CIVILEX

Supporting European Civilian External Action

Policy brief
July 2017

Recommendations for the development of a future Situational Awareness, Information Exchange and Operation Control Platform (OCP) in EU civilian CSDP missions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700197

Preface

This policy brief presents findings and recommendations from the CIVILEX project. The CIVILEX project was funded through a 'Coordination and Support Action[1]' call in the H2020 Research and Innovation Framework of the European Commission. The call titled '*Next generation of information systems to support EU external policies*' invited consortia to submit proposal to establish recommendations for the development of a future common Situational Awareness, Information Exchange and Operation Control Platform (OCP for short), to be employed in EU civilian CSDP missions. The resulting recommendations form the basis for a subsequent 'Pre-Commercial Procurement' project[2], eventually leading to the development of the platform.

In response to the call, a consortium consisting of ATOS (SP), TNO (NL), Fraunhofer (DE), ECDPM (NL), IAI (IT) and the EU Satellite Centre (SP) proposed the CIVILEX project (Supporting European civilian external action). The EU selected the proposal for funding, and the CIVILEX project ran from 1 May 2016 to 30 April 2017.

The objective of the CIVILEX project was to identify a comprehensive set of requirements and to develop recommendations and a roadmap for a future common Situational Awareness, Information Exchange and Operation Control Platform. To this end the CIVILEX consortium: a) analysed communication and information management procedures and technologies in current civilian EU CSDP missions, b) reviewed state-of-the-art of communication and information management technologies and c) provided technical, organisational and institutional recommendations for further research, acquisition and implementation of a future OCP.

Through desk research and interviews with stakeholder in Brussels and in EU CSDP missions, the CIVILEX project obtained a comprehensive overview of the current state of affairs on information management, situation awareness and operational control within the EU civilian crisis management structures, including the European External Action Service (EEAS), the European Commission, in particular the Foreign Policy Instruments (FPI) and the Council.

The dynamic foreign policy landscape and the rapidly evolving crises across the globe require the European External Action Service to enhance its effectiveness and agility for the planning and conduct of CSDP missions. This is especially the case for EU civilian missions that can rely less on proven practices and tools than their military counterparts, and typically run in a very complex and susceptible multi-stakeholder environment. The Union recognises this need, and has reinforced this notion in the EU Global Strategy (EUGS)[3].

The CIVILEX research has led to the conclusion that communication and information management in EU civilian CSDP missions is currently in a **rather fragmented state**. Gaps during operations emerge: these seem characterized by enduring fragmentation in information exchange procedures and systems across missions, and a widespread prevalence of ad-hoc measures and practices. Additionally, there seems to be an uncomfortable relationship between formal information classification rules and practical information security practices, which results in a placating yet underappreciated attitude towards information security. Although

[1] H2020-BES-11-2015
https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/bes-11-2015.html
[2] H2020-BES-13-2017
https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/sec-13-bes-2017.html
[3] EU Global Strategy
https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

classified information is handled through proper, strict procedures and well-guarded communication systems, the analysis highlights a lack of an information security culture.

EU and CSDP officials interviewed for the project provided examples of inadequacies in communications and information sharing within and among CSDP civilian mission bodies, as well as with external partners and stakeholders. Therefore, improvement of information management procedures and systems would be widely and warmly welcomed. This seems especially important since future mission might need to interact with growing numbers of external partners, and become increasingly information-dependent for their success.

Even though most stakeholders agree that technology on itself is insufficient to solve current shortcomings, the development of an integrated mission-spanning information platform is seen as a crucial asset to ensure that future CSDP civilian missions can meet their objectives more efficiently. Various efforts to define and implement such a platform have been undertaken, but a common, integrated platform concept has not yet emerged. The planning and implementation of these missions is a complex effort that involves different EU structures and bodies, and touches upon many services and information sources. In this context, the powers of each Head of Mission in the definition, selection and establishment of communication and information management tools, due to the absence of common platforms, has an obvious impact on the proliferation of diverse systems and tools across missions, raising inherent interoperability issues.

A long-term strategy on information management in EU civilian CSDP missions is needed. Without clearly defined ambitions and performance criteria, it is difficult to orchestrate innovation and to create unity of vision and effort across EU external actors. There are various ongoing innovation activities (e.g. the Mission Support Platform development, future OCP to be funded by SEC-13 H2020 call) and efforts to achieve harmonised cross-mission information management procedures), but these will considerably improve their impact and efficiency by being supported by an overarching strategy.

Policy recommendations

As stated, the CIVILEX project is a first stage in a multi-year procurement trajectory of the EU for a future common Situational Awareness, Information Exchange and Operation Control Platform, to be employed in EU civilian CSDP missions. As such, the results of this project were meant to inform the subsequent stage, the pre-commercial procurement which is part of the H2020 work programme.

We recommend the following issues to be taken into account in subsequent development and procurement activities:

- **Invest in strategy, leadership, unity of vision and in technology.** The proposed procurement process is technology-oriented, and will result in two pilot systems. These tangible prototypes – implemented with support from purported end-users – will inform the discussion of possible adjustments and adaptations in current EU civilian missions: a room for improvement in strategy and leadership on information management innovation. The interplay of strategy, unity of vision and technology is a recipe for successful adoption of the CIVILEX workplace.
- **Examine existing initiatives and make OCP development a joint and unifying effort.** There are many innovation initiatives in EU external action, but they do not stem from an overarching strategy. This particular procurement trajectory runs independent

from some important actions in the EEAS landscape, such as the Mission Support Platform. 'OCP development' should be a joint effort by all stakeholders in the EEAS organisation – from HQ level to the mission field. Any subsequent activity (such as the procurement activity under the H2020 programme) should engage directly with related innovation activities (such as the MSP), and make an explicit effort to build a common vision for a future OCP.

