a centralized, unclassified web-based application to support core administrative processes of all (civilian) CSDP missions. Currently, the focus of development is on human resources functionalities (address book, personnel status, inventories, and so on). CIMA will be piloted in the EUCAP Sahel Mali mission in June 2017. In a later stage, it will also comprise a telephone system and a planning infrastructure. It could also integrate other functionalities (e.g., for procurement) and offer interfaces with systems of other bodies such as FPI. Developing a new finance system is currently considered to be too complicated and is hence not prioritized. Situational awareness is also not a priority, indicating that a future OCP could be complementary to CIMA and the work of the MSP. Interviewees could also envisage CIMA being built in a complete communication and information system that also offers wiki, fora, etc.[161] CIMA will be Internet-based—that is, it will be installed in Brussels and mission staff will be able to access it via the Internet only. As some CSDP missions operate in adverse conditions where Internet is not reliable, this may impact the effectiveness of the system. A key challenge for the MSP in general is the limited resources available, which constrains its level of ambition, as only very basic services can be developed and implemented with the resources currently available. That said, EU staff interviewed are convinced of the value of the MSP in terms of cost efficiency, claiming that the investment would be recouped after the launch of one new mission.[162]

- **IT Security Portal:** This is a portal created by the EEAS Field Security Division. It comprises different kinds of security-related information, including travel of staff members, location of local agents, tracking of armed vehicles and an overview of security-trained staff. The portal aggregates information and also provides GIS-based applications.

[160] Council of the EU, Council Conclusions on the Mission Support Platform, 18 April 2016. http://www.consilium.europa.eu/en/press/press-releases/2016/04/18-fac-mission-support/.
[161] EU, Interviews, 18 January 2017.
[162] EU, Interviews, 18 January 2017.

In short, within the EEAS context as well as the wider EU institutional environment, several tools and initiatives have been used or are currently in place that aim to support information exchange, situational awareness and operational control in the context of EU crisis response and CSDP. At the same time, the overall picture of existing systems remains very fragmented. It should therefore be avoided to create yet an additional layer. Instead, any new system should be used as an opportunity to contribute to more coherent information exchange and communication by building on and linking with existing systems and initiatives that work well (e.g. the MSP), rather than duplicating their efforts and add to the complexity. This is illustrated by the OPCEN and its SCOPE portal, which proved to have little added value as users pointed out that it duplicated existing channels of information exchange.

This is particularly true for situational awareness. No system or standard practice is currently in place to feed situational awareness information and analysis present across the EU institutions (e.g. DEVCO, EEAS, other CSDP missions) into the planning phase of new CSDP missions. However, the WKC plays an important role as a hub for information exchange and situational awareness and as a link between the CSDP missions and the HQ level, and therefore has untapped potential to fill in existing gaps and missing links across EU stakeholders involved in mission planning.

4.2.2 Field-level practice

In addition to the tools for communication and coordination described above, CIVILEX has undertaken several case studies on communication and information exchange systems and practices used in specific CSDP missions. Summaries of these are provided in section 3.2 above. In addition, D2.2 of the CIVILEX project contains more detailed analysis and lessons learned on the Horn of Africa and the Kosovo case studies.

Based on this work, a number of observations can be made regarding field-level practice on information exchange and communication. While there have been several initiatives and attempts to improve information exchange, situational awareness and operational control at the HQ level, deployed CSDP missions still face a lack of standardized, harmonized and user-friendly tools available to them to perform these functions. This has led to three common practices: 1) a reliance on simple IT solutions and face-to-face communication; 2) mission-to-mission exchanges of IT systems; and 3) use of shadow IT solutions.

First, in the absence of more advanced IT solutions, much communication inside missions and with other actors in the field and at the HQ level relies on face-to-face communication or simple IT options such as email with attachments. As a consequence, information

exchange is very dependent on personal relations. As missions are often faced with high staff rotation, this has potentially adverse consequences for effective communication and business continuity. Moreover, several mission support tasks have been described as very cumbersome in the absence of more sophisticated IT tools.

Second, a bottom-up exchange of practices and IT tools between CSDP missions can be observed as well. For instance, EUCAP Nestor uses a system for logistics developed by EULEX Kosovo, while the procurement system of EUCAP Nestor is also used in EUMM Georgia. Another example is the sharing of secure terminals by EUNAVFOR Atalanta with EUCAP Nestor staff to foster secure exchange of information between both CSDP entities. However, interviews also revealed a number of issues with such practices: each CSDP mission operates in a different context and has a different mandate, resulting in diverging needs. As a consequence, the systems used in one mission are not always adequately designed to serve the needs of another mission. Moreover, as some missions rely on systems developed and managed by other missions, they have little control over the IT solutions that are in use. Such observations support the case for making available a variety of developed IT solutions for mission support tasks that can be centrally developed yet easily tailored to the specific needs of each mission.

Third, missions (and, to a certain degree, headquarters staff) have been found to often rely on non-official publicly available information exchange tools, such as WhatsApp or Facebook messenger, which are used to circumvent the prescribed means and procedures. Such applications are often used in the absence of user-friendly and reliable alternatives for open and flexible information exchange. Use of such "shadow IT" has been revealed for exchange of both formal and informal information, including for operational information exchange with EU and non-EU counterparts.[163] Within missions, WhatsApp is also used for security alerts.[164] While such shadow IT solutions offer quick and flexible options for communication and exchange of documents, they may come with risks for both information security and staff security.

To sum up, despite several efforts to improve and streamline information exchange at the HQ level of the EU, missions lack standardised tools to exchange information and communicate within missions, as well as with the HQ level and other actors in their theatre of operations. This forces mission staff to rely on simple IT solutions, face-to-face communication and shadow IT applications, with consequences for the effectiveness and efficiency of communication and business continuity, as well as both information and staff security. How these observations and lessons learned outlined in this section 4.2 relate to the implications for the design of a future OCP will be detailed in section 5 below.

[163] EU, Interviews, 23 August 2016 and 24 November 2016.
[164] See CIVILEX D2.2.

4.3. Managing sensitive data: Regulations and policies in the field of security

The purpose of this section is to identify and analyse the most relevant regulatory tools applying to the management, exchange and distribution of information and data in civilian CSDP civilian missions, which interviews have identified as one of the key areas for improvements in CSDP civilian missions. The management of sensitive data is of critical interest in the design of a future OCP, especially in the context of security missions and operations. Indeed, data management is a transversal action in the CSDP missions and it is applicable to all the phases: Identification of a crisis, development of CMC, operation planning, deployment, strategic review and closure. For instance, the availability of the appropriate systems of information classification would facilitate synergy and collaboration among stakeholders, improvement of the decision-making process (the appropriate people having the correct information at the right time) and lower possibility of security breaches. Likewise, rigorous data protection regimes define and shape how personal data can be gathered by and transmitted among EU actors.

Based on these needs, the *sensitivity of the information* is the data policy focused on providing a framework for handling information that can potentially pose a threat to European security and to the safety of European citizens. Data policy regarding sensitivity of information will deal with regulation on how data is handled and under which conditions it can or must be distributed, with a view to ensure that the information is kept at all times in the right hands. Therefore, it is subsumed under precise regulatory frameworks on Classified Information and on Personal Data.[165]

4.3.1. Classified and sensitive information

EU Classified Information definition and classification

According to Article 2 of the EEAS Decision,[166] EU Classified Information (EUCI) should be understood as *"any information or material designated by and EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States"*.

The notion of "EUCI" covers both "information" (recorded in a document or not) and "material". Material means any document or item of machinery or equipment, either manufactured or in the process of manufacture.

[165] Another aspect of data management, licensing of intellectual property rights protected material—a data policy focused on providing a framework in which the terms of usage of the information, including its commercial value, are clearly established—is presented in Annex VIII.

[166] EEAS, Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service (2013/C 190/01), Official Journal of the European Union, 29 June 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0629(03)&from=EN.

The access to this information is strictly controlled and managed throughout its life cycle by security measures designed to protect its confidentiality, integrity and availability.

Such information is protected by a security classification. This classification, common among European bodies, is categorized in four levels, defined by the severity of the impact of disclosure from the highest to the lowest level:

- ***TRES SECRET UE/EU TOP SECRET****: information and material the unauthorized disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the member states. Official categories of classified information will be listed and defined.*
- ***SECRET UE/EU SECRET****: information and material the unauthorized disclosure of which could seriously harm the essential interests of the European Union or of one or more of the member states.*
- ***CONFIDENTIEL UE/EU CONFIDENTIAL****: information and material the unauthorized disclosure of which could harm the essential interests of the European Union or of one or more of the member states.*
- ***RESTREINT UE/EU RESTRICTED****: information and material the unauthorized disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the member states.*

All EUCI data must fall under one of these levels of confidentiality. There is a fifth level of document security, called **LIMITE UE,** which is used for the day-to-day work and the internal management of documents. This label applies to papers which are often published later, such as a statement by Jean-Claude Juncker before he makes it, or draft EU summit conclusions. Any EU official or diplomat can read, email or print such documents, and they are frequently leaked to the press.[167]

If the document is outside these marking levels (meaning that its disclosure does not prejudice the interests of the EU or one of the member states), it is classified as **UNCLASSIFIED, For Official Use Only**.

