EU-CIVCAP

Preventing and Responding to Conflict: Developing EU CIVilian CAPabilities for a sustainable peace

Report on Technological Shortcomings in Early Warning and Conflict Analysis

Deliverable 3.1
(Version 1.4)
30 January 2017

Jenny Berglund and Denis Bruckert

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 653227.
How to cite this report

Summary of the document

<table>
<thead>
<tr>
<th>Title</th>
<th>DL 3.1 Report on Technological Shortcomings in Early Warning and Conflict Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last modification State</td>
<td>30 January 2017 Final</td>
</tr>
<tr>
<td>Version</td>
<td>1.4</td>
</tr>
<tr>
<td>Leading Partner Other Participant Partners Authors</td>
<td>EUSC UBRIS Jenny Berglund and Denis Bruckert</td>
</tr>
<tr>
<td>Audience</td>
<td>☑ Public □ Restricted □ Internal</td>
</tr>
<tr>
<td>Abstract</td>
<td>The report aims to map and analyse the available technological tools for conflict early warning and conflict analysis of the EU, identify possible shortcomings and propose solutions.</td>
</tr>
<tr>
<td>Keywords</td>
<td>• Conflict Early Warning • Conflict Analysis • Information • Data • Analysis • Earth Observation Geospatial Information • Horizon 2020 • ICT • Big Data • Information Exchange Technologies</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF FIGURES</td>
<td>4</td>
</tr>
<tr>
<td>Executive summary</td>
<td>5</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>7</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>8</td>
</tr>
<tr>
<td>1.1 THE EU’S CONFLICT EARLY WARNING SYSTEM AND CONFLICT ANALYSIS</td>
<td>9</td>
</tr>
<tr>
<td>1.2 CONFLICT EARLY WARNING SYSTEM</td>
<td>10</td>
</tr>
<tr>
<td>1.3 CONFLICT ANALYSIS</td>
<td>12</td>
</tr>
<tr>
<td>2. MAIN TECHNOLOGIES FOR EARLY WARNING AND CONFLICT ANALYSIS</td>
<td>15</td>
</tr>
<tr>
<td>2.1 EARTH OBSERVATION GEOSPATIAL INFORMATION</td>
<td>15</td>
</tr>
<tr>
<td>2.2 INFORMATION ANALYSIS AND MEDIA MONITORING TOOLS</td>
<td>21</td>
</tr>
<tr>
<td>2.3 HORIZON 2020 TECHNOLOGICAL SUPPORT IN EU EARLY WARNING AND CONFLICT PREVENTION</td>
<td>25</td>
</tr>
<tr>
<td>2.4 INFORMATION AND COMMUNICATION TECHNOLOGIES</td>
<td>28</td>
</tr>
<tr>
<td>2.5 BIG DATA</td>
<td>33</td>
</tr>
<tr>
<td>2.6 INFORMATION EXCHANGE TECHNOLOGIES FOR EARLY WARNING AND CONFLICT ANALYSIS OF THE EU</td>
<td>36</td>
</tr>
<tr>
<td>CONCLUSIONS AND RECOMMENDATIONS</td>
<td>39</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>41</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1. Four steps of the EU’s Conflict Early Warning System ................................................. 12
Figure 2. The EU’s conflict-prevention internal mechanism .......................................................... 14
Figure 3. SatCen IMINT product for the monitoring of military activity in a crisis area ............ 18
Figure 4. Example of a SatCen Copernicus product in support of external action: Risk assessment of the production of illicit crops ......................................................................................... 19
Figure 5. SWOT for Earth observation geospatial information ......................................................... 21
Figure 6. Example graph from EMM.NewsBrief.eu ......................................................................... 23
Figure 7. SWOT for information analysis and media monitoring tools ............................................. 24
Figure 8. SWOT for Horizon 2020 technological support ................................................................. 27
Figure 9. Mobile network coverage and evolving technologies ....................................................... 28
Figure 10. SWOT for ICTs ............................................................................................................... 32
Figure 11. SWOT for Big Data ........................................................................................................ 36
Figure 12. SWOT for information exchange technologies ............................................................... 38
EXECUTIVE SUMMARY

According to Arts 3(1) and 21(2) of the Treaty on European Union, the EU aims to “promote peace, its values and the well-being of its peoples” and to “preserve peace, prevent conflicts and strengthen international security”. Consequently, one of the main tasks of the European External Action Service (EEAS) consists of preventing the emergence of conflicts in non-EU countries. Towards this aim, the EEAS has established a Conflict Early Warning System (EWS) and a conflict analysis method to detect potential situations in non-EU countries that possibly could lead to a violent conflict if unattended.