- **Make information management a key growth factor in EEAS mission performance innovation.** The EUGS calls for more efficient information exchange and more agility and flexibility in mission planning and execution. The strategy fails to recognise information management maturity as the most important factors in that ambition. The EEAS should recognise that it needs to go beyond information management technology, and invest in stronger information management policies, structures, procedures and competences.

- **Support transformation of CSDP civilian missions and EEAS into an organization 2.0.** The integration of advanced Web applications such as Wiki, blog systems or 'social network systems' into the CIVILEX workplace will improve the cooperativity, flexibility and the knowledge of the organization. These widely used applications support the diversity of users in CSDP civilian missions and in EEAS.

OCP development recommendations

In general, an improvement of information management procedures and systems is welcomed by the stakeholders in the EU external action community and civilian CSDP missions. The research in the CIVILEX project resulted in a number of key recommendations on the development trajectory of an 'Operation Control Platform'.

- **Development of an 'OCP' must be regarded as a comprehensive challenge that involves innovation at the technical, organisational, procedural and institutional level.** Failing to address either of these dimensions properly will result in an OCP that will not yield the desired increase in performance.

- **OCP development must be driven by clear ambitions on information management, and in line with strategic objectives.** OCP development must start with a comprehensive discussion among stakeholder and end-users about expected values, functionalities and innovation criteria. Failing to do so will result in suboptimal solutions and waste of resources during development.

- **Build an OCP and the surrounding information management structures in an incremental fashion.** EU external action and the global geopolitical landscape are in flux. This might cause OCP demands to change over time (e.g. necessitate different information management functions). To accommodate such changing demands, OCP development must be incremental and flexible in nature.

- **Make the development of the OCP and the surrounding information management structures an ongoing innovation process with systematic evaluation and decision junctures, guided by a transparent roadmap.** OCP development should not be regarded as an isolated technology acquisition activity, but rather as part of a continuum of information management innovation. There must be continuous innovation in this domain, and systematic evaluation of performance. This process must be guided by a

transparent and widely accepted roadmap that links innovation activities with ambitions, and sets performance criteria.

Platform recommendations

The project has resulted in the following recommendations on the platform, and its position in the organisation.

Institutional and OCP positioning recommendations

- **Ownership of the OCP must be clarified, in a legal and practical sense**. 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". It needs to be clarified who holds responsibility over the content, management and implementation of the OCP.
- **The CPCC should establish a Chief Information Management role, mandated to develop an information management innovation strategy and to oversee standardisation, innovation and technology development.** This role would provide the leadership to create unity of vision and effort on information management innovation.
- **The OCP should provide controlled access channels for external parties within the EU and in the theatre of operation.** Through these channels, the mission organisation and external parties will share background knowledge and situational awareness information.
- **Establishment of central body dealing with standardized architectures, Standard Operating Procedures (SOPs), and Standard Operating Instructions (SOIs) across missions.** The majority of interviewed staff members indicate that a central body is required with a strong mandate to align not only operational procedures, but to ensure that senior EEAS mission staff complies with future directives for information handling.
- **Information management SOP's and functional information profiles need to be aligned with the institutional decision making structure.** Currently, there are no specialized staff members who are made responsible to manage the information flow within their organisation. To ensure implementation of future SOP, SOI's that are in line with working practices and the EEAS mission decision making structure, interviewees indicated a need for information managers to address this issue.

Organisational and process level

- **There must be standardization of procedures, systems and information formats.** Respondents indicated that there are differences in procedures, systems and formats across missions. The future OCP must work from a common baseline, agreed upon and implemented throughout the EEAS organisation. Business continuity should be a default concern when building up a mission.
- **Information access management needs to be centrally organised, and standardized via profiles.** Currently, access to information is managed at mission level, and in a non-standardized manner. The OCP must use standard profiles for information

access, and the assignment of profiles to actors should be managed at a central agency at HQ level.

- **The OCP must provide inclusive support for informal communication and collaboration.** Informal communication means (e.g. chat, file sharing and teamwork applications) are used widely, and outside of the formal procedures and platforms. The OCP should provide support to include such applications, or replicate their functionality. This is a major factor for acceptance of a future OCP, and needs to be organised at the organisational level.
- **Security awareness in information exchange needs to be improved among mission staff.** Even though security is a high priority for EU actors, it is somehow considered as a burden in information exchange. It is essential to improve the security culture so that mission staff is more aware of threats and vulnerabilities and trained to process and exchange information in a secure manner.

Technical level

- **The OCP must offer an integrated, streamlined experience to its users.** Currently, there are different systems for secure and non-secure communications, and information processing. A future integrated system must provide its users with a personalised, integrated information environment that encapsulates all vital information functions, such as secure communication, reporting mechanisms and personal communication.
- **The OCP must be interoperable with other existing information systems in- and outside of the EU civilian CSDP missions**. It is essential that the OCP is made interoperable with other systems in use by in- and external actors such as local organisations, peer missions, international organisations, NATO, UN and others.
- **The OCP must enable secure information exchange with varying levels of security.** The OCP must enable secure information exchange, preferable with options to provide varying levels of communication security (e.g. encryption, communication channel selection).
- **The OCP should contain functionalities to help to manage resources and assets – or be linked to such systems**. While the core functions of the OCP should focus on operational information, it is recommended to also let the platform support functionalities that help to manage people, budgets and payments, buildings and assets – or be linked closely to such systems.

Further information

For further information, please visit http://civilex.eu