The regulation requires marking the information according to a security classification. All classified material must be assigned to one of these levels by its author. When the classified information comes from a member state introducing it into the structures of the Union, the Council or the EEAS, this information should be protected in accordance with the requirements applicable to EUCI.[168]

[167] Rettman A., What is 'SECRET UE' anyway?, EUobserver, 24 September 2012, https://euobserver.com/secret-ue/117634.

[168] A table of equivalence of security classification is included in Appendix B to Council Decision 2013/488/EU of 23 September 2013.

Security Measures

Measures for protecting classified information extend to: persons having access to classified information (access restrictions), classified information-carrying media (management of EUCI in paper and electronic format) and all premises containing classified information (physical security).

In the context of the development of an OCP, here the interest is in the access restrictions and in the management of electronic information and material through Communication and Information Systems (CIS).

These guidelines cover the conditions regulating the access, permission, creation, transmission, destruction, carriage and exchange of EUCI.

Access restrictions

The "need-to-know" principle means that EUCI is authorized only for persons who, by reason of their duties and for the requirements of the service, need to have knowledge of, or to use, such information. This principle applies to all levels of classification.

EUCI access can also be granted if the person has been security cleared to the relevant level and has been briefed on his or her responsibilities. Depending on the level of classification, these requirements apply differently, as shown in Table 3.

Classification level	Need to know	Authorization (Security Clearance)	Security briefing
EU RESTRICTED	yes	no	yes
EU CONFIDENTIAL	yes	yes	yes
EU SECRET	yes	yes	yes
EU TOP SECRET	yes	yes	yes

Table 3 - Summary of requirements for accessing EUCI

Protection of EUCI handled in Communication and Information Systems (CIS)

In the context of EUCI, CIS refers to any system enabling the handling of EUCI in electronic form (e.g., IT system, secure telephone, secure video conference, etc.). Such systems are designed for rapid retrieval, communication and use, but they are vulnerable to many risks. These include access to the information by unauthorized users, or denial of access to authorized users. There are also the risks of unauthorized disclosure, corruption, modification or deletion of the information. Furthermore, the complex and sometimes fragile equipment is expensive and often difficult to repair or replace rapidly.

These systems are therefore attractive targets for intelligence-gathering operations and

sabotage, especially if security measures are thought to be ineffective.

The main purpose of information security measures is to provide protection against unauthorized disclosure of information (loss of confidentiality) as well as against loss of integrity and availability of information, and where appropriate to assure information authenticity and non-repudiation of actions. They are based in the Information Assurance principles and characteristics, as defined in Decision 2013/C 190/01:

- *Authenticity: the guarantee that information is genuine and from bona fide sources.*
- *Availability: the property of being accessible and usable upon request by an authorized entity.*
- *Confidentiality: the property that information is not disclosed to unauthorized individuals, entities or processes.*
- *Integrity: the property of safeguarding the accuracy and completeness of information and assets.*
- *Non-repudiation: the ability to prove an action or event has taken place, so that the event or action cannot subsequently be denied.*

To mitigate risks to CIS, a range of technical and non-technical measures that shall be implemented are listed in Annex A IV (16) of Decision 2013/C 190/01:

- *Deterrence: security measures aimed at dissuading any adversary planning to attack the CIS.*
- *Prevention: security measures aimed at impeding or blocking an attack on the CIS.*
- *Detection: security measures aimed at discovering the occurrence of an attack on the CIS.*
- *Resilience: security measures aimed at limiting impact of an attack to a minimum set of information or CIS assets and preventing further damage.*
- *Recovery: security measures aimed at regaining a secure situation for the CIS.*

In the prevention domain, there are many techniques to detect and avoid a security attack. Users usually represent the weakest point, so it is very important that all staff keep a high level of awareness of the risks and follow all security procedures. For example:

- Don’t allow users to install or reconfigure any software/hardware, run unauthorized software or bring any unauthorized devices into the Secured Area where the CIS is located.
- CIS users must inform security authorities about any incidents.
- Do not give access or bring unauthorized persons into the Secured Area.
- Do not accept requests to modify or disclose data, even from authorized superiors, without having undergone approved authentication procedures.
- Users shall only be given access, privileges or authorization they require to perform their tasks, in order to limit any damage resulting from accidents, errors or unauthorized use.

- Information Assurance education and awareness training shall be mandatory for CIS users.

All the users authorized to use the platform should be clearly identified and assigned to a profile. A robust authentication system must control the access. Depending on the profile, a restricted number of tasks and operations are available and the information is filtered according to the access permission of the user.

The other sensitive point of any CIS, from which majority of threats and cyber-attacks arise, is the interconnection. The best way of transferring data, better than carriage of removable storage media between systems, is to transmit it electronically. For that purpose both networks should be interconnected, which means "the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way."[169] These are the basic requirements applying for all interconnections of CIS:

- *There shall be no interconnection between an accredited CIS and an unprotected or public network.*
- *Any exchange of information should be controlled and protective measures implemented.*
- *Operational requirements for such interconnections should be defined and approved by the competent authorities.*
- *All interconnections should be accompanied by a risk management and accreditation process*
- *Boundary Protection Services shall be implemented at the perimeter of the CIS.*

Depending on the level of classification and the users involved in the information distribution, different networks for communication and information are available at the EU level (Table 4).

Classification level	Internal transmission	Transmission to Delegation
EU RESTRICTED	Through ROLAN	Through Extranet-R or for COREU[170] via CORTESY
EU CONFIDENTIAL	Through SOLAN[171]	Through COREU via CORTESY
EU SECRET	Through SOLAN	Only on paper
EU TOP SECRET	Specific arrangements made by the Director of the GSC Security	Specific arrangements made by the Director of the GSC Security Office

[169] Wikipedia, Interconnection, https://en.wikipedia.org/wiki/Interconnection

[170] COREU is an EU communication network between the 28 EU countries, the Council, the EEAS and the Commission. In providing a regular flow of information, it facilitates cooperation on foreign policy matters. In particular, COREU allows decisions to be taken swiftly in emergencies.

[171] SOLAN is the Secure Office Local Area Network in which European Command and Control Information System (EUCCIS) and other applications run.

	Office or his designated representative	or his designated representative

Table 4 - Electronic transmission means at European level

There are also a number of cryptographic rules and TEMPEST[172] policies and guidelines that must be implemented according to the classification level of the information transmitted, which will be deeply covered in "D3.1 – An overview of core OCP requirements".

A number of authorities exist in the frame of the EEAS to advice, review and verify that all the above-mentioned measures and policies are correctly implemented: Information Assurance Authority, TEMPEST Authority, Crypto Approval Authority, Crypto Distribution Authority, Security Accreditation Authority, Security Accreditation Board and the Information Assurance Operational Authority.

A future platform for situational awareness should rely on the principles mentioned above for the protection of EUCI handled in communication and information systems, as they are articulated to govern the EU architectures and structures for managing EUCI. Nonetheless, further elaboration will be required to tackle the requirements of stakeholders in CSDP missions. In addition to the EU policies and rules, national agencies may play an important role as they may be responsible for a number of processes that could influence the mission's workflow. Two examples are provided below:

- Provision of security clearance to manage EUCI to national citizens according to their own internal procedures that include user needs, purpose of handing EUCI and personal background and data.
- Certification of equipment (hardware and software) for managing and distributing EUCI according to the required standards and protocol.

4.3.2. Personal data

Data protection legislation and principles

While section 4.3.2 focused on the European security policies and rules driving the management of EUCI, the current section tackles other type of sensitive data, such as personal data.

Personal data is defined as information relating to an identified or identifiable natural person, that is, information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information.[173] If data about such a person is being processed, this person is called the "data subject". Thus, for the protection rules to be applicable, there is no need for high-quality identification of the data subject, just a piece of

[172] TEMPEST refers to spying methods that use leaking emanations, including unintentional radio or electric signals, sounds and vibration, in order to reconstruct intelligible data.

[173] European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, European Union Agency for Fundamental Rights, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

information containing some elements through which the person can be directly or indirectly identifiable.