The EWS is based on systematic collection and analysis of information coming from a variety of sources, in order to identify and understand the risks of violent conflict in a country and to develop strategic responses. Conflict analysis gathers and analyses, in a structured framework, the context, the causes of the conflict, the actors and the various dynamics; it also identifies the existing and planned responses, the key gaps, options and realistic strategies to respond to conflict. In support of these activities, the EU has various technological tools at its disposal. The aim of this report is to map possible technological tools for the implementation of conflict early warning and conflict analysis, assess their use in the EWS and the conflict analysis of the EU, identify any possible shortcomings and gaps, and finally propose solutions and recommendations to bridge them.

The assessed tools have been grouped into five clusters: Earth observation geospatial information, analytical tools, Horizon 2020 projects, information communication technologies (ICT), Big Data¹ and finally, a logistical cluster, necessary for the effectiveness of the EWS and conflict analyses, which is information exchange systems. Each cluster is analysed by using a SWOT model (on strengths, weaknesses, opportunities and threats).

While Earth observation geospatial information and analytical tools are commonly used in the EU’s early warning and conflict analysis, the Horizon 2020 projects, ICT and Big Data are analysed in the light of their potential use in this area, since this report cannot find evidence that these technologies are officially being used by the EU in its methodology for early warning and conflict analysis. The outcomes of ongoing Horizon 2020 projects in this area are still to be validated and implemented.

The findings of this report show that the first two clusters mentioned above serve as evidence bases for the EU in predicting possible future conflicts and, consequently, in deciding on early reaction. The main strengths of Earth observation geospatial data are the possibilities to obtain information in a non-intrusive manner, in real or near real-time, and from remote and inaccessible areas. The fact that Earth observation data only can detect physical signs of change to a situation, that this information should be processed and analysed by skilled imagery analysts or an automated system in order to be useful, and that technological means of secure communication are needed to share sensitive information, can be considered weaknesses of Earth observation geospatial data.

---

¹ The concept of big data is differentiated in this report by using uppercase letters when referring to Big Data as a ‘field of practice’ and lowercase letters when referring to the data as such.
The analytical tool used in the initiation of the EWS cycle, the Global Conflict Risk Index, is based on quantitative indicators, using a linear regression model to calculate the risk and probable intensity of a violent conflict in a country within one to four years. The index is based on the principle of ‘data in, data out’, which means that if the source data have errors, are not updated or are missing, the outcome will reflect that. It also lacks perception-based data.

In view of the development of ICT and the huge amount of data that it generates, the EU should consider integrating it, together with Big Data technologies and analytics, in order to complement and optimise the information already obtained from the two technologies above.

Technical support from Horizon 2020 projects can enable a comprehensive, comparative and multidisciplinary analysis and development of EU capabilities in this area. Horizon 2020 projects take into account user requirements in various policy areas of the EU and bring together key actors in the private and public domains to address new technologies. The weaknesses identified include the complexity of financial rules and agreements, which could discourage smaller organisations, structures and innovative small and medium-sized enterprises from participating in a project. Nevertheless, among the opportunities are the support received from users and institutional actors, the potential development of new tools and services for early warning, conflict analysis and prevention.

Finally yet importantly, this report highlights the lack of a unified information exchange system within the EU structures, with almost every EU policy area and service having its own classified system (civilian, military, intelligence, etc.). Given the lack of interconnectivity both on a technological level and on a human as well as physical level – as the EU’s conflict prevention structures are based in different premises – good personal contacts and cooperation between different actors and services, willing to share information and cooperate, are key conditions for a smooth and effective exchange and sharing of information among the assorted Brussels-based bodies and EU delegations.

