European Journal for Security Research (2019) 4:51–71
https://doi.org/10.1007/s41125-018-00038-1

ORIGINAL ARTICLE

Situational Awareness, Information Exchange and Operational Control for Civilian EU Missions

Hans-Christian Schmitz[1] · **Matthias Deneckere**[2] · **Tommaso De Zan**[3] · **Wolfgang Gräther**[4]

Received: 12 September 2018 / Accepted: 18 December 2018 / Published online: 9 January 2019

Abstract

The European Union conducts a common security and defence policy (CSDP) that follows an integrated approach to external conflict and crisis. One means of the CSDP are external civilian missions, in some cases operating with military missions in the same operational environments. In order to better support the conduct of civilian missions, a Horizon 2020 project was awarded to propose design options for a "Situational Awareness, Information Exchange and Operational Control Platform", in short an "operational control platform" (OCP). The design of the OCP raises challenges that are relevant not only for European CSDP missions but also for crisis management operations in general, namely questions of situational awareness, interoperability, security and local versus remote operational control. The Civilex project has provided an overview of the actual state of operational control in CSDP missions, investigated current challenges, collected requirements for an OCP and, ultimately, proposed design options for a future platform with the goal to improve situational awareness, information exchange and operational control for CSDP missions. This paper presents the outcomes of the Civilex project.

Keywords Civilian crisis management · European Union common security and defence policy · Information systems · Interoperability · Operational control · Situational awareness

1 Introduction

The European Union (EU) and its member states play a significant role in global crisis management. Global crisis management is part of the EU's Common Security and Defence Policy (CSDP). The CSDP follows an integrated approach to external conflicts and crises, which has lately attempted to coordinate civilian, military

✉ Hans-Christian Schmitz
hans-christian.schmitz@fkie.fraunhofer.de

Extended author information available on the last page of the article

and Freedom, Security and Justice (FSJ) actors (Council of the EU 2018a). The EU external action is marked by a complex organisational structure, comprising both supranational components (such as trade or development aid, with the European Commission in the lead) and intergovernmental elements (such as the CSDP, where EU member states retain control). Consequently, CSDP is executed in a highly complex institutional environment, inhibiting a coherent use of different crisis response instruments at the disposal of the EU. Moreover, CSDP missions are deployed as ad hoc projects, with limited standardisation of tools and procedures, inadequate centralisation of deployable equipment and capabilities and minimal lessons learning from past missions. All of this has a negative impact on the effectiveness and efficiency of civilian CSDP missions and of broader EU crisis response more generally.

Civilian and military external missions are means of the CSDP to manage complex crisis outside EU borders. At the time of writing, (June 2018), the EU is conducting 17 missions in total, including eleven civilian and six military missions (EEAS 2018a), with 18 further missions which have been already completed in the past. The first civilian mission was launched in 2003,[1] and since then, CSDP missions have been an evolving endeavour. In 2016, the European Union Global Strategy for Foreign and Security Policy (EEAS 2016) and an Implementation Plan on Security and Defence (Council of the EU 2016b) were published. More recently, the Council of the EU adopted conclusions on the EU's integrated approach (Council of the EU 2018a) and on strengthening civilian CSDP (Council of the EU 2018b). Member states recently also adopted a civilian CSDP Compact, containing a number of commitments to strengthen capabilities for civilian CSDP missions (Council of the EU 2018c).

In these latest documents, the EU stated the intention to better support the execution of civilian CSDP missions by improving situational awareness, information exchange and operational control. Furthermore, it was stressed that the synergies between the different actors involved in global crisis management are to be enhanced. In order to do that, the Civilex project had been created as a Coordination and Support Action, funded by the EU's Horizon 2020 research and innovation programme[2] to envisage a future "Situational Awareness, Information Exchange and Operational Control Platform", in short an "Operational Control Platform" (OCP). An OCP is intended to meet existing challenges of CSDP missions, support ongoing crisis management practices and shape the conduct of future missions and operations. It involves technological components, as well as the establishment of standard procedures, guidelines and regulations.

[1] The first Civilian CSDP mission was the European Union Police Mission in Bosnia and Herzegovina (EUPM/BiH). Cf. EEAS (2012).

[2] The Civilex project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 700197. The Civilex consortium consisted of six partners, including the company Atos (Spain), the public research institutions Fraunhofer (Germany) and TNO (The Netherlands), the EU Agency SatCen (Spain) and the policy think-tanks ECDPM (The Netherlands) and IAI (Italy). The project had a runtime of 1 year and was concluded in 2016–2017. More information can be found on the Civilex-Website (Civilex 2017), where also the reports that have not been classified as confidential can be downloaded.

EU civilian missions operate in adverse, security-critical environments. Moreover, they have to cope with a challenging institutional landscape. An OCP is to be designed to better support missions in fulfilling their actual tasks, ensure the security of the mission staff and meet the EU's institutional requirements. An OCP would provide the tools to rapidly deploy a mission and conduct its core business from the very beginning.

The objectives of Civilex were, firstly, to take stock of the communication and information systems already in use within EU civilian missions; secondly, to record the stakeholders' requirements regarding a future OCP; thirdly, to give recommendations on the design and implementation of such a platform. To this end, the project consortium had to gain an overall understanding of the broader institutional context in which missions take place and their operational challenges. Civilex undertook multiple activities, including desk research, interviews, field visits and workshops. The consortium interviewed approx. 80 persons in total, including representatives of various EU institutions (among them EU missions like EUCAP Somalia and EULEX Kosovo) and staff members of the United Nations (UN). The interviews took place at EU facilities in Brussels, during field visits at offices of EUCAP Somalia[3] (in Nairobi, Mogadishu and Berbera) and at UN offices in New York. Moreover, case studies on various EU missions, both civilian and military, have been carried out. Civilex recommended three technical design options for an OCP, which fit into a growth model. The commissioning of respective prototype implementations is the aim of the follow-up project Civilnext (Civilnext 2018), which started in 2018 and is ongoing.