It is worth stating that the right to the protection of personal data has the status of a unique fundamental right. In Europe, with one of the most restrictive systems in this domain, the entry into force of the Treaty of Lisbon in December 2009 implied that its protection became legally binding (Article 16(1) of the Treaty of the Functioning of the EU).

In recent times a reform of data protection rules has been performed in the EU. On 4 May 2016, the official texts of the Regulation (Regulation 2016/679) and the Directive (Directive 2016/680) were published in the EU Official Journal. While the Regulation entered into force on 24 May 2016, it shall apply from 25 May 2018. The Directive entered into force on 5 May 2016 and EU member states have to transpose it into their national law by 6 May 2018 (see Annex I for more details).

In article 9 of the Directive (EU) 2016/679, the particular case of sensitive data is addressed. This type of data is sensitive in relation to fundamental rights and freedoms and includes data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex life. In principle, the processing of this data is prohibited, however a number of exceptions are described in article 9(2) among which:

- *(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.* Such consent has to be explicit and can be given orally, in writing or any other appropriate form. Data subject must receive sufficient information in advance, in order to understand the scope and consequences of consent.
- *(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.*
- *(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

Relevant input to a future Situational Awareness, Information Exchange and OCP for supporting CSDP missions should specify that the management of personal data must follow the EU principles, policies and rules and must foresee the implementation of these legal

guidelines. CSDP Missions can produce a lot of personal data, which due to its sensitivity requires a protective framework. EU data protection legislation and principles must fulfil this need in terms of personal data, in complement to the existing EUCI regulation. For illustrative purposes, the high level of personnel turnover in the CSDP missions requires that personal data be dealt with on a continuous basis.

Processing of personal data

Processing of personal data could be understood as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[174]

Under EU law, the rules on security of processing imply an obligation of the controller to ensure that technical and organizational measures are undertaken so as to protect the personal data with an appropriate level of security. The controller remains legally responsible if someone who works for the controller discloses personal data and breaches data protection legislation. The measures mentioned by the Regulation 2016/679 include:

- *the pseudonymisation and encryption of personal data;*
- *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
- *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
- *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

However, data security is not achieved just by having the right equipment (hardware and software) but also by changing provisions for employees and the internal organizational procedures. Some of the internal rules include:

- Distribution of responsibilities and assigning a clear responsibly for data processing ("controller of the processor").
- Keeping a record of the personal data processing activities.
- Applying the data protection by design and by default principle, which implies collecting only the necessary amount and extent of personal data for each specific purpose, and keeping it the required period of time.
- Offering adequate data security training and education to staff members about these topics.

European bodies and authorities

Application of data protection policy within the CSDP missions mainly depends on three

[174] Ibid.

main stakeholders as described below.

European Data Protection Supervisor (EDPS)

The EDPS is the EU institution acting as independent supervisor authority at the EU level with the following responsibilities:

- Tracking and supervising the processing of personal data by the EU institutions and bodies according to the data protection rules. This ranges from prior checking to analysis of specific risks and management of complaints and enquiries.
- Consultation: Giving advice on policies and legislation which relate to personal data including the proposal of new legislation.
- Cooperating with authorities to ensure consistent data protection.

The EDPS, as an institution, relays the daily work to the office of the EDPS which is intended to serve as a neutral centre for enforcing and reinforcing EU data protection and privacy standards in practical and legal terms.

Data Protection Office at EEAS

The purpose of this Office is to meet day-to-day obligations. EEAS usually needs to collect personal data including sensitive information such as professional data and experience through various processes such as conference invitations, calls for tenders, etc.

The Office follows the EEAS Decision of 8 December 2011 which applies the EU Regulation 45/2001. These rules apply to all departments within the EEAS and all EU Delegations that process information identifying individuals. The Data Protection Office at EEAS works through a Data Protection team that has several roles:

- Creating awareness about data protection issues for staff, visitors, providers and, in general, any EEAS-related citizen.
- Providing notifications and privacy statements.
- Providing advice (formal advice and informal tips, recommendations on rights and obligations).
- Maintaining and updating the personal data register.
- Notifying risky processing of personal data to the EDPS and responding to requests from the EDPS.
- Investigating matters and incidents on request or on its own initiative.

National Agencies

National agencies are responsible for the development of national legislation transposing the information content of the EU regulation and its corresponding application via appropriate procedures and implementation measures. Likewise, national agencies assume all the responsibilities and roles applied to the EDPS but at the member state level.

For the purpose of the CSDP missions, they provide the legal regulatory framework for the personnel of member states who could be part of CSDP missions. As an example, these national agencies might create the rules and procedures that ministries of foreign affairs and defence have to follow with regard to treatment of the personal data of their own staff.

5 Institutional policy aspects and lessons learned

The following chapter is drawing together the findings and analysis of the CSDP in the context of EU external action (chapter 2), of the evolution, current state and recent developments for the strategic background of CSDP operations (3), and of the comprehensive analysis and review of the institutional/administrative dynamics, the institutional technological landscape and the data management environment (chapter 4). On the basis of the desk research, mission case studies, the field visits, interviews and stakeholder engagements activities carried out as part of the CIVILEX project, this research arrived a set of observations and recommendations dealing with institutional policy aspects which should be taken into account when further developing the OCP. In particular through the analysis of the literature available on past and present missions and through the assessment of current and future trends in CSDP activities, the OCP has the potential to offer remedies in an institutional and administrative environment for civilian CSDP that this research considers not be substantially changing in the coming few years. The research refrains from making particular recommendations regarding specific missions and scenarios as the OCP is anticipated to be phased-in to respond to future operational needs primarily and not to rectify shortcomings in currently ongoing operations. In this respects, the case studies (chapter 3) helped to identify specific shortcomings and gaps illustrating generic challenges and needs for CSDP civilian missions. Section 5.1 of this chapter recalls of peculiarities of civilian CSDP relevant for the OCP. The following sections contain observations and recommendations for enabling the OCP to support the effectiveness of civilian CSDP within external action (5.2.) and EU action at large (5.3); and considerations for CSDP on the global scene (5.4.).

5.1. Persisting institutional peculiarities in the field of civilian CSDP

The field of civilian crisis management saw considerable growth from 1999 to 2008, with the first mission becoming operational on 1 January 2003 (the EUPM BiH). Civilian crisis management operations have primarily been deployed to support and build the capacity of police, security and rule-of-law institutions. Information exchange and the management of operational information is an indispensable element of their activities.

Following the establishment of the EEAS, civilian external action has started to become more comprehensively integrated. CSDP missions in general have also gained an enhanced integration and access to the information sphere of the EEAS, as the structures were integrated into the EEAS and led by a Deputy Secretary General.

At the same time, the CSDP structures, including those for CSDP civilian missions and in particular the CPCC, continue to maintain a separate position within the wider EU external action set-up. The "insularity" of the CPCC in a separate building (as part of the Cortenbergh structures) exemplifies the particular identity of civilian CSDP within the context of the larger EU civilian external action.

The practical implementation of decisions on CSDP civilian operations is led by the CPCC, headed by a Director who is as well the CivOpCdr of all civilian operations. Command and control for the missions lies with the CivOpCdr, and is exercised through individual Heads of Mission in the field.

However, CSDP civilian missions are financed through the Community budget whereby the funding is managed by the FPI Service of the European Commission.

The salaries for the seconded personnel are borne by the respective member states (or seconding EU institution) while the salaries for contracted personnel are covered by the mission budget. The specific staffing arrangements add complexity due to rotations, staff turnover and the resulting lack continuity. Costs for mission support (i.e., communication and information technology, transport, offices, supplies, etc.) are also decentralized and borne by the mission budget. The upshot of this is fragmentation and heterogeneity in terms of information technologies across missions. The generic procurement rules of the PRAG apply. Yet, framework contracts exist for certain items. Specific arrangements are being put in place to centralize mission support structures through a MSP. Within the CPCC a specific mission support division deals with these issues as well as personnel, recruitment and training questions.

This particular set-up contributes considerable challenges in information exchange, situational awareness and operational control. These challenges concern both the CPCC level and the civilian CSDP operations in the field. The following institutional policy aspects and procedural lessons learned have been identified which will need to addressed to contribute to the effectiveness of an OCP.