To respond to the different shortcomings highlighted in this report, it is recommended that the EU envisage the following actions:

1. **Reflect on how new technologies such as ICT and Big Data could be added, in a sustainable manner, to the existing technological tools for early warning and conflict analysis.**

2. **Update, mainstream and coordinate the various capacities and their use within different services dealing with conflict early warning and conflict analysis, in order to bridge gaps, improve interconnectivity and avoid duplication.**

3. **Properly familiarise staff involved in the early warning and conflict analysis cycle with the available tools.**

4. **Assure that technological tools for early warning and conflict analysis are aligned with EU policies on conflict prevention and vice versa.**
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFSP</td>
<td>Common Foreign and Security Policy</td>
</tr>
<tr>
<td>CSDP</td>
<td>Common Security and Defence Policy</td>
</tr>
<tr>
<td>DG DEVCO</td>
<td>Directorate-General for International Cooperation and Development</td>
</tr>
<tr>
<td>DG ECHO</td>
<td>Directorate-General for Humanitarian Aid and Civil Protection</td>
</tr>
<tr>
<td>EC3IS</td>
<td>European External Action Service Corporate Classified Communication and Information System</td>
</tr>
<tr>
<td>EEAS</td>
<td>European External Action Service</td>
</tr>
<tr>
<td>EMM</td>
<td>European Media Monitor</td>
</tr>
<tr>
<td>EUMS B</td>
<td>EU Military Staff Intelligence Directorate</td>
</tr>
<tr>
<td>EWS</td>
<td>Early Warning System</td>
</tr>
<tr>
<td>FFP</td>
<td>Fund for Peace</td>
</tr>
<tr>
<td>FSI</td>
<td>Fragile States Index</td>
</tr>
<tr>
<td>GCRI</td>
<td>Global Conflict Risk Index</td>
</tr>
<tr>
<td>GEOINT</td>
<td>Geographical intelligence</td>
</tr>
<tr>
<td>HR</td>
<td>High Representative</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communication technologies</td>
</tr>
<tr>
<td>IMINT</td>
<td>Imagery intelligence</td>
</tr>
<tr>
<td>IntCen</td>
<td>EU Intelligence and Situation Centre</td>
</tr>
<tr>
<td>JRC</td>
<td>Joint Research Centre</td>
</tr>
<tr>
<td>PSC</td>
<td>Political and Security Committee</td>
</tr>
<tr>
<td>RPAS</td>
<td>Remotely piloted aircraft systems</td>
</tr>
<tr>
<td>SatCen</td>
<td>Satellite Centre</td>
</tr>
<tr>
<td>SECPOL</td>
<td>Security Policy and Conflict Prevention Directorate</td>
</tr>
<tr>
<td>SECPOL.2</td>
<td>Conflict Prevention, Peacebuilding and Mediation Division, European External Action Service</td>
</tr>
<tr>
<td>SIAC</td>
<td>Single Intelligence Analysis Capacity</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small and medium-sized enterprises</td>
</tr>
<tr>
<td>SWOT</td>
<td>Strengths, weaknesses, opportunities, threats</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

Early warning and conflict analysis increasingly require the use of a wide range of technological tools. Today, the more ‘classic’ technologies, such as geospatial information supported by remote sensing applications, are accompanied by newer technologies, notably data analysis and information communication technologies (ICT) like mobile phones, smartphones, different software and big data. Mobile phones and the Internet have modified our communication habits and how we relate and engage with the world. “In the 21st century, the revolution may not be televised – but it likely will be tweeted, blogged, texted and organised on Facebook.”²

The Arab Spring is maybe the most striking example of the important role that social media plays today in the information, perception and evolution of events. During the week before the resignation of Egyptian President Hosni Mubarak, for example, the total rate of tweets from Egypt – and around the world – about political change in the country ballooned from 2,300 a day to 230,000 a day.³ Such a change of pattern of course raises the question of whether current technologies for early warning systems to prevent violent conflict are accurate and, if not, how they could adapt to the sociotechnical circumstances of today.

This report analyses technologies for peacebuilding and conflict prevention, with the aim of mapping possible technological tools for the implementation of conflict early warning and conflict analysis, assessing their use in the EU’s Early Warning System (EWS) and conflict analysis, identifying any possible shortcomings and gaps, and finally proposing solutions or recommendations in order to bridge them.