In the report at hand, we present a summary of the outcomes of the Civilex project. To give the reader a representation of the domain in which an OCP is to be deployed, we describe the institutional and operational context of EU civilian CSDP missions. Furthermore, we draw a distillation of the technological and operational requirements for an OCP and, finally, propose technological design options for IT-components of the platform.[4]

2 European External Missions and Operations

2.1 The European Union's Common Security and Defence Policy

The EU pursues a Common Security and Defence Policy (CSDP), which was originated for the task of crisis management, with both civilian and military means. The CSDP is conceptually and institutionally a "work in progress". It is under constant debate to which extent foreign and security policy is a national prerogative of the

[3] EUCAP Somalia has been launched in 2012 under the name "EUCAP Nestor". It has been renamed in 2016. A field scenario analysis on EUCAP Somalia has been published by Schmitz et al. (2017).

[4] We will cover issues of information security only superficially since information on such issues is to be considered classified. Nevertheless, such issues are undoubtedly of significant importance for the operation of a mission and, thus, the design of an OCP.

member states and to which extent it can be delegated to EU institutions. Under the current EU treaties, CSDP has been established as an intergovernmental pillar of the EU, with decision-making residing with the member states within the Council of the EU and requiring unanimous consent.[5]

Civilian crisis management covers "the entire range of non-military instruments which are called for in crisis situations—whether pre- or post-conflict" (Howorth 2014, p. 31). This includes humanitarian and rescue tasks, peacekeeping, conflict prevention and peace building, support to the rule of law and justice, and other tasks. To cope with these tasks, European external action follows an integrated approach and has recently tried to establish stronger ties between civilian and military CSDP as well as with European Commission actions in domains such as international cooperation and humanitarian aid and with Freedom, Security and Justice actors.

The main representations of the CSDP are civilian and military external missions. Missions are currently deployed in Africa, Eastern Europe, the Middle East and the Mediterranean Sea.[6] The EU separates civilian and military activities—a mission is either civilian or military, but not both. That is, for applying both civilian and military means in the same theatre of operations, more than one mission has to be deployed. This is the case, e.g. at the Horn of Africa, where two military missions (EU NAVFOR Atalanta and EUTM Somalia) and one civilian mission (EUCAP Somalia) are being conducted.

The institutional set-up of civilian crisis management within CSDP is as follows: decisions on CSDP are taken within the Council of the EU, comprising national representatives of all member states at the ministerial level. Missions under the CSDP can only be deployed upon unanimous decision of all member states. Within the Council of the EU, the Foreign Affairs Council (FAC), comprising the member states' foreign ministers, acts as the main strategic decision-making body for CSDP. Under the authority of the Council, the Committee of Permanent Representatives (COREPER II) and the Political and Security Committee (PSC) discuss and advise the Council on issues of crisis management operations. When it comes to civilian aspects of crisis management, the Political and Security Committee is supported by the Committee for Civilian Aspects of Crisis Management (CivCom), the civilian counterpart of the EU Military Committee (EUMC). The Working party of Foreign Relations Counsellors (RELEX) deals with legal and financial matters of CSDP missions (Fig. 1).

Civilian CSDP missions and some military operations are executed by the European External Action Service (EEAS). The EEAS has been designated as the EU's diplomatic service with approx. 4.000 staff members, both in Brussels and at the 140 delegations worldwide—EU delegations essentially are embassies of the EU. The EU currently also has eight EU Special Representatives who act as emissaries to promote EU policy in most difficult regions and coordinate various EU actions. The EEAS is headed by the High Representative of the Union for Foreign Affairs

[5] For overviews on EU CSDP, cf. Arnaud et al. (2017) (which is, in fact, a Civilex Project Deliverable) and Howorth (2014).

[6] For an overview cf. EEAS (2018a).

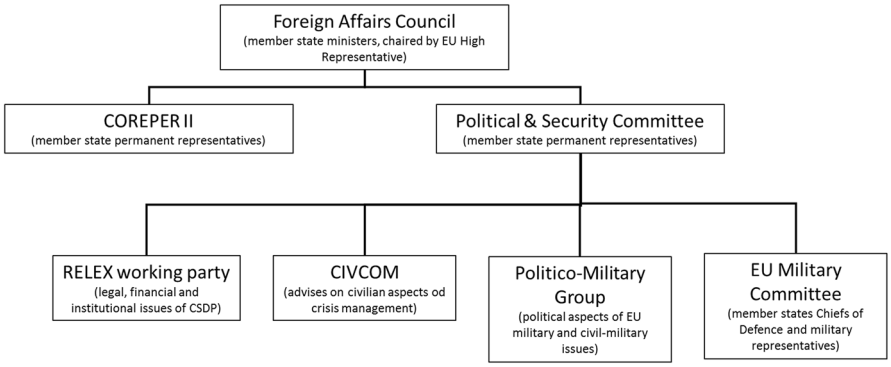

Fig. 1 Bodies of the Council of the EU

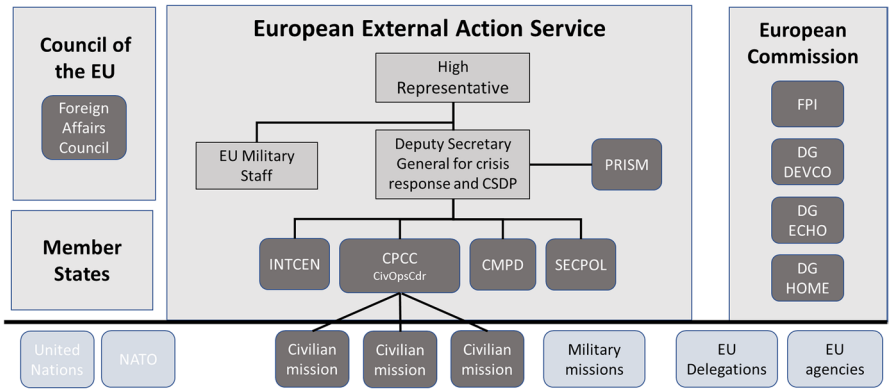

Fig. 2 Institutional set-up of the CSDP

and Security Policy who is also Vice-President of the European Commission and presides over the Foreign Affairs Council (Fig. 2).