5.2. Observations and recommendations: scope, lesson learned and ownership

Scope of the OCP

In order to add value and impact to the operational effectiveness of civilian CSDP action, an OCP should help CSDP structures and officials access existing information and data within the EEAS and beyond. Especially during the phasing-in stage of civilian CSDP, a recurring

observation is that it is necessary to strengthen situational awareness for planning and deployment of civilian CSDP operations, thereby accelerating the achievement of initial operational capability. Conversely, knowledge gathered within the mission, at all stages of its deployment cycle, should feed into wider decision-making and implementation of EU external action. Specifically, the OCP should allow conduits:

- to provide CSDP missions with access to information from other information providers within the EU system (EEAS, Commission, Council and EU agencies);
- to provide CPCC with systematic access to information and data, political background analysis and archival information on the theatre of operations and on past and ongoing EU activities, including in the phasing-in stage of a mission;
- to provide access to information for EEAS, Commission (especially FPI) and Council stakeholders through dedicated windows in the OCP user interface to contribute to their knowledge and situational awareness in the mission's theatre of operations;
- to create a common information space for the civilian and military branches of the CSDP, to which the OCP can seamlessly contribute;
- during phasing-out of a mission, to ensure that situational awareness products within a mission are made available for further use for other EU external action instruments;
- to ensure full compatibility with the WKC (WKC) as a key link between the mission and headquarters level to further strengthen an integrated approach to situational awareness; and
- to better integrate information from the CSDP civilian missions' Mission Analytic Capability (MAC) into the overall information flows of EU external action.

<u>Lessons learned on information management</u>

In the area of information and knowledge management there is a need to update the CSDP environment through an appropriate set of policy and guidance tools for CSDP personnel at all levels, as well as other EU personnel working with CSDP operations. There is a need:

- to encourage, develop and support a culture of institutional memory-building and knowledge-sharing, including through enhanced training and in-mission learning;
- to continuously develop and adapt standardized information storing and archiving tools and procedures;
- to harness the possibilities of modern information technologies (including meta-information searchability);
- to review and reassess current information exchange agreements between CSDP and other EU actors;
- to develop an information management concept and revise rules for mission staff, e.g., political advisers, security staff, MAC analysts or press and public information officers ;
- to develop information plans for various theatres of operation, in conjunction

with all EU external action bodies, to identify common information needs to benefit the more transitional and temporary character of CSDP operations; and

- to allow access to and use of mobile devices and provide a user-friendly information exchange tool.

Ownership of the OCP

The question of information management also relates to the key issue of ***ownership*** of a future OCP, in the physical and legal sense far more than conceptually. Currently, the CPCC technological infrastructure is financed through the administrative budget of the EEAS while the missions are financed through the CFSP operational budget managed by the FPI, with missions having "legal personality". Provided that the overall framework of the financing of civilian CSDP is not changed, the following (not exhaustive) options would seem feasible:

- OCP financed and owned by the EEAS (administrative budget) and put at the disposal and management of the CPCC/MSP (unlikely option);
- OCP financed through the individual CSDP civilian mission budgets (as part of a framework contract), managed by the CPCC/MSP (likely option); or
- Initial financing through EEAS budget, and ownership and management by CPCC/MSP and fee-based contributions by the individual CSDP civilian missions.

The question of which institution should bear the costs, where the platform should be institutionally anchored, who activates and manages the OCP, and whether this should be centrally within the CSDP divisions of the EEAS or rather decentralized within the missions deployed in the field leads to another set of questions about the balance that should be found between centralization and standardization. To what extent should the OCP provide standardized information management practices or allow flexibility to tailor functionalities to the specific contexts, mandate and needs of each mission? In this context, the study would recommend the following:

- to design an OCP that can function as the information system for all CSDP civilian missions, and that is placed under the responsibility of the CivOpCdr, who sets the rules and provides guidance, including on intra-CSDP information exchange;
- to create "mission branches" within the OCP that should be made available with the official start of mission planning and allow for mission-internal information exchange and management; while the overall responsibility for the OCP rests with the CivOpCdr, the HoMs could be granted the right to manage and control (and customize) parts of the OCP which provide information management services related to the exercise of their contractual obligations (e.g., in the area of finance, etc.);
- to further clarify the question of the legal personality of missions with regard to the data ownerships rights and obligations of data stored in the OCP;
- to consider cost-sharing options for paying for the OCP, including for future development and maintenance costs which may not be foreseen by the CSDP budget;
- to build on and work with existing information management systems and

initiatives that are in place in the context of civilian CSDP and wider EU external action, such as the IPCR arrangements and the ARGUS system;

- to concentrate mission support functions under a coherent umbrella or platform, bringing together FPI and CPCC functions, based on an operational strategy or guidance;
- to use the MSP as the tool to underpin and support the development of the future OCP;
- to approach the OCP through a modular design concept to respond to the diverse needs and contexts of CSDP civilian missions;
- to design the OCP not *for* the users but *with* the users, following an interactive design process.

Also related to the question of ownership of the OCP and its underpinning processes of information exchange are questions of data security and EUCI. More harmonized information exchange practices are central in fostering information security. Therefore, the process of developing OCP will need to contribute:

- to fostering a classification- and security-aware working culture and practice;
- to distinguishing more clearly between classification of information (which happens by decision) and information security (which should become the rule);
- to increasing security through the introduction of personal ID access systems;
- to improving business intelligence processes for security (both information and mission security, including mission personnel) and better general data protection and protection of person-related data.

To enhance the full potential of a future OCP, this study also recommends considering a review of existing classification rules and their respective technological requirements.

5.3. Observations and recommendations: OCP in the EU external action context

This section formulates recommendations on the internal institutional and policy aspects of civilian CSDP and wider EU external action. It looks not only at how to streamline and improve information flows between the missions deployed in the field and at the headquarters level, but also at how horizontal communication between CSDP civilian missions and other EU external actors can be improved. This also concerns the intra-CSDP cooperation between civilian and military structures in Brussels as well as operations in the field. This is especially important given that military operations and EU actors in the area of freedom, security and justice are increasingly being deployed in the same theatre or region of operations, such as the Mediterranean.

CSDP civilian missions are deployed in theatres where the EU has been already active before through other external action instruments (e.g., CFSP, humanitarian aid, development programmes). EU Delegations are hence a key reference point for CSDP operations in the field.[175]

With the strengthening of the internal–external security nexus, increasingly, civilian CSDP operations interact with other civilian activities with an external dimension such as FSJ actors and their relevant agencies (e.g., Frontex, Europol). CSDP civilian missions have limited access to knowledge and information generated by previous and current external actions and EU actions with an external dimension in a systematic manner, although agreements of CSDP exist on operational cooperation with Europol and others.

The information technology infrastructure of the CSDP civilian missions varies considerably as missions purchase and utilise different types of hard- and software. More harmonization in this area is expected after the establishment of more harmonized mission support structure, yet those structures will not be able to replace a more strategic decision within the EEAS on technical standards and adaptation to newer information technology development such as cloud computing, collaborative working and social media applications.

Based on the findings and observations, the following recommendations can be formulated:

- Define information management roles between the CPCC and EEAS as well as the Heads of Mission and the EU Delegations, e.g., through adapted profiles and interfaces for political advisers, security officers and other mission functions;
- Specific arrangements should be developed for certain mission-internal business processes such as finance or personnel issues, in accordance with existing legal provisions (taking into account the legal personality of mission since 2013).
- Design the OCP so that it contributes to field security both across missions and in a given country or theatre by gathering field security-related information and situational awareness from diverse EU actors deployed in the field;
- Evaluate the possibility to provide dedicated windows within the OCP that can be accessed by actors in the field of freedom, security and justice (Frontex, Europol) to foster information exchange with CSDP actors;
- Strengthen information exchange between military and civilian CSDP by reviewing existing arrangements for civil–military information exchange both in view of the opportunities offered by the OCP and in view of new scenarios for deployment, and develop SOPs/SOIs for the LNO system (e.g., through Single User Systems); and
- Provide strategic guidance on information exchange and situational awareness to

[175] European Special Representatives (EUSR) used to be systematically deployed alongside CSDP operations. This practice has been changing in the last years. While information exchange and situational awareness remain areas for EUSR–CSDP cooperation, the interaction with EU Delegations is becoming more dominant in the field.

CPCC and the missions through a joint PSC–COSI agenda in the area.