A wide definition of technologies has been applied in this report, in which technology refers to i) the application of practical sciences to industry or commerce; ii) the methods, theory and practices governing such application (e.g. a highly developed technology); and iii) the total knowledge and skills available to any human society for industry, art, science, etc.⁴

These technological tools have been clustered in the following categories:

- Earth observation geospatial information (including imagery intelligence and remotely piloted aircraft systems (RPAS));
- analytical tools (provided by the EU Joint Research Centre (JRC));
- the added value of Horizon 2020 research in addressing technological shortcomings;
- ICT (mobile phones, smartphones, the Internet and software);
- Big Data; and
- information exchange systems.

---

³ Ibid.
The first set of tools can be considered ‘classic’ tools for information collection and analysis for early warning and conflict analysis-related activities. They have existed for a few decades and are widely used and consolidated, while ICT and Big Data often are referred to as ‘new technologies’, which during the last decade have had an impact on our way of relating and communicating with our surrounding environment. In line with the findings of this report, these tools are not yet (officially) being used in early warning and conflict analysis methodologies, and therefore they are described more in the light of their possible usage, and assessing their potential influence on early warning and conflict analysis working methods.

To apply an analytical framework to this report, the different tools presented will be evaluated through a SWOT analysis (on strengths, weaknesses, opportunities and threats); the first two elements look at internal aspects, while the last two assess the external environment in which these tools are used. This framework allows for an integral analysis that can serve for planning and strategic purposes.

Due to the limited scope of analysis of this deliverable (EWS and conflict analysis), this report will concentrate on the tools useful for this purpose, those we know are already used by the EU in this area, and tools that could have potential use and bring added value to those activities. Other tools that we found more applicable to crisis management and peacebuilding, but not specifically to early warning and conflict analysis, such as satellite communication systems (SATCOM) and satellite navigation and positioning systems (SNAP), have not been included in this report, but are mentioned in the EU-CIVCAP report on “Preventing Conflicts: Personnel, Procedures and Technology in Conflict Prevention and Peacebuilding” (DL 2.1), which maps key capabilities by using case studies from four EU Member States. Furthermore, another EU-CIVCAP paper (DL 2.3) will focus on dual-use technologies, such as different satellite technologies in conflict prevention and peacebuilding.

This report is based on primary documents (official documents and reports) and secondary scholarly sources. In-house expertise of the EU Satellite Centre (SatCen) has been used in the elaboration of this deliverable, especially for the sections on Earth observation geospatial information and Big Data.

1.1 THE EU’S CONFLICT EARLY WARNING SYSTEM AND CONFLICT ANALYSIS

According to Arts 3(1) and 21(2) of the Treaty on European Union, the EU aims to “promote peace, its values and the well-being of its peoples” and to “preserve peace, prevent conflicts and strengthen international security”. Consequently, one of the main tasks of the European External Action Service (EEAS) is preventing the emergence of conflicts in non-EU countries. Preserving peace in the EU neighbourhood is also a way of guaranteeing security within the European borders. To anticipate effectively the emergence of new conflicts, the EEAS relies on its EWS and conflict analysis capabilities.

The EWS was implemented in 2011, in accordance with the Treaty of Lisbon (Art. 21c). It consists of the “systematic collection and analysis of information coming from a variety of sources in order to identify and understand the risks for violent conflict in a country and to
develop strategic responses to mitigate those risks”.\(^5\) The goal is to assess the structural risks of conflict emergence, which will allow the pursuit of more efficient, early preventive actions. With a time horizon of four years, the EWS is updated every six months.