Subordinate to the High Representative, the Deputy Secretary-General of the EEAS for CSDP and Crisis Response heads over the key civilian crisis response bodies at the EEAS:

- The Civilian Planning and Conduct Capability (CPCC) is the Brussels-based permanent headquarters for civilian missions, responsible for operational planning, command and control of civilian missions. It is led by the Civilian Operations Commander (CivOpsCdr) who acts under political control of the Political and Security Committee and under the overall authority of the High Representative. The CPCC maintains links to and coordinates with the EU Military Staff (EUMS), the EU member states, third states and international organisations.
- The Crisis Management and Planning Directorate (CMPD) is tasked with the strategic planning of CSDP missions and operations. Like the Civilian Planning

and Conduct Capability, it is under political control of the Political and Security Committee.

- The Security Policy Directorate (SECPOL) is responsible for policy-making in domains such as counter-terrorism, sanctions policy and disarmament, non-proliferation and arms export control.
- The EU Intelligence and Situation Centre Directorate (INTCEN) is the civilian intelligence capacity of the EEAS that provides intelligence analyses, situational overviews and early warning to the EEAS, CSDP missions and further EU institutions. It houses the EU Situation Room that serves as an information hub for EU Delegations, Special Representatives, missions and others. The Situation Room is closely linked to the EU's Watch-Keeping Capability (WKC), which monitors all missions, carries out information management and alerts the CSDP stakeholders in case of crisis. The WKC belongs to the EU Military Staff and is, thus, under a different chain of command than the Situation Room. Nevertheless, the INTCEN Situation Room and the WKC share information.
- The CSDPCR.PRISM Division (Common Security and Defence Policy, Conflict Resolution—Prevention of conflicts, Rule of law/Security Sector Reform, Integrated approach, Stabilisation and Mediation), commonly referred to as PRISM, was created to drive the implementation of the EU's integrated approach to conflict. PRISM is responsible for policy development related to CSDP and crisis response, the development of early warning systems, internal coordination, support to mediation activities and support to country teams, e.g. on promoting conflict sensitivity.

Within the EU's institutional organisation, the EEAS is not mandated to manage any operational funding deriving from the EU budget, which is an exclusive competency of the European Commission (EC). Therefore, the Service for Foreign Policy Instruments (FPI) has been set up as part of the Commission—but physically located within EEAS premises—to support and control civilian missions regarding their financial and budgetary matters, and also check procurement processes. It represents the European Commission within the Committee for Civilian Aspects of Crisis Management (CivCom) and the RELEX working party.

The European Commission is also responsible for various other external action policy domains relevant for crisis response, such as development aid, humanitarian relief and home affairs. These domains are not part of the CSDP but instead belong to the supranational pillar of EU decision-making. This implies that the European Commission can initiate activities in these domains using the EU budget, with a more limited role for the member states. Within the European Commission, these policy domains are implemented by various Directorates-General (DGs), in particular the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO), which operates field offices in 40 countries, 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). Directorates-General often work side-by-side with CSDP missions in the field and exchange information, albeit often not in a systematic way.

Finally, a set of civilian EU agencies collaborate with CSDP missions and crisis management operations, often on matters where internal and external security dimensions meet. To these agencies belong the EU's law enforcement agency EUROPOL, the European Border and Coast Guard Agency FRONTEX, the European Asylum Support Office EASO, the EU's Judicial Cooperation Unit EUROJUST and the EU's Satellite Centre. As we also take military matters into consideration, the European Defence Agency is an important stakeholder, too.

To sum up, the CSDP is an element of a broader EU external action domain that comprises various instruments and acts within a complex institutional environment. Linking up the various EU external action actors is a challenge as they belong to different EU institutions, obey different chains of command, receive their funds from different lines of the EU's budget and, to some extent, pursue different objectives. In light of the EU's ambition to implement an integrated approach to external conflict and crisis, this poses particular challenges for coordination and the formulation of more holistic responses.

2.2 European Civilian CSDP Missions

The EEAS Crisis Response System is activated when there is a crisis outside EU borders. A part of the Crisis Response System is a platform that is intended to give guidance on crisis management. The platform includes members of EEAS departments, the EU Military Staff, the EU Military Committee and relevant Commission services. If a CSDP mission appears to be an appropriate response, then member states in the Political and Security Committee (PSC) can invite the High Representative to outline a Crisis Management Concept, which describes the options, the design, the risks and a possible exit strategy for a mission. This concept is drafted by the Crisis Management and Planning Directorate (CMPD). The PSC debates on the concept, sends it with further options to the Committee of Permanent Representatives (COREPER II), which finds a consensus, still to be confirmed by the Foreign Affairs Council (FAC). The PSC, supported by Committee for Civilian Aspects of Crisis Management (CivCom) and the EEAS, in particular the Civilian Planning and Conduct Capability (CPCC), works out further strategic options and sends these to COREPER/FAC, which decide on a Joint Action and instruct the PSC to work out a Concept of Operations (CONOPS), again with substantial support by CivCom and the CPCC. The CONOPS has to be approved by COREPER/FAC, before an Operational Plan (OPLAN) is drafted by CPCC with the support of the future Head of Mission. The OPLAN is handed over via the PSC to COREPER/FAC. As soon as it is approved, the mission can be launched. While the OPLAN is still under consideration by COREPER/FAC, the member states can already start the process of force generation for the mission.

The planning and launch of a civilian mission is, thus, a complex, iterative process that involves Council services, EEAS services and member states. Via the Council, the member states preside over missions. They also decide on the financing of missions and furthermore contribute by force generation, i.e. seconding of mission staff.

Missions are temporary undertakings, they are not intended to run permanently. They are set up as legal personalities with their own budget. From a legal perspective, therefore, they are not part of the permanently established EEAS, even though they are steered by the EEAS via the Civilian Planning and Conduct Capability (CPCC). The Civilian Operations Commander (CivOpsCdr), who is director of the CPCC, exercises command and control of civilian missions at the strategic level. The CivOpsCdr is under political control of the Political and Security Committee (PSC) and reports to the Foreign Affairs Council via the High Representative. Command and control in theatre is exercised by a dedicated Head of Mission, who reports to the CivOpsCdr and the PSC.

Missions are separated from the EEAS' administrative system as their budget is managed by the European Commission via its Service for Foreign Policy Instruments. The missions' communication and information systems are also largely detached from the EEAS. Therefore, when initiated and deployed, missions have to set up their own information system architecture from scratch. This particular problem is to be addressed by the deployment of an Operational Control Platform (OCP) for *all* missions.