5.4. Considerations for an OCP in the context of CSDP on the global scene

As civilian CSDP operations are deployed in regions and theatres where the EU has been active before, CSDP operations also have a natural link to UN activities. The document "UN-EU Strategic Partnership on Peacekeeping and Crisis Management: Priorities 2015-2018" outlines how, apart from cooperation in political, substantive and operational aspects, "closer cooperation on mission support, logistics, and the exchange of information and analysis are other important goals of our deepening cooperation".[176] As furthermore all EU member states, as well as the third states contributing to CSDP, are members of the UN, it is important to take into account lessons learned by the UN in the area of information exchange, situational awareness and operational control. With currently 16 peacekeeping operations running and 55 completed, considerable institutional memory on both military and civilian aspects of such operations exists in the UN with reference to information management. Deliverable 4.2. further elaborates the issues related to the UN; key observations are:

- While the Department for Peacekeeping Operations is investing substantial resources and intellectual work into questions related to information exchange and information management arrangements, and despite Peacekeeping Operations having single chains of command and financing, fragmentation remains a challenge.
- Technology development happens within the UN, but remains insular between departments, programmes, funds, etc.
- With the UN, the centrality of information management has been recognized by the Secretary-General and the UNOCC (UN Operations and Crisis Centre), resulting in a more strategic and visible leadership. This has also resulted in the investment in the necessary intellectual and organizational capacity to develop and frame information and move to an information-centric information. An example is the work of the special Committee on Peacekeeping Operations (C34) on a new intelligence framework.
- Given the relatively small scale of civilian CSDP in comparison to the UN, it remains to be seen whether a separate department for mission support, as exists in the UN with the Department for Field Support, would be justifiable and desirable.
- Standardization of business processes seems to enhance efficiency and "esprit de corps". Yet, over-centralization carries risks and needs to be avoided, as evidenced by the development by the enterprise system UMOJA which has run over budget and lacks functionality to date.

[176] Council of the EU, Strengthening the UN–EU Strategic Partnership on Peacekeeping and Crisis Management: Priorities 2015-2018, 7632/15, Brussels, 27 March 2015, http://data.consilium.europa.eu/doc/document/ST-7632-2015-INIT/en/pdf.

- The exchange of classified information between the EU and UN has been agreed but will remain difficult due to different standards and security cultures.

While this study has focused on the civilian CSDP, the various case studies highlight the fluidity between civilian and military forms of external action, including in the field of intelligence and information gathering, as well as among the uniformed officials of member states (e.g., gendarmerie) and other forms of cooperation. Several missions are cooperating with NATO, and the developing maritime military CSDP is interacting with a broad variety of actors. Existing cooperation shows the necessity for an OCP to remain flexible and open enough for theatre-based information exchange and situational awareness sharing with non-CSDP/non-EU actors.

6 Conclusions

The EUGS and its related Implementation Plan are the latest of a series of policy documents that have been increasingly zeroing in on the importance of situational awareness, information exchange and operational control for a successful security and defence policy. The endorsements by the Council gave the political mandate to pursue such efforts.

Better information exchange, situational awareness and operational management of missions are much needed in the context of evolving EU civilian missions. Whereas these missions follow a specific set of rules and procedures concerning budgeting, mandate and decision-making, they are strongly linked with other actors involved in the broader EU civilian crisis management enterprise, contextualized in the broader framework of EU external action. This has clear repercussions on the conduct of these missions and their interactions with other EU institutions. As seen in sections 2 and 3, CSDP civilian missions are launched after a rather complex, if not convoluted, process in which many institutions have a say in the nature and features of a mission. Once a mission is launched, interactions with these actors are kept constant, and communications with other operational actors in the field increase. CSDP civilian mission activities occur in complex environments in which communicating and knowing one's surroundings is a priority for the success of the mission. As seen from the EUCAP Sahel case study, civil–military coordination is becoming as key as other forms of engagement between EU entities. In another example, the case study of EUNAVFOR MED is an important instance of a military mission deeply cooperating with numerous civilian external partner: local, European and international, institutional and not. Another key relation is between CSDP civilian missions and JHA actors such as Europol, Frontex, CEPOL and Eurojust. European JHA actors are increasingly engaged in planning and implementation of the CSDP civilian missions, evidencing how typical internal security threats such as organized crime and terrorism now need to be tackled also with external policies. Other case studies in this report but also in other deliverables (see for instance D2.2) demonstrate how CSDP civilian missions are not linked up merely with EU actors, but also international players such as NATO, the African Union and the UN. The natural implication for a future OCP platform is that the system will not have to be close to EU actors only, but will have to be accessible to other relevant stakeholders in the field.

The CIVILEX project intends the OCP as an information exchange platform. The term "information exchange" refers to bidirectional information transmission among actors. Since the beginning of civilian CSDP after 2001, computer and telephony (mobile) networks have proven that they can function as a conduit for the exchange. Yet, networks remain insular because of the institutional genesis and the organizational arrangements in place.

Furthermore, the exchange process is not fully harnessing additional computer functions (e.g., visualization, addressing, clustering, filtering, chat-functions, encryption, etc.). A strategic-level decision in the EEAS on technical standards and the inclusion of newer information technology developments such as cloud computing, collaborative working and social media applications may also be required before the end of the decade. The OCP should hence become the principal means to exchange information within CSDP operations and with the CPCC and to provide additional information management functions, including with the wider EU external action community. Those functions should also be devised to create a common information culture and space, spanning the wide-ranging backgrounds and qualifications of the many thousand CSDP officials working in the missions.

A changed approach to information management will allow improvement of the conditions for situational awareness within the CSDP arena. Situational awareness is the (human) cognitive ability of CSDP officials to comprehend how environmental elements (data, information, observations) relate, and to develop an understanding of their meaning and a projection thereof in the future. In an environment where information exchange is changing rapidly—and outside the institutional set-up of EEAS and CSDP structures at an even faster pace—the OCP needs to support users to attain common situational awareness by providing them with timely, relevant and useable information. For the entire chain of command, including the Civilian Operations Commander and the Heads of Mission and their senior staff, shared situational awareness is required inter alia (i) to ensure mandate implementation and in turn to allow for political control and strategic direction to be exercised; (ii) for safety and security of the mission, personnel and assets; and (iii) to contribute to situational awareness shared with military CSDP operations, non-CSDP actors in EU external action, and the civilian EU actors in the area of freedom, justice and security.

In this respect the OCP also responds to the requirements for operational control described by the Council (2007) as “a continuous sense, assess, decide and act cycle executed in order to accomplish and assigned mission”. The OCP therefore responds to the need for (i) information exchange (to sense); (ii) the generation and use of situational awareness (to assess); (iii) rules (to decide); and (iv) tools (to act). The study makes recommendations therefore on the institutional policy aspects to define during the further development of the OCP:

- **The scope of the OCP**: The study found that the OCP should add value to CSDP missions that require better access to information within the EU system (EEAS, Commission, Council); that the CPCC should be provided with systematic access to information and data, political background analysis and archival information on the theatre of operations and on EU activities, throughout the operational life-cycle; and that “dedicated information windows” in the OCP should be provided to EEAS, Commission (especially FPI) and Council stakeholders to contribute to their information and knowledge on EU activities in the domain of civilian CSDP and its

theatres of operations.

- **The information management approach**: The study identified that a facilitator for the success of the OCP will be to encourage, develop and support a culture of institutional memory-building and knowledge-sharing, including through enhanced training and in-mission learning; This should also include the promotion of collaborative information management,; to the development and adaptation of standardized information storing and archiving tools and procedures,; and to develop information plans for various theatres of operation, in conjunction with all EU external action bodies, that identify common information needs.
- **The civilian CSDP context**: To add value and move beyond current limitations, there is a need to design an OCP for all CSDP civilian missions and place it under the responsibility of the Civilian Operations Commander who sets rules and provides guidance. In this respect, the research also found that the CivOpCdr can play an important role in promoting a culture of information-sharing and cooperative working methods, which would be crucial for the effectiveness of any OCP. Furthermore the OCP should allow for the creation of individual "mission branches" with the official start of mission planning and allow for mission-internal information exchange and management. The OCP work place could become the single access point for information in the CSDP context. It should hereby respect the "legal personality" of missions, and in particular the right to manage and control parts of the OCP (e.g., in the area of finance, etc.) should be reserved at the appropriate level. Overall effectiveness and acceptance by the CSDP community will stem from a modular design concept to flexibly respond to the diverse needs and contexts of CSDP civilian missions.
- **The data security and protection context**: The current institutional arrangements are not fostering a data classification- and security-aware working culture and practice. It is paramount to distinguish more clearly between classification of information (which happens by decision) and information security (which will need to become the rule). The study found that the OCP development provides an opportunity to consider a review of existing classification rules and their respective technological requirements.
- **The ownership of the OCP**: Ownership in the physical and legal sense will need to be decided by the end of the development phase. With the suggested scope of the OCP a tension may arise as the CPCC technological infrastructure is financed through the administrative budget of the EEAS, while the missions are financed through the CFSP operational budget managed by the FPI.
- **The OCP within the overall context of EU external action beyond CSDP**: For the OCP to contribute the advancement of EU external action, it is necessary to provide strategic guidance through a joint PSC–COSI agenda to open dedicated windows within the OCP for freedom, security and justice (Frontex, Europol) actors; to review and adapt existing CSDP civil–military information exchange for the OCP; and to take into account the EU–UN cooperation agreement, as well as cooperation with NATO

and third states.