Conflict analysis aims to provide EU decision-makers with accurate information about the structural elements of a conflict, in order to allow for a comprehensive approach to conflict analysis and response. According to the EEAS guidance note on the use of conflict analysis in support of EU external action, a conflict analysis “uses a structured framework as the basis for information gathering, analysis, interpretation, appreciation of the realms of the possible and prioritisation of responses”.\(^6\) The key elements analysed are the context, the causes of the conflict, the actors and the various dynamics; also identified are the existing and planned responses and finally, the key gaps, options and realistic strategies to respond to the conflict.\(^7\)

Before the Treaty of Lisbon, EU conflict prevention was guided by the EU Programme for the Prevention of Violent Conflicts established in 2001, with the Policy Planning and Early Warning unit being responsible for early warning activities. Currently, conflict prevention and crisis response are under the responsibility of the Deputy Secretary General of the Common Security and Defence Policy (CSDP). The division SECPOL 2 – Conflict Prevention, Peacebuilding and Mediation – is specifically dedicated to these issues (see Figure 1 in section 1.2).

### 1.2 CONFLICT EARLY WARNING SYSTEM

The EWS process can be divided into four steps – risk scanning, prioritisation, shared assessment and follow-up, and monitoring – each step associated with various institutions and actors.

**The risk-scanning** phase focuses on the preparatory work of the EWS. It consists of collecting data and risk information to enable the prioritisation and assessment of the risks. This is mainly done by the EU Intelligence and Situation Centre (IntCen) and the Military Staff Intelligence Directorate (EUMS B) through the Single Intelligence Analysis Capacity (SIAC) and the Security Policy and Conflict Prevention Directorate (SECPOL). IntCen compiles information through its two divisions IntCen 1 (Intelligence Analysis) and IntCen 2 (Open source intelligence), while the Situation Room (IntCen 3) will intervene for launching early alerts and provide worldwide monitoring. The data acquired by the SIAC is used alongside the Global

---

\(^5\) EEAS, “EU Conflict Early Warning System”, Fact Sheet, Brussels, September 2014.


\(^7\) Ibid., p. 4.
Conflict Risk Index (GCRI), the main resource for this stage of the EWS. Other tools are used for risk scanning, such as the InfoRM index or the early warning watch list.

Drawing on these elements, prioritisation can take place. The management and staff of the EEAS and Commission services, including delegations, review the preparatory risk scanning, assessing it in conjunction with specific EU interests and the value of reviewing, enhancing or expanding EU engagement to increase the EU’s impact on prevention and/or peacebuilding. The result of this is shared with Member States through the Political and Security Committee (PSC). These actors discuss the results provided by the risk scanning with Member States, and according to the prioritisation decision, ask for further analysis.

Following the result of the discussion in the PSC and, if relevant, upon its appropriate guidance, the shared assessment and follow-up involves many participants: EU delegations, field offices of the Commission’s Directorate-General for Humanitarian Aid and Civil Protection (DG ECHO), CSDP missions in-country, EU Special Representatives, Member States’ embassies in non-EU countries, the geographical and thematic staff of the EEAS and Commission services' headquarters, Council working groups and the PSC. In-country, all EU actors are consulted based on a structured discussion around a series of factors linked to human security, covering political, social cohesion and public security, conflict prevalence, geography and environment, and economic factors provided by the Conflict Prevention, Peacebuilding and Mediation division of the EEAS (SECPOL 2).

Conflict analysis reports prepared by the Commission's Directorate-General for International Cooperation and Development (DG DEVCO) and by DG ECHO on existing conflicts or risks of conflict, through deep political economy analysis or simply through light-touch analysis (see section 1.3), are also taken into consideration and evaluated in this step. The outcomes of this process are regrouped into checklists for the structural risks of conflict, which represent the collective assessment of EU actors at the country level. These checklists are then used by the EEAS geographical services to write conflict prevention reports that present the risks noted and some recommendations for action. These reports are discussed within the EEAS, Commission services and with Member States in order to determine the actions and stance of the EU. The conflict prevention reports stemming from this process are shared and

---

8 The GCRI is based on quantitative indicators from open sources; it provides evidence-based statistics about the probability and intensity of violent conflicts for the next four years. This tool is further described in section 2.2 of this report.
9 The SIAC is a working arrangement between the EUMS B and IntCen, producing joint civil–military intelligence assessments.
10 The index proposes a ranking of countries according to their levels of risk of emergencies and disasters (very high, high, medium and low). The index is the result of interagency cooperation (http://www.inform-index.org/).
11 Every six months the International Crisis Group publishes an early warning watch list of up to ten countries particularly vulnerable to an outbreak of violent conflict in the following six or twelve months (http://www.crisisgroup.org/en/publication-type/watch-list.aspx).
discussed with the relevant geographical working groups of the Council and serve as a basis for follow-up by the various EEAS/Commission services, EU delegations and Member States.\textsuperscript{13}