Heads of Missions are based in their respective mission headquarters—in the exemplary case of EUCAP Somalia, the mission headquarters is situated in Mogadishu. They are responsible for day-to-day management and coordination, and lead their operational staff in the headquarters, field offices and, possibly, a back office. EUCAP Somalia, by example, runs field offices in Hargeisa and Garowe, and a back office in Nairobi/Kenya.

Civilian missions are usually established in theatres of operations where the EU is already active by other means. Referring to Somalia again, an EU Delegation to Somalia was established in 1993, which was later complemented by the nomination of a Special Representative for the Horn of Africa in 2012. In addition, two military missions, namely EU NAVFOR Atalanta and EUTM Somalia, are active in the region since 2008 and 2010, respectively. It is in this complex institutional context that the civilian mission EUCAP Somalia was launched in 2012. Civilian missions have to interoperate with EU partners in the field, and they also have to interoperate with third parties that do not belong to EU institutions, but play a significant role in the theatre of operations. These are institutions of the respective host state, the EU member states or international organisations. In Somalia, e.g. various UN organisations, NATO and the African Union Mission in Somalia (AMISOM), are engaged, among other actors (cf. Schmitz et al. 2017).

3 Lessons Learnt from the Civilex Project

An Operational Control Platform (OCP) was envisaged to better support missions regarding information management and exchange, situational awareness and overall operational control in the complex institutional and operational environments in which civilian CSDP missions find themselves. An OCP is to support civilian missions during their entire life cycles, from planning to phasing-out. It shall close collaboration gaps and improve business continuity and lessons learning. The range

of tasks to be supported by the OCP is broad, covering mission-internal coordination, exchange with EU institutions at the Brussels level and interoperation with other partners, both EU and non-EU. The development and installation of an OCP is therefore a comprehensive endeavour that demands changes on the technical and the operational level, and takes into account the institutional environment and dynamics of EU external action.

3.1 Information Management in Civilian CSDP Missions

We conducted interviews with representatives of the EU institutions involved in launching, running and controlling civilian CSDP missions, as well as with mission staff deployed in the field. It turned out, that, in essence, an OCP could support missions in four areas, namely

(1) horizontal information exchange and internal working processes,
(2) vertical information exchange and procedures with Brussels,
(3) collaboration with other partners and
(4) security.

Ad (1), the OCP shall support missions-internal organisation and coordination, including overall situational awareness and management of the local security situation. Ad (2), the exchange with the institutions located in Brussels is perceived to be burdensome. This is especially true for processes involving the Service for Foreign Policy Instruments (FPI). FPI applies EU regulations that are difficult to implement in the operational environments of the missions (cf. Arnaud et al. 2017). Therefore, complex administrative procedures—regarding human resources, procurement and finances, among other task areas—have to be adapted to the field situations. Ad (3), relations between CSDP missions and other partners have been described as very positive. However, exchange takes place nearly exclusively on a personal basis; technical interoperability of the various information systems in use is only partial. Information exchange with the military is often hampered due to different practices of information classification. Ad (4), an OCP is expected to significantly contribute to both mission and information security by defining standard procedures, technically and organisationally enabling varying levels of security, providing transparent and unobtrusive security measures and, consequently, helping to create a security culture within the overall management of unclassified information in crisis management. It is the aim to define and implement an effective security framework that in day-to-day practice requires as little "practical illegality" ("brauchbare Illegalität", Luhmann 1999) as possible.

As a result of the institutional set-up of external missions, the EEAS does not traditionally equip missions with IT systems, but the missions have to acquire their equipment through their own budget and design their communication and information systems architecture from scratch. While some steps are currently being taken to develop or purchase systems available to all missions (e.g. a decision was recently taken to set up a warehouse for rapid deployment of equipment and assets of civilian

CSDP missions, see European Commission 2018), the overall picture remains fragmented. There is neither an integrated system available for financial management, human resources management and field security, nor is there a comprehensive set of Standard Operational Procedures (SOP) for administration, command and control. An OCP should ideally change the situation, as it will make systems/services and SOPs available to missions right at their onset. Instead of designing their systems from scratch, missions shall access and adapt systems and services from a given OCP.

At present, the software used by missions is very simple compared to the complexity of the missions' tasks—in the project, we observed a heavy reliance on email and standard office software for data storage and processing. Since all missions design their own systems architectures, only little uniformity across missions is given. Missions would need:

- Enterprise Application Systems (EAS) for mission support and administration,
- basic support for cooperative work,
- standardised data bases for operational information and intelligence,
- Standard Operational Procedures (SOP) for archiving and business continuity, and
- Geographical Information Systems (GIS) for displaying security-related information in their theatre of operations.

Some of these systems—like EAS—can be commercial off-the-shelf products, while others will have to be specifically developed. Geographical Information Systems (GIS) for situational awareness are to fulfil the purpose that Command and Control Information Systems (C2IS) fulfil in the military domain: providing a situational overview by displaying symbols on maps. These symbols represent relevant objects in the theatre of operations, concrete objects such as camps or groups of people, and abstracts objects such as control measures like organisational boundaries, and events. Civilian GIS support field security. They are expected to function similarly to military C2IS—even the sets of symbols to be displayed will most probably overlap to a large extent. Therefore, the development of respective OCP components can rely on respective pre-work from the military domain.

A fundamental concern is to improve knowledge management and provide respective tool support: firstly, information has to be distilled and linked in order to create a comprehensive overview on all topics related to the mission. Secondly, information has to be exchanged with others, especially other EU institutions. To this end, missions must be given access to information providers and they must themselves contribute information and knowledge to others, even after the closure of a mission. An important goal is to create a Common Information Domain for military and civilian missions.[7] Another requirement is to ensure the compatibility with intelligence platforms like the Watch-Keeping Capability.

[7] Cf. the concept of a Shared Information Space described by Angelstorf et al. (2017).

Given the multitude of components needed, an OCP should rather be a framework than a stand-alone system. It should consist of specialised services and systems, enterprise architectures, Standard Operational Procedures and templates. It must be flexible enough to support a variety of actors and tasks. To this end, it must support different user roles and task-specific user interfaces that also enable mobile access to information and processes. While the OCP's services are to be diversified in that respect, the unity of the platform is to be ensured by a common user experience that allows users to take on different roles and tasks easily.