Whereas the study of civilian missions' needs and requirements is a necessary step in the design of a future information system, one should be aware that these primarily stem from the mission's task, duty and mandate. Consequently, if task, duty and mandate change, needs and requirements also will. The EUGS has outlined a strategic vision that will prompt changes in how the EU conducts its foreign and security affairs. These changes will in turn modify needs and requirements. Although this is difficult to completely foresee, the "paradigm shift" in which civilian missions now find themselves is likely to make missions evolve in the same direction we have observed in this deliverable: more civil–military–JHA synergies in the framework of the internal–external security nexus rather than large missions with the ultimate goal of state-building. Regardless of the specifics—certainly important in the context of the design of an information system platform—the changing security environment coupled with the a renewed political mandate to seek more information exchange, improved situational awareness and better conduct of missions make the establishment of an OCP a matter of priority. The OCP has the potential to become an important part of the CSDP operational set-up. This study has identified the strategic and policy drivers and described the institutional barriers and facilitators for the development of an OCP. The changes required to allow for a more effective information exchange, situational awareness and operational control approach within the field of civilian CSDP remain within reach, provided that the cause of establishing a modern operational environment for civilian CSDP can find enough institutional champions with determined vision and leadership.

Bibliography

- Azzoni A. and Pirozzi N., Civili in missione: l'esperienza italiana nelle missioni dell'Unione europea, Roma, Nuova Cultura, March 2016, http://www.iai.it/sites/default/files/civili_in_missione.pdf.

- Benmansour A., Sorensen A., Cannarozzi N., Feasibility Study: Centralised and Integrated Resource Management System for CSDP Missions and Headquarters, Brussels: CPCC, December 2014.

- CivCom advice on the introduction of the overarching principles for a mission analytical capability in a civilian crisis management operations, Council document 15883/09, 13 November 2009.

- Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01, art.15, 18, 21, 27, 38, 43, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M021.

- Council Decision 2012/389/CFSP of 16 July 2012 on the European Union Mission on Regional Maritime Capacity Building in the Horn of Africa (EUCAP NESTOR), Official Journal of the European Union, L 187/40, Art. 2., 17 July 2012, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede121112cd389_/sede121112cd389_en.pdf.

- Council Decision 2013/87/CFSP of 18 February 2013 on the launch of a European Union military mission to contribute to the training of the Malian Armed Forces (EUTM Mali), Official Journal of the European Union, L 46/27, 19 February 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:046:0027:0027:EN:PDF.

- Council Decision 2014/860/CFSP of 1 December 2014 amending and extending Decision 2012/173/CFSP on the activation of the EU Operations Centre for the Common Security and Defence Policy missions and operation in the Horn of Africa, Official Journal of the European Union, L 346/32, 2 December 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0860&from=EN.

- Council Decision (CFSP) 2017/50 of 11 January 2017 amending Decision 2014/219/CFSP on the European Union CSDP Mission in Mali (EUCAP Sahel Mali), Official Journal of the European Union, L 7/18, 12 January 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0050&from=EN.

- Council Joint Action 2008/851/CFSP of 10 November 2008 on a European Union military operation to contribute to the deterrence, prevention and repression of acts

of piracy and armed robbery off the Somali coast, Official Journal of the European Union, L 301/33, 12 November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:301:0033:0037:EN:PDF.

- Council of the EU, Civil-military Co-Ordination: Possible Solutions for the Management of EU Crisis Management Operations: Better Sharing of Information in Theatre", 13218/5/06, REV 5, Brussels, 31 October 2006, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260410cmcoinformationsharing_/sede260410cmcoinformationsharing_en.pdf.

- Council of the EU, Civilian Headline Goal 2008, doc. 15863/64, 7 December 2004, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015863%202004%20INIT.

- Council of the EU, Civilian Headline Goal 2010, doc. 14823/07, 19 November 2007, https://www.consilium.europa.eu/uedocs/cmsUpload/Civilian_Headline_Goal_2010.pdf.

- Council of the EU, Council Conclusions on the Mission Support Platform, 18 April 2016. http://www.consilium.europa.eu/en/press/press-releases/2016/04/18-fac-mission-support/.

- Council of the EU, Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management, 9919/07, 23 May 2007.

- Council of the EU, Implementation Plan on Security and Defence, 14392/16, Brussels, 14 November 2016, https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf.

- Council of the EU, Joint Staff Working Document Taking forward the EU's Comprehensive Approach to external conflict and crises - Action Plan 2015, doc. 7913/15, Brussels, 14 April 2015, http://data.consilium.europa.eu/doc/document/ST-7913-2015-INIT/en/pdf.

- Council of the EU, Outcome of the Council Meeting, 3498th Council meeting, Foreign Affairs (including defence issues), 14418/16, Brussels, 14 and 15 November 2016, http://www.consilium.europa.eu/en/meetings/fac/2016/11/14-15/.

- Council of the EU, Outcome of the Council Meeting, 3525th Council meeting, Foreign Affairs, 7019/17, Brussels, 6 March 2017, http://www.consilium.europa.eu/en/meetings/fac/2017/03/06/.

- Council of the EU, Strengthening the UN–EU Strategic Partnership on Peacekeeping and Crisis Management: Priorities 2015-2018, 7632/15, Brussels, 27 March 2015, http://data.consilium.europa.eu/doc/document/ST-7632-2015-INIT/en/pdf.

- Difesaonline, Intervista al comandante dell'OperazioneEUNAVFOR MED SOPHIA, Amm. Enrico Credendino, 3 August 2016, http://www.difesaonline.it/evidenza/interviste/intervista-al-comandante-delloperazione-eunavfor-med-sophia-amm-enrico.

- DG ECHO, Who we are, http://ec.europa.eu/echo/who/about-echo_en.

- DG DEVCO, About International Cooperation and Development - DG DEVCO, Last update 3 April 2017, http://ec.europa.eu/europeaid/general_en.

- DG DEVCO, Relations with the EEAS, EU institutions and Member States, Last update 3 April 2017, http://ec.europa.eu/europeaid/relations-eeas-eu-institutions-and-member-states_en.

- DG NEAR, Who we are, Last update 6 December 2016, https://ec.europa.eu/neighbourhood-enlargement/about/directorate-general_en.

- DG HOME, Who we are, Last update 3 April 2017, https://ec.europa.eu/home-affairs/who-we-are/about-us_en.

- EEAS, Civilian Operations Commander Instructions VII: Guidelines on document management and procedures for the transfer of closed archives to EEAS HQ, EEAS/CPCC/A2/UK (2016), 23 March 2016.

- EEAS, CMPD Food for Thought Paper: From strengthening ties between CSDP/FSJ actors towards more security in EUROPE, doc. 10934/16, 5 July 2016, http://statewatch.org/news/2016/jul/eeas-food-for-thought-more-security-in-europe-10934-16.pdf.

- EEAS, Conflict Prevention, Peace building and Mediation, Last reviewed 15 June 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/426/conflict-prevention-peace-building-and-mediation_en#Conflict+prevention.

- EEAS, CSDP structure, instruments, and agencies, Last reviewed 8 July 2016, http://eeas.europa.eu/csdp/structures-instruments-agencies/cmpd/index_en.htm#sp.

- EEAS, Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service (2013/C 190/01), Official Journal of the European Union, 29 June 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0629(03)&from=EN.

- EEAS, EU Crisis Response System, https://eeas.europa.eu/headquarters/headquarters-homepage/412/crisis-management-and-response_en#The+EU+Situation+Room.

- EEAS, EU Operations Centre Horn of Africa & Sahel (EU OPCEN), Updated: June 2015, http://eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-operations-centre/docs/factsheet_eu_opcen_23_06_2015.pdf.

- EEAS, Factsheet: EU relations with Sahel countries - Burkina Faso, Chad, Mali, Mauritania, Niger, 17 June 2016, http://eeas.europa.eu/archives/docs/factsheets/docs/sahel-european-union-factsheet_en.pdf.

- EEAS, Multi-annual Civilian Capability Development Plan: Action Lines for 2012-2013, doc. 12111/12, 6 July 2012, http://www.statewatch.org/news/2012/aug/eu-eeas-civilian-capability-action-plan-2012-2013-12111-12.pdf.

- EEAS, "Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign And Security Policy," June 2016, http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

- EEAS, The EUCAP Sahel Mali civilian mission, Updated: June 2016, http://eeas.europa.eu/csdp/missions-and-operations/eucap-sahel-mali/docs/factsheet_eucap_sahel_mali_en.pdf.

- EEAS, European Union Naval Force – Mediterranean Operation Sophia, Update: 30 September 2016, http://eeas.europa.eu/csdp/missions-and-operations/eunavfor-med/pdf/factsheet_eunavfor_med_en.pdf.