\textit{Figure 1. Four steps of the EU’s Conflict Early Warning System}

![Diagram showing the four steps of the EU's Conflict Early Warning System]


Finally, the \textit{monitoring} step is the ‘review moment’ of the EWS cycle, occurring every six months and through which services report on progress with regard to recommendations identified in the conflict prevention reports, issued at the shared-assessment level. Proposals for early action that have been identified, initiated or implemented and their impacts are assessed. At this stage the identified options for action may be modified, updated and revised. This monitoring serves as a trigger for new guidance on future action as well as a basis for lessons learned during the EWS process. This step is carried out by the staff of the EEAS and Commission services, as well as by Member State representatives.\textsuperscript{14}

\section*{1.3 CONFLICT ANALYSIS}

Conflict analysis is the second pillar of the EU conflict prevention system, indispensable to assess effectively the roots of a conflict and, consequently, to implement an efficient set of actions. One of the goals of conflict analysis is to be able to apply a \textit{proactive conflict-sensitive approach}, in order to comply with the ‘do no harm’ European value.\textsuperscript{15} Conflict analysis follows a precise path, which has been defined by the \textit{EEAS guidance note on conflict analysis} in support of EU external action. This guidance identifies seven key elements that have to be taken into consideration: the context of the conflict, its roots (structural, proximate causes, 

\textsuperscript{13} Ibid., pp. 5-6.

\textsuperscript{14} EEAS and European Commission (2013), op. cit., pp. 6-7.

\textsuperscript{15} Ibid., p. 1.
factors of resilience, etc.), the actors, the various dynamics, potential outcomes, the possible responses and finally the identification of key gaps, options and realistic strategies to respond to the conflict. Still, according to this guidance, a conflict analysis process should involve “the active participation of all the EU stakeholders who need to own and use its findings. Typically, this will include the delegation(s), the EEAS and DG DEVCO, and other Commission services such as DG ECHO and the Foreign Policy Instrument (FPI).” The conflict analysis procedure can be initiated by an EU delegation, country desks or staff at the headquarters of the Commission, the EEAS and EU Special Representatives, or numerous other actors (see Figure 1). SECPOL 2 and the DG DEVCO unit for Fragility and Crisis Management will provide, for example, analytical support. Depending on the situation, two types of conflict analysis can be applied. The first one is a light-touch conflict analysis that can quickly provide an overview of the situation to the decision-maker. If not sufficient, it can be completed by a more in-depth study. Light-touch analysis is based on an interactive, cooperative conflict-analysis workshop, which can be undertaken in one or two days with, if possible and necessary, external experts. The light-touch analysis is best suited when a quick response is needed.

The second one is a conflict-sensitive, political economy analysis. It is applied for in-depth assessments and provides a deeper understanding of the country, sector dynamics, interests and issues. It focuses on the particular interests of groups and individuals, and on the distribution of power, wealth, etc. Here also, DG DEVCO’s Fragility and Crisis Management unit along with the Quality of Delivery Systems unit are part of the process. Similarly, civil society input is also taken into account in this process.

Figure 2 provides an overview of the internal structure and procedures for the EWS and conflict analysis.
DL 3.1 Report on Technological Shortcomings in Early Warning and Conflict Analysis

Figure 2. The EU’s conflict-prevention internal mechanism

- Political and Security

- Deputy Secretary General CSDP and crisis response

- EARLY WARNING
  - Shared-assessment
  - Prioritisation

- CONFLICT ANALYSIS
  - Political economy
  - Light-touch analysis

- Early response

- Risk-scanning

- SECPOL 2
  - Conflict prevention, peace building

- Technological support

- EU delegations, EU representatives, EEAS & Commission services, PSC.