Missions must be able to self-regulate and act autonomously in the field, even without a stable connection to the headquarters and institutions in Brussels.[8] Nevertheless, some services—administrative as well as intelligence services—can be centralised and provided from Brussels. To this end, it has been decided to set up a Mission Support Platform (MSP) at the Brussels level "aimed at improving the management, rapid deployment and efficient conduct of civilian crisis management missions" (Council of the European Union 2016a). The MSP, housed within the Civilian Planning and Conduct Capability (CPCC), is intended to be a Shared Service Centre that helps to improve in particular the vertical information exchange with the EEAS and the Service for Foreign Policy Instruments.

It seems as if autonomy of missions and the ability to self-regulate are in conflict with the high-level requirement of standardisation: standardisation leads to a greater harmonisation of administrative procedures which would be beneficiary for all missions. It would also help implement a comprehensive security concept. Last but not least, an OCP must provide standard services that are available right at the beginning of a mission. Therefore, standardisation is a key requirement. However, missions must still be able to adapt to their actual situations and tasks. They must not be constrained by standards that are introduced by an OCP without taking the local situations into account. Also, it has to be considered that EU policy is in constant flux and that, therefore, all solutions must be adaptable to be sustainable.

To take stock: the current IT infrastructure of CSDP missions is very simple, consisting to a large extent of standard office software plus some tailored services. To cope with the broad range of tasks to be fulfilled, missions require specialised services for internal mission management, security assurance, coordination with the Brussels level, and interoperation with EU and non-EU partners. It is rather inefficient to provide these services by one single, stand-alone system. Instead, an entire portfolio of systems and services is needed that supports a mission from its very beginning. The portfolio can be extended step-by-step and on demand, addressing individual tasks and roles related to the missions. The systems and services are to be provided by the EEAS. Some of them can be operated remotely from Brussels; others will have to be deployed locally, on the mission level.

[8] The question of remote versus local control and execution of operations is being extensively discussed. Security requirements foster a tendency towards withdrawing services from their immediate application area, while the effectiveness of operations demands a local involvement. Cf. among others, Duffied (2012), Sandstrom (2014) and, regarding the use of humanitarian technologies, Kalkman (2018).

Despite the many challenges in relation to information management in the context of civilian CSDP, it is important to note that a number of steps have recently already been taken to provide more harmonised tools available to missions, among them the establishment of the Mission Support Platform and the creation of a warehouse for equipment and assets. For the development of the OCP, it is essential to take into account such developments, to avoid overlap between the supported processes and ensure complementarity.

3.2 Lessons Learnt from the UN

While for the EU CSDP is a relatively new field of activity, the United Nations (UN) has a long history and a wide range of experience regarding the execution of operations, which belong to the core of its mandate. At the time of writing this paper, the UN has completed 57 peacekeeping operations (PKOs), and 14 additional PKOs are running (UN 2018). PKOs often combine civilian and military activities. While the EU separates civilian from military structures, the UN creates a single chain of command with a civilian Special Representative of the Secretary-General acting as head of operations and operational control being executed under the Special Representative by a military force commander and a police commissioner.

To elicit lessons learnt from the UN, the Civilex consortium conducted interviews with members of the UN's peace and security departments, as there are the Department of Peacekeeping Operations (DPKO), the Department of Field Support (DFS) and the Department of Political Affairs (DPA). In addition, interviews were conducted with staff from the Office for the Coordination of Humanitarian Affairs (OCHA), which is tasked with enabling and coordinating UN humanitarian response to complex emergencies and natural disasters.

UN peacekeeping operations and EU civilian missions face similar challenges regarding information management and exchange. Both have to deal with critical business continuity and information security demands while being situated in adverse and multi-lingual environments, depending on external actors and having to cope with a multitude of systems, among them legacy systems and mission-specific systems. UN organisations use information systems during all phases of an operation in order to increase the effectiveness and efficiency of task processing, in particular the processing of routine tasks. In doing so, the UN has to solve problems in day-to-day communication and information handling quite like the EU: information fragmentation, loss and deficits; the full potential of automation not being exploited; need for better contribution to intelligence tasks for improving situational awareness.

The UN has made the experience that the improvement of information management and exchange is not a singular activity but must be implemented as a continuous process. It demands the management of policies, procedures and services. Information management therefore includes IT-Service management but goes beyond. A portfolio of procedures and services, including their documentations, has to be established and maintained. It is reasonable to follow best practices and align to international standards. A continuous improvement process must be anchored at the strategic level and made a clear and strong priority.

Effective use of services will not be possible without extensive training and campaigning. Within staff, an attitude of knowledge and information sharing has to be developed, and the organisation itself has to be geared towards an information-centric organisation: "An information-centric organization is concerned with the efficient and accurate use of information. This involves understanding where information is stored, where the workload (processing) is running and how information is synchronized between these activities". (Chessel 2012) Usability as a precondition of use is fostered by the promotion of user-centred design. To this end, the UN has specified its own design principles (Principles for Digital Development 2018).[9]

Insights from the EU interviews were confirmed by members of the UN: processes and services should be standardised as far as possible, in particular for routine tasks. Standardisation is also a precondition for effective knowledge management, and it certainly contributes to security management. However, standardisation must leave room for adaption to the field situation.

3.3 Interoperability Requirements

Within the theatre of operations, civilian EU missions have to cooperate with civilian and military partners. In order to effectively cooperate, the partners have to be interoperable, that is, they have to be able to exchange information with well-defined semantics and to align their activities. Operational interoperability of partners does not necessarily presuppose technical interoperability of information systems—there are situations in which interoperability can be achieved by telephone, email or liaison officers alone.[10] However, as soon as there is a high volume of information to be exchanged or information is complex or information has to be exchanged with high velocity, technical interoperability between information systems becomes increasingly important. Moreover, the exchange of complex information as structured data supports the automation of tasks and thus adds significant value to the mission processes of the individual partners. Therefore, technical interoperability is an enabler of operational interoperability; it significantly contributes to collaboration in complex environments.