- EEAS, EU 2014 Chairmanship Contact Group on Piracy off the Coast of Somalia, 14 May 2014, http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2014/140514_piracy-contact-group_en.htm.

- EASO, European Asylum Support Office: Who we are, https://www.easo.europa.eu/sites/default/files/EASO-Brochure-EN%20.pdf.

- EUAM Ukraine, Our Mission, http://www.euam-ukraine.eu/en/what-we-do/our-mission.

- EUBAM Libya, Factsheet, https://eeas.europa.eu/csdp/missions-and-operations/eubam-libya/pdf/factsheet_eubam_libya_en.pdf.

- EUCAP Nestor, EU Maritime Security Capacity Building Mission in Somalia (EUCAP Nestor), https://www.eucap-nestor.eu/data/file/1427/EUCAP NESTOR_Factsheet_November_2016.qF1oOOwtvM.pdf.

- EULEX Kosovo, EULEX implements its mandate through two operational objectives, http://www.eulex-kosovo.eu/?page=2,44.

- EUPOL COPPS, Mandate: EUPOL COPPS is the European Union Co-ordinating Office for Palestinian Police Support, http://eupolcopps.eu/en/content/what-eupol-copps.

- EUROJUST, Mission and tasks, http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx.

- European Commission, Service for Foreign Policy Instrument (FPI), Last Update 12 January 2016 http://ec.europa.eu/dgs/fpi/about/index_en.htm.

- European Commission and the High Representative of the European Union and for foreign affairs and security policy, Joint Communication to the European Parliament and the Council: The EU's comprehensive approach to external conflict and crises, Brussels, JOIN(2013) 30 final, 11 December 2013, http://www.eeas.europa.eu/archives/docs/statements/docs/2013/131211_03_en.pdf.

- European Commission, 2012 Annual Activity Report Service for Foreign Policy Instruments (FPI) http://ec.europa.eu/dgs/fpi/documents/fpi_activity_report_2012_en.pdf.

- European Council, EU Border Assistance Mission at Rafah Crossing Point (EUBAM RAFAH), Updated: March 2009, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/wgme/dv/13_factsheeteubamrafahversion10_/13_factsheeteubamrafahversion10_en.pdf.

- European Council and Council of the European Union, Coreper II, Last reviewed 7 April 2016, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coreper-ii/.

- European Council and Council of the European Union, Foreign Affairs Council configuration (FAC), Last reviewed 24 January 2017, http://www.consilium.europa.eu/en/council-eu/configurations/fac/.

- European Council and Council of the European Union, Committee for Civilian Aspects of Crisis Management (CivCom), Last reviewed 20 March 2015, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/committee-civilian-aspects-crisis-management/.

- European Council and Council of the European Union, Political and Security Committee (PSC), Last reviewed 20 February 2017, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/.

- European Council and Council of the European Union, Working Party of Foreign Relations Counsellors (RELEX), Last reviewed 8 January 2015, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-foreign-relations-counsellors/.

- European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

- European Union Delegation to the United Nations – New York, Factsheet on EU Intelligence Analyses Center (INTCEN), http://eu-un.europa.eu/factsheet-on-eu-intelligence-analyses-center-intcen/.

- European Security and Defence College, Handbook for Decision Makers: The Common Security and Defence Policy of the European Union, 2014, http://eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/european-security-defence-college/pdf/handbook/handbook-for-decision-makers.pdf.

- Europol, About, https://www.europol.europa.eu/about-europol.

- Europol, Europol Work Programme 2016, EDOC # 736915v18A, The Hague, 3 February 2016, https://www.europol.europa.eu/publications-documents/europol-work-programme-2016.

- European Union Institute for Security Studies, EUISS Yearbook of European Security (YES) 2016, 2015, http://www.iss.europa.eu/uploads/media/YES_2016.pdf.

- Frontex, Mission and Tasks, http://Frontex.europa.eu/about-Frontex/mission-and-tasks/

- Howorth J., Security and defence policy in the European Union, Palgrave Macmillan, 2014, https://he.palgrave.com/page/detail/Security-and-Defence-Policy-in-the-European-Union/?K=9780230362352.

- Minard P., The IPCR Arrangements: A Joined-Up Approach in Crisis Response?, EUISS, Brief Issue 38, December 2015, http://www.iss.europa.eu/uploads/media/Brief_38_IPCR.pdf.

- Ministero della Difesa – Marina Militare, EUNAVFOR MED Operation Sophia - Situazione, http://www.marina.difesa.it/cosa-facciamo/operazioni-in-corso/Pagine/EUNAVFORMED.aspx.

- Oceans Beyond Piracy, Shared Awareness and Deconfliction (SHADE), http://oceansbeyondpiracy.org/matrix/shared-awareness-and-deconfliction-shade.

- Rettman A., What is 'SECRET UE' anyway?, EUobserver, 24 September 2012, https://euobserver.com/secret-ue/117634.

- Rutten M., From Saint-Melo to Nice. European Defence: core documents, EUISS,

Chailot Paper N.47, 2000, http://www.iss.europa.eu/uploads/media/cp047e.pdf.

- EU SATCEN, The Centre, https://www.satcen.europa.eu/about_the_eu_satcen/the_centre.

- Simon L., Command and control? Planning for EU military operations, EUISS, Occasional Paper 81, January 2010, http://www.iss.europa.eu/uploads/media/Planning_for_EU_military_operations.pdf.

- Tardy T., Recasting EU civilian crisis management, EUISS Report, N.31, 01 March 2017, http://www.iss.europa.eu/uploads/media/Report_31.pdf.

- Wikipedia, Interconnection, https://en.wikipedia.org/wiki/Interconnection.

- William A., Jeannine E. A. A. and Wendyam A. S., West Africa Report Assessing the Multinational Joint Task Force against Boko Haram, Institute for Security Studies, Issue 19, September 2016, https://issafrica.s3.amazonaws.com/site/uploads/war19.pdf.

Annex

Annex I: Managing sensitive data: regulations and licensing in the field of security

This annex focuses on two important topics that should be addressed in the provision of recommendations for a future OCP. Firstly, it presents the main regulations the OCP will have to comply with according to the classification level of the information it will be designed to exchange. Secondly, it debates the topic of licensing, which regulates how the situational awareness information (data) and material (software and hardware) created and developed by different stakeholders (e.g. a company, an Internet website or a Member State) could be used in the frame of CSDP missions.

1 European framework of the security rules

As seen in section 4.3, the handling of information in field of security (thus CSDP missions and beyond) is an important topic, especially in times of constant security breaches, that should be considered in the design of a possible OCP platform. Data have to be handled according to the different types of classification. Depending on the level of classification that the future OCP will support, it will have to comply with the numerous regulations related with protection of EUCI that have been approved in the EU in the last few years.

The following table contains a summary of the last published:

DECISION of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service	Decision 2013/C 190/01	EEAS structure, including Union Delegations
COUNCIL DECISION 2013/488/EU of 31 March 2011 on the security rules for protecting EU classified information, and amended by COUNCIL DECISION 2014/233/EU of 14 April 2014	Council Decision 2013/488/EU	The council, the General Secretariat of the Council and Member States
COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information	Commission Decision 2015/444	Commission, including all departments and premises; Euratom

Table 5 - European framework of the security rules

The treatment of EUCI in the EEAS is thus governed by the *Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the security rules for the European External Action Service*, which entered into force on the 19 April 2013.

With the objective of being homogenous and applying equivalent security standards, the content of these regulations is very similar. Hereafter is presented a comparative summary of the most relevant articles:

Purpose, scope and definitions	Art. 1	Art. 1, Art. 2, APPENDIX A	Art. 1, Art. 2
Definition of EUCI, security classifications and markings	Art. 2	ANNEX A – 2	Art. 3
Classification management	Art. 3	Art. 3, ANNEX A – 3	Art. 4
Protection of classified information	Art. 4	Art. 5, ANNEX A – 4	Art. 5
Management of EUCI	Art. 9, ANNEX III	Art. 7, ANNEX A – 7, ANNEX A III	Chapter 4 (Articles 21 - 30)
Protection of EUCI handled in communication and information systems	Art. 10, ANNEX IV	ANNEX A – 8, ANNEX A IV	Chapter 5 (Articles 34 – 38)
Exchange of classified information with third States and international organizations	Art. 13, ANNEX VI	ANNEX A – 10, ANNEX A VI	Chapter 7 (Articles 51 - 57

Table 6 - Structure and organisations of the most relevant topics in the Council, the EC and the EEAS

Furthermore, specific agreements on security procedures for exchanging classified information between the EU and third states and international organisations have been signed (i.e. with Israel,[177] Ukraine,[178] etc.). A complete list of the existing agreements is accessible through the Treaties Office Database of the EEAS.[179]

The following table shows the most relevant legislation applicable at European Level:

DIRECTIVE 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DECISION of 8 December 2011	Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection
REGULATION (EC) 45/2001	REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

[177] Official Journal L 192, 24.7.2009, p.64
[178] Official Journal L 172, 05.7.2005 p.84 - 86
[179] http://ec.europa.eu/world/agreements/default.home.do

	of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
REGULATION (EU) 2016/679	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
DIRECTIVE (EU) 2016/680	DIRECTIVE (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Table 7 - Data policy European regulation

2 Licensing

Another peculiar topic in the design of a platform that is thought to support situational awareness is licensing. In order to integrate Situational Awareness products and capabilities in the OCP platform, the licensing is of a paramount importance as it regulates how the information (data) and material (software and hardware) created and developed by different stakeholders (e.g. a company, an Internet website or a Member State) could be used in the frame of CSDP missions.