- ECHO field offices

- INTCEN

- EUMS

- Collect data

- DG DEVCO

- DG ECHO

- Foreign Policy Instruments

- Political and Security

- SatCen Geospatial Intelligence

- Networks for Information Exchange

- JRC analytical tools

- Horizon 2020 Projects & new technologies
2. MAIN TECHNOLOGIES FOR EARLY WARNING AND CONFLICT ANALYSIS

This section examines a number of technological tools and their potential to support early warning and conflict analysis activities. More specifically, this section will analyse the following tools:

- Earth observation geospatial information;
- analytical tools;
- the added value of Horizon 2020 in addressing technological shortcomings;
- information exchange technologies (including classified networks);
- ICT (mobile phones, smartphones, the Internet and software); and
- Big Data.

2.1 EARTH OBSERVATION GEOSPATIAL INFORMATION

Geospatial information relies first and foremost on Earth observation data obtained by remote sensing techniques (satellites, aerial imagery and RPAS) used to elaborate imagery intelligence (IMINT) and geographical intelligence (GEOINT) products.\(^\text{16}\)

Different satellites give images with a different resolution and different wavelength depending on the specification of the instrument (sensor) carried by the satellite (optical, radar, infrared, video, etc.). The election of acquiring imagery from a satellite with one type of sensor or another depends on the purpose for the usage of the imagery, weather conditions and other contextual conditions. Today, commercial satellites can give imagery resolution as high as approximately 23-25 centimetres, while governmental satellites can perform slightly better. Technical developments are continually compensating for the flaws of satellite imagery (cloud coverage, sun synchronous orbits making satellites pass over an area more or less during the same period of the day, poor resolution and programming issues such as shuttle control). The introduction of microsatellites on the commercial market, expected within two to three years, will make it possible to have more satellites in orbit that will be constantly active (vs programmed acquirement), permitting access to a huge quantity of data. Multispectral satellites carrying different sensors also make it possible to use one or another depending on the current conditions at the moment of acquiring an image. Satellite constellations consist of a group of satellites working in concert with coordinated ground coverage, operating together under shared control. Satellites within a satellite constellation are synchronised so that they overlap well in coverage (meaning the period in which a satellite or other spacecraft is visible above the local horizon). An example of an Earth observation satellite constellation is the Disaster Monitoring Constellation for the International Charter for Space and Major Disasters, consisting of satellites from China, Spain, Nigeria and the UK. Another type of constellation is the Copernicus Sentinel Satellites supporting the different...

\(^{16}\) In this report, geospatial information in the domain of Earth observation to retrieve information and intelligence for security purposes is considered.
services of the Copernicus programme with Earth observation data. The Sentinels consist of six different ‘families’, with each family consisting of two satellites operating in tandem.\(^\text{17}\)

In view of the improved access to geospatial intelligence, and considering the role of the EU SatCen and the Copernicus programme services in support of EU external action, which soon will be operational, the EEAS functions involved in EU early warning and conflict analysis will consequently have access to better and regularly updated geospatial information.

Aerial vehicles such as surveillance airplanes and RPAS, more commonly known as drones, also offer imagery with higher resolution since they operate much closer to the earth, and thus the observed locations, than satellites. Unlike satellites, drones can monitor a location or an area continuously over a long time span. They can also be multisensory and transmit data in real time by streaming. There are several disadvantages of using aerial vehicles such as drones for early warning purposes, however. For instance, unlike satellites, they can be considered intrusive (with the consequences that this implies, i.e. territorial sovereignty, personal privacy issues, etc.). Furthermore, in order to use and navigate a drone in a non-EU country, permission should be given by the authorities of the state on which territory the drone is to be operated. RPAS are piloted under special aerial navigation rules, and naturally, drones are more vulnerable and can easily be jammed or annihilated.

GEOINT combines several disciplines, such as mapping, charting, imagery analysis and imagery intelligence. The basic principle of GEOINT is to organise and combine all available data around its geographical location on Earth, and then exploit it in order to prepare products that can easily be used by planners, political advisers and decision-makers. GEOINT products derived from Earth observation data are considered accurate and useful tools for crisis management, to obtain information from the battleground, to elaborate evacuation plans or to analyse a humanitarian crisis and migration movements in connection with an ongoing conflict. They can similarly be used for conflict prevention purposes, serving as an early warning tool and supporting a conflict analysis by mainly confirming or denying an assumption, for detection and/or monitoring of physical, geographical signs, showing evidence of tension or changes to a precarious situation between or within states.

When it comes to GEOINT, the EU SatCen provides the EU with this capability. The EU SatCen is an agency of the EU and its products and services span over the wider field of crisis management and peacebuilding by providing products that range from analyses of military capabilities to humanitarian aid and non-proliferation.\(^\text{18}\) It operates under the supervision of the PSC and under the operational direction of the High Representative of the Union for Foreign Affairs and Security Policy (HR). The mission of the SatCen has been defined, by Art. 2 of the Council Decision, as “supporting the decision making and actions of the Union in the field of the CFSP [Common Foreign and Security Policy] and in particular the CSDP, including European Union crisis management missions and operations, by providing, at the request of

\[\text{17} \text{ See https://sentinels.copernicus.eu/web/sentinel/home, last accessed on 29 November 2016.} \]
\[\text{18} \text{ For more detailed information on the different products and services of the EU SatCen, see https://www.satcen.europa.eu/services/geospatial_intelligence.} \]
the Council or the HR, products and services resulting from the exploitation of relevant space assets and collateral data, including satellite and aerial imagery, and related services”. 19

The Centre works upon being tasked by the EU or its Member States, while the Council Decision also lays down the provision for cooperation with other EU agencies, institutions, international organisations and non-EU states. Consequently, the SatCen works closely with numerous partners, such as the European Defence Agency, FRONTEX, the European Maritime Security Agency (EMSA), the European Commission and the European Space Agency. It also cooperates and works closely with international organisations, such as the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE) and the Organisation for the Prohibition of Chemical Weapons (OPCW).

In the fields of conflict prevention and early warning, the SatCen works in close cooperation with the crisis management structures of the EEAS under the operational direction of the HR, of which the EUMS B and IntCen are the main task initiators and users of the Centre. As already mentioned above, SatCen products for early warning and support for conflict analysis can be used mainly for the confirmation or the denegation of an assumption of a fact, for detection and/or monitoring of physical, geographical signs showing evidence of tension or changes to a precarious situation between or within states. As such they have their natural place in the early warning system process as seen in section 1.2. In the risk-scanning phase they serve to complement, verify and contrast data obtained from quantitative tools such as the GCRI, and to support the shared assessment and the deeper risk analysis carried out at this stage. They are also useful at the monitoring stage to report on the follow-up of proposed actions and their impact.

Examples of products generated by the EU SatCen, which can serve and feed the early warning and conflict analysis structures of the EU, include border control and border monitoring, treaty verification, arms control and non-proliferation (encompassing chemical weapons), as well as the detection and monitoring of illegal cropping.

---

Furthermore, the involvement of SatCen in the Copernicus services in support of EU external action will complement its current capabilities, by augmenting its capacity to assist stakeholders in the EU external action domain in early warning, conflict prevention and crisis management. The Copernicus Sentinel Satellites and contributing missions are available to feed the SatCen with geospatial information to underpin, for example, the study and monitoring of infrastructure (such as dams, pipelines and other critical infrastructure) in order to prevent natural disasters, which in some circumstances could trigger social tension and conflict.
Finally, the SatCen has been developing new tools that also can serve for early warning and conflict prevention, such as geoportals – web-based applications allowing the consultation on, editing and sharing of geospatial information. Especially developed for situational awareness and crisis management, they offer specific features like the calculation of evacuation routes. The GISMO project (“Geospatial Information to Support decision Making in Operations”), developed together with the European Defence Agency, facilitates the access to SatCen products and services for key CSDP actors. These tools could easily be adapted for use in an early warning and conflict analysis context.

The SatCen does not have direct control over or access to satellite sensors. Although its sources of primary data are commercial, governmental providers are involved on a case-by-case basis, and it gives preference to European space assets when the quality, reactivity and costs are even.

While the EU SatCen is considered the capability of the EU with regard to GEOINT for crisis management, security and defence, the JRC\textsuperscript{20} also supports the EU with satellite imagery analysis for agricultural, environmental, disaster and forest observation purposes, as well as for disaster and crisis management. The JRC supports the Emergency Management Service of

\textsuperscript{20} Among the Directorate-