The most straightforward way to achieve technical interoperability seems to be the harmonisation of information systems in use: ideally, all partners would use the same type of system. This, however, is not achievable: firstly, partners—even within the EU institutions—have to fulfil very different tasks. These tasks require specialised systems, and it is not the case that one and the same system can equally well support all given tasks. Secondly, some of the partners are already equipped with information systems. It will not be possible to convince all partners to procure the same, new system. Even if a set of partners used the same type of system, issues would arise if they did not deploy the same versions or did not update their systems in a coordinated fashion. This makes interoperability by harmonisation even less

[9] Cf. also ISO (2010).

[10] For the relation of operational and technical interoperability and the distinction of different levels of interoperability cf. Schade and Dürr (2005a, b).

feasible. Therefore, missions and their partners will have to deal with a multitude of information systems, including legacy systems, and they will have to define interoperability solutions for heterogeneous systems.

In principle, an interoperability solution consists of operational experts, information systems and information to be exchanged: operational experts of all partners must be equipped with information systems that include both local processing services and exchange services. Via the exchange services, they send and receive messages. The definition of information formats and exchange mechanisms must rest on Information Exchange Requirements (IERs). This means that the development of an interoperability solution demands that all partners are equipped with suitable information systems, and that there are defined IERs. Civilex's fieldwork found out that both preconditions are often not met: neither are all actors equipped with suitable information systems, nor are staff members always able to express their needs by IERs. They must be provided with respective support so that expressions of interoperability needs can be turned into proper solutions.

It is thus a desideratum to develop light-weight information systems that can be easily deployed by partners who are not yet equipped with suitable systems. Such systems can be part of the OCP portfolio, and they can be used in missions, e.g. for situational awareness. They can also be provided to cooperation partners (Meyer et al. 2017).

Interoperability is a major issue in the military domain. Civilian missions and systems can benefit from respective groundwork. Various means—processes, tools, reference frameworks—for designing and implementing interoperability solutions already exist and can be exploited for interoperability in civilian crisis management. However, the core of an interoperability framework should be a reference model that defines the semantics of information, assures the mutual understanding of partners and guides the implementation of solutions for needed capabilities. In the military domain, such information models have been defined (most notably the MIP Information Model, MIM 2018). It is a desideratum to create a comprehensive information model for civilian crisis management.[11]

4 Technological Challenges and Opportunities for Improving Information Management and Situational Awareness

Following the work presented in the previous chapters, an OCP is to support information and knowledge management for the different actors involved in CSDP civilian missions. In addition, there are high-level topics of standardisation and interoperability that have to be considered. To meet these demands, we developed an

[11] There are initiatives addressing the problem, like the establishment of the Centre for Humanitarian Data by UN OCHA in 2017 (UN OCHA 2018). However, current products (like the Humanitarian Exchange Language, HLX 2018) are not sufficient to serve the interoperability requirements of civilian crisis management.

OCP design framework that includes three technical design options, which fit into a growth model.

As mentioned above, the EEAS has a staff of approx. 4.000 persons. According to the EEAS (2018b), civilian missions have an additional staff of roughly 2.000, including local staff. The mission members will immediately profit from an OCP in everyday work. In addition, the OCP will facilitate the work of other departments and agencies, like the Service for Foreign Policy Instruments (FPI).

The introduction of an OCP will necessarily raise the demand of training. By implementing a growth model and, thus, introducing the OCP in a stepwise manner, the training effort can be managed. The OCP is intended to cope with various important trends that are increasingly adopted in the workplace, ranging from social networks via Wikis to blogs or microblogs, as well as easy-to-use interfaces for multiple devices, among them desktop computers, tablets and smart phones. Uptake of such trends in an OCP will raise user acceptance, and it will reduce training efforts and increase efficiency of work processes.

There are concerns and conflicting demands related to an OCP. For example, from a user's perspective data and privacy protection are crucial and have to be balanced with the information needs for desired features, such as support of situational awareness by including location information of people. From a system's perspective, a good balance between centralisation of the platform and distributed resources (storage, computation, network connectivity, etc.) is required. In addition, the ICT security framework should be designed to be effective and efficient, yet not affect the usability of the OCP.

When new ICT systems are introduced into the workplace, the user acceptance and user participation is of paramount importance. User interfaces that are easy to use and have a well-designed user interaction help to attract users (cf. Blythe and Monk 2018). Furthermore, the user interface and user interaction must consider the diversity of prospective users that have different work cultures as well as professional and educational backgrounds. Effects of this diversity could be alleviated by involvement of users in the design process of an OCP. This, however, is a challenge since mission members, including local staff, come from various countries and have different backgrounds regarding competences and working cultures.

The growth model consists of three options that are intended to build on each other:

1. When we examined ICT usage in the context of CSDP civilian missions, we found out that email is prevalent in all aspects of information exchange, be that horizontally or vertically. In addition, we revealed that the current ICT landscape does not offer tools for efficient team collaboration in the context of CSDP civilian missions. These findings led to the development of the first technical option referred to as "Information sharing and collaborative information management".

   The first option complements and connects to the currently used systems and provides services for better information exchange that lead to improved work processes for all actors in the field, in missions, in Brussels or in other EU entities. It is a first step to overcome the fragmentation of the current ICT landscape and achieve a new streamlined experience for all users.

The option is characterised by

- collaboration: flexible shared workspaces, called "team spaces";
- user interaction: web portal; user registration, access control, single sign-on; responsive design for good usability on mobile devices;
- access point to services and systems: connection with external services;
- security: simple means for encryption and decryption of multimedia documents.

Team spaces are the core module of the first technical option. They support collaborative information management for flexible teams and should significantly reduce information exchange by email. A team space is only accessibly through its members and consists of a shared information space for multimedia documents as well as a set of common tools such as wikis or microblogs for information management. The access rights for the information in team spaces should be based on roles that define which actions could be performed. Roles are assigned to persons, and we suggest predefining a few roles such as manager, member and restricted member. However, the component for membership management should allow the further definition of specialised roles such as reader or information provider as well as temporary member.

From a technical point of view, team spaces are containers for information and tools. Shared information spaces are augmented by tools such a wiki, blog, microblog, calendar and decryption/encryption systems. It must be possible to structure team spaces just like nested folder hierarchies. On each level of the hierarchy, it must be possible to invite further members. These additional members would only have access to information in that subtree of the hierarchy. The concept promises to be especially useful for collaboration with external co-workers.

2. On the Brussels level, we recognised different web platforms, an E-Learning tool and Wiki systems to share guidelines, instructions or standard operation procedures. Their usage results in the creation of information silos where the information is scattered across different actors and systems. The insight into this effect led to the development of the second technical option referred to as "Information integration".

   The second option is to extend the first technical option by services for information integration. It enables integration of information from heterogeneous sources, in particular application systems of CSDP missions. The integrated information is required by the European External Action Service (EEAS) in order to efficiently run routine control processes. It would be beneficial to missions, as it avoids duplication of work. It enables access to relevant information across missions and could support the semi-automatic creation of reports. In the short term, it will improve control processes.

   The second option is characterised by

   - interaction of the OCP with external systems: system-to-system integration, standardised and self-describing interfaces, interoperability;

- caching strategy;
- special access restrictions for personal data;
- user interaction with the OCP: web portal as in first option, unified look and feel; merged information.

3. Currently, there is little IT tool support for analysis and presentation of dynamic data and information such as location of personnel, status of mobile assets or information about the overall political situation. Such information combined in a common operational picture is necessary not only for day-to-day business but also to cope with crisis and emergency situations. This finding led to the development of the third technical option referred to as "Decision and analysis support".

   The third option complements the first and the second technical option by services for situational awareness and operation control. It focuses mainly on decision and analysis support. More dynamic data sources than the static sources in the first two options are included, such as data and information about personnel, mobile assets and about the overall political situation. With the third option, the OCP supports situational awareness by offering continuous updates on observed events in shared visualisations. The third option is especially useful when mission personnel enters high-risk regions or for evacuation planning and it is helpful in crisis and emergency situations, e.g. In the short term, the services introduced by the third option can provide actionable information for decision makers on demand.

   The third option is characterised by

   - location data and sensor data: dynamics of information;
   - information extraction;
   - interaction of the OCP with external systems: alignment of representation and semantics;
   - user interaction with the OCP: web portal as in first two options, decision and analysis support; rich visualisations.

   The proposed options of the OCP framework consist of several modules and systems, which are flexible to support the different actors involved in CSDP civilian missions. The OCP would support different roles as well as task-specific user interfaces and enable access to information and processes with various devices. The unity of the platform would be ensured by a common user experience.

   The prospective OCP enables fast and direct information exchange between missions and more effective sharing of knowledge on best practices. For example, the OCP can provide interoperability solutions for specific capabilities or offer means to tailor team spaces according to the co-workers needs. The latter feature could help reducing time and effort of HR activities, when mission staff changes.

   The deployment of OCP services enables new ways of working and conducting a mission. Yet, instead of presupposing operational change, it already supports mission staff in their current way of working. The introduction of an OCP *enables* operational and even organisational change without *enforcing* it. People, not technology, have the final say in conducting a mission.

The OCP as outlined will add value to the operational effectiveness of civilian CSPD missions as it would help CSDP structures and staff access information within the EEAS and beyond. This is important, not only during the implementation of the mission, but also during its phasing-in and phasing-out, as it will accelerate the achievement of initial operational capability, while also feeding into wider EU external action decision-making and practice. Moreover, the use and effectiveness of the OCP raises questions with regard to the institutional ownership of the platform, especially regarding who would activate and manage the OCP, and whether this should happen centrally or rather in a decentralised way. Civilex research recommended to institutionally anchor the OCP under the responsibility of the Civilian Operations Commander, who is well placed to provide rules and guidance for all civilian CSDP missions. The creation of mission branches within the OCP could further allow for mission-internal information exchange management, including customised services, under the management and control of the Heads of Mission, thus providing a balance between centralisation and tailoring to specific mission needs (Arnaud et al. 2017).

It is now the task of the Civilnext project (Civilnext 2018) to commission prototypes for the OCP following the design options. In the course of refining the design solutions and implementing prototypes, concepts of deployment and operations are to be detailed and questions regarding the costs and effort—infrastructure, personnel, etc.—associated with the platform have to be answered.

5 Conclusions

To sum up, in order to better support the execution of civilian CSDP missions, the EU has decided to develop a "Situational Awareness, Information Exchange and Operational Control Platform", namely an "Operational Control Platform" (OCP). The platform should be designed to facilitate ongoing crisis management as well as future missions and operations, which are currently characterised by the use of fragmented, unharmonised and not sufficently efficient information systems. The OCP is to support the EU CSDP and its Global Strategy more broadly and, thus, to enable interaction between various both EU and non-EU actors.

The Civilex project has investigated with strong user participation the institutional and operational context in which the OCP is to be deployed and has elicited key requirements. Based thereupon, it has proposed three technological design options:

- The first option focusses on enabling "Information sharing and collaborative information management". It promotes the concept of "team spaces" as containers for information and tools which support collaborative information management for specific groups ("teams"). It can thereby support information exchange within the mission (horizontal), with institutions in Brussels (vertical) and with external partners.
- The second option extends the first option by services for "Information integration". The aim is to integrate various systems and information sources, stream-

line operations and operational control, and improve in particular vertical information exchange with EU institutions in Brussels. The integration of information from various systems and sources leads to a uniform operational picture and, in consequence, better situational awareness.

- The third option extends the second by services for "Decision and analysis support". Such services are to provide distillations of information from various sources and a coherent overview on the overall situation (static) as well as the course of actions and events (dynamic). Ultimately, services for decision support are meant to further improve operational control.

All three design options are to come with a comprehensive security concept.

An OCP will not be a monolithic solution but rather a portfolio of systems, services, procedures and guidelines. The design of an OCP is therefore not a purely technological endeavour. Keeping in mind that the institutional architecture and processes within the EU are complex and subject to political decision, the OCP has to enable operational change, but without enforcing it.

The development of the OCP should take into account other initiatives currently being put in place, especially in the context of the Mission Support Platform, to ensure complementarity. Moreover, it could refer to related endeavours, like UN initiatives and NATO Federated Mission Networking (NATO 2018). In return, the OCP development will be significant for other crisis management organisations, firstly, because the EU is an important actor and cooperation partner in the field, and, secondly, because issues of standardisation versus context-specificity and remote versus local management, among other issues, arise for others in almost the same manner. The various actors face similar challenges. Therefore, to a large extent, lessons learnt will be universally valid.

Acknowledgements We would like to thank all members of the Civilex project team. We also gratefully acknowledge the insights from our interviewees in Brussels. In addition, we thank the people we talked to during our field visits and the people participating in our workshops.

References

Angelstorf F, Apelt S, Bau N, Jansen N, Käthner S (2017) Shared information space. A solution for a global information grid. In: International Conference on Military Communications and Information Systems (ICMCIS), IEEExplore, Oulu

Arnaud Y, Barbieri C, Deneckere M, De Zan T, Flessenkemper T (2017) Analysis of CSDP institutional and policy aspects. http://www.civilex.eu/content/analysis-csdp-institutional-and-policy-aspects. Accessed on 27 June 2018

Blythe M, Monk A (eds) (2018) Funology 2: from usability to enjoyment. Springer, Heidelberg

Chessel M (2012) Information centric organisation. IBM developerWorks Wiki. https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W4108ee665aa0_4201_8931_923a96c3653a/page/InformationCentricOrganization. Accessed on 11 June 2018

Civilex (2017) Civilex-website. http://civilex.eu/. Accessed on 27 June 2018

Civilnext (2018) Civilnext-website. https://www.civilnext.eu/. Accessed on 22 Nov 2018

Council of the European Union (2016a) Council conclusions on the mission support platform. http://www.consilium.europa.eu/en/press/press-releases/2016/04/18/fac-mission-support/. Accessed on 11 June 2018

Council of the European Union (2016b) Implementation plan on security and defence. 14392/16, Brussels. https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf. Accessed on 11 June 2018

Council of the European Union (2018a) Council conclusions on the integrated approach to external conflicts and crises. https://ec.europa.eu/europeaid/sites/devco/files/2018-01-cnl_conclusions_on_ia.pdf. Accessed 11 June 2018
Council of the European Union (2018b) Council conclusions on strengthening civilian CSDP. http://www.consilium.europa.eu//media/35380/st09288-en18.pdf. Accessed on 11 June 2018
Council of the European Union (2018c) Conclusions of the council and of the representatives of the governments of the member states, meeting within the council, on the establishment of a civilian CSDP compact. https://www.consilium.europa.eu/media/37027/st14305-en18.pdf. Accessed on 20 Nov 2018
Duffied M (2012) Challenging environments: danger, resilience and the aid industry. Secur Dialogue 43(4). http://data.consilium.europa.eu/doc/document/ST-5413-2018-INIT/en/pdf. Accessed on 11 June 2018
EEAS (2012) Fact sheet on the European Police Mission in Bosnia and Herzegovina (EUPM). https://eeas.europa.eu/archives/csdp/missions-and-operations/eupm-bih/pdf/25062012_factsheet_eupm-bih_en.pdf. Accessed on 11 June 2018
EEAS (2016) Shared vision, common action: a stronger Europe. A global strategy for the European Union's foreign and security policy. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf. Accessed on 11 June 2018
EEAS (2018a) EU in the world. https://eeas.europa.eu/headquarters/headquarters-homepage/area/geo_en. Accessed on 11 June 2018
EEAS (2018b) Strengthening the civilian side the EU's common security and defence policy (CSDP). https://cdn4-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/a1BWaHLkkIzu7LTEeWHxArWV3NugGr896Rb6wwfUjo4/mtime:1542655676/sites/eeas/files/strengthening_the_civilian_side_of_the_eu.pdf. Accessed on 20 Nov 2018
European Commission (2018) Equipping our deployed experts—a warehouse for the civilian CSDP missions. https://eeas.europa.eu/csdp-missions-operations/eubam-libya/45729/equipping-our-deployed-experts-warehouse-civilian-csdp-missions_en. Accessed on 23 Nov 2018
Howorth J (2014) Security and defence policy in the European Union. Palgrave, London
HXL (2018) Humanitarian exchange language website. http://hxlstandard.org/. Accessed on 11 June 2018
ISO (2010) ISO 9421-210. Ergonomics of human–system interaction—part 2010: human-centred design for interactive systems. https://www.iso.org/standard/52075.html. Accessed on 11 June 2018
Kalkman JP (2018) Practices and consequences of using humanitarian technologies in volatile aid settings. J Int Humanit Action 3:1
Luhmann N (1999) Funktionen und Folgen formaler Organisationen, 5th edn. Schriftenreihe der Hochschule Speyer, Speyer
Meyer O, Schmitz H-C, Bau N, Bulach C, Gallesio F, Gerz M (2017) MIP solutions for civil-military cooperation. In: Proceedings of the 22nd International Command and Control Research and Technology Symposium, Los Angeles
MIM (2018) MIP information model website. https://www.mimworld.org/. Accessed on 11 June 2018
NATO (2018) Federated mission networking website. http://www.act.nato.int/fmn. Accessed on 11 June 2018
Principles for Digital Development (2018) Website. https://digitalprinciples.org/. Accessed on 11 June 2018
Sandstrom K (2014) Remoteness and 'demonitored space' in Afghanistan. Peacebuilding 2(3):286–302
Schade U, Dürr G (2005a) Die Stufen der Interoperabilität. Strategie und Technik 1(2005):16–18
Schade U, Dürr G (2005b) "Over the Edge": Die Stufen der Interoperabilität II. Strategie und Technik 9(2005):39–41
Schmitz H-C, Pieneman R, Deneckere M (2017) Information management in a civilian mission—EUCAP Somalia case study. In: Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS). IEEExplore, Oulu
UN (2018) United Nations peacekeeping website. https://peacekeeping.un.org. Accessed on 11 June 2018
UN OCHA (2018) Centre for humanitarian data website. https://centre.humdata.org/. Accessed on 11 June 2018

Affiliations

Hans-Christian Schmitz[1] · Matthias Deneckere[2] · Tommaso De Zan[3] · Wolfgang Gräther[4]

Matthias Deneckere
mde@ecdpm.org

Tommaso De Zan
tommaso.dezan@linacre.ox.ac.uk

Wolfgang Gräther
wolfgang.graether@fit.fraunhofer.de

1 Fraunhofer FKIE, Fraunhoferstr. 20, 53343 Wachtberg, Germany

2 ECDPM, Onze Lieve Vrouweplein 21, 6211 HE Maastricht, The Netherlands

3 Centre for Doctoral Training in Cyber Security, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

4 Fraunhofer FIT, Schloss Birlinghoven, 53754 St. Augustin, Germany