Licenses focus on providing a framework in which it is known by all parts the terms of usage of the data, and in particular its commercial exploitation. Data is subject to a license that specifies the terms of use (the copyright) and that should be in line with the specifications of the Data Policy.

It is important to review few concepts related with copyright issues and licencing before advancing in the analysis of the EC regulation on Data Policy for licensing conditions. The following concepts (license, copyright, 'gratis' free, 'libre' free and public domain) will be briefly reviewed:

- **License**: License makes reference to the legal framework for usage of intellectual product. It is issued by the IPR owner of the given intellectual product and it is the

default use if no specific permission is provided. The license regulates the default copyright of an intellectual product.

- **Copyright**: "Copyright" literally means the right to copy but has come to mean that body of exclusive rights granted by law to copyright owners for protection of their work.[180] The copyright is inherent to the IPR owner, and comprehends all parameters of usage of an intellectual product. The copyright is regulated by the license.
- **'Gratis' free**. This term is used to indicate the difference between free of charge and free of use.[181] 'Gratis' free, or free of charge refers exclusively to the price of an intellectual product. It makes no reference to the usage allowed to users. Free of charge is a condition that can be (or not) specified in the license.
- '**Libre' free**. The term 'libre' is adopted from the various Romance languages and makes reference to a different meaning of the term 'free'. It refers to the usage allowed to the receipts of the license (the users). To clarify the difference between 'libre' free and 'gratis' free, this term is many times expressed as 'free and open', making a reference to the open-source term, which refers to computer science. A license compliant with a 'free and open' philosophy will allow the user to modify and re-use the product without specific permission of the issuer of the license.
- **Public Domain**. If an intellectual product fails to acquire any type of license, or the copyright validity period has expired, it falls under the category of public domain. A Public Domain product can be used by anyone in any way without prior permission of the originator because the work does not have an owner anymore.

Licenses cover many aspects of the usage of data by users. The following is a list of aspects that are usually covered by a license text:

Attribution	Licenses specify whether the IPR owner should be credited and, if so, in which way.
Intellectual Property Rights	The licenses specify the owner of the IPR, and to which extent this IPR is applicable to derivative products.
Usage	The default use that the user can perform with the data received. Normally the usage allowed is: - Without modification. The user can only take the data as it is and cannot create other products derived from that data. - With modifications. The user is allowed to create products derived from the licensed data.
Distribution	The default distribution the user of the licence can apply to this licensed data. - No Distribution. The user is not allowed to distribute data

[180] This definition is obtained from the U.S. Copyright Office at http://www.copyright.gov/help/faq/definitions.html (16 Jan 2014)
[181] Often known as the difference between Free as in Free Beer and Free as in Freedom.

	under the license outside its own organization. - Limited Distribution. The user can only share data inside a limited community. - Non Commercial Distribution. The user can freely share data as long as it is not for any commercial application. - Commercial Distribution. The user can freely share this data without any restrictions.
Licence Sharing	In case in which the license allows usage with modifications, or distribution to third parties (commercial or non-commercial), the license may specify what license is applicable to such distributed data.
Warranty/Liability	This the warranties on the data provided by the owner of the IPR that are applicable for as long as the license is respected. In very open licenses, allowing re-usability and re-distribution, it is common to find disclaimers of exemption of liability once the original data is altered or distributed.

Table 8 - Licenses aspects to be considered

In the frame of CSDP missions, there might be unlimited and unforeseen number of providers of information and each of them as managers of the IPR apply different licenses. For the purpose of CIVILEX, the potential provision of geospatial information has been studied.

A good practice that might be relevant for the purpose of the CSDP is the provision of satellite imagery funded by the European Commission and managed by the European Space Agency (ESA). In a hypothetical case in which this data would be distributed among EEAS staff, two different licenses shall apply:

- **ESA license on Sentinel data:** This is the license issued by ESA that applies to all the data obtained with Sentinel satellites. This earth observation missions, developed jointly by ESA and the European Commission have the objective of monitoring different aspects of Earth: Atmospheric, Oceanic and Land.[182] Its IPR is owned by the ESA and its Copernicus Programme.
- **ESA license on Contributing Missions** data: this is the license issued by ESA that applies to all satellite imagery acquired other that with Sentinel.

Further information on these two study cases for License and IPR is provided in the following sub-sections.

Copernicus Sentinel Data License

In this case, the IPR manager[183] established different levels of usage of the data provided:

[182] https://sentinel.esa.int/web/sentinel/home

[183] ESA is the manager of the IPR of Sentinel data by delegation, and the issuer of the license, although the

- Primary and Altered products: these are products which are presented as delivered, or which is original state can be reconstructed.
- Derivative Works: products that used Sentinel original products, but where the original data cannot be reconstructed.

With this in mind, this license applies the following:

Attribution	For both layers of products (Primary/Altered and Derivative), users of the license must acknowledge the source at all times.
Intellectual Property Rights	The licenses specify the owner of the IPR, which in the case of Primary/Altered products is the satellite owner. The IPR of derivative products belongs to the user of the license.
Usage	The user may use or alter product in any desired way. The user may take Primary/Altered products and transform them anyway they wish. That transformation may convert products into Derivative product, which has an effect in other aspects of the license.
Distribution	Users are allowed to: - Share with partners, with no restriction, any kind of product. - Publish and Distribute products. Publishing derivative products is done without restriction, but the publishing of Primary or Altered products shall not allow the downloading of copies that allow to reconstruct the original data unless recipients take note of the license.
Licence Sharing	The license sharing is different depending on the type of product. - Primary/Altered products can only be shared as long as the license is respected. This means that recipients of Primary/Altered product will need to agree with this license, and will not be able to alter it. - Derivative Products can be shared under any license appropriate as long as acknowledgement is provided via a copyright quotation.
Warranty/Liability	No liability is accepted by the issuer of the license regarding either Primary, Altered or Derivative products.

Table 9 - Sentinel data license

Copernicus Contribution Missions Data License

The CSC-DA ESA User License[184] applies to satellite imagery, but in this case to contributing

ultimate IPR relies on the owner of the system, which is the Copernicus Programme.

[184] https://spacedata.copernicus.eu/documents/12833/14545/CSCDA_ESA_User_License_version_23_March_2015.pdf

missions who are IPR owner of their own data. This license divides products as well in between Primary/Altered and Derivative. The license has the following characteristics:

Attribution	For both layers of products (Primary/Altered and Derivative), users of the license must acknowledge the source at all times
Intellectual Property Rights	The contributing mission providing the data is the owner of the IPR of all Primary/Altered products and these IPR are not inherited to the user of the license. Users of the license may claim IPR over value added product, which may be Derivative products, or processes to transform Primary into Altered products.
Usage	Users of the license may use Primary and Altered products to generate Value Added products (Derivative products, or processes). In order to achieve this, the users may copy products or distribute them with other users of the license. Any other use, such as distributing primary or altered products to the general public, or to users not signees of the license, is not authorized. Publication of primary and altered products is authorized provided that: - Attribution is respected. - Publication allows visualization, but not access to the data (Download). - The purpose of this publication is non-commercial.
Distribution	The distribution of products under this license (Primary and Altered) is only allowed under the signees of the license.
Licence Sharing	There is no license sharing since the distribution is not authorized. Value Added products where users of the license claim the IPR are not committed to use any particular type of license, except the one of attributing if derivative products are present.
Warranty/Liability	Although limited, there is a certain liability that can be addressed to the IPR owner (the correspondent contribution mission in any case) via the appropriate authorities (as governed by the law of the State in which the contributing mission has its office).

Table 10 - Copernicus contribution mission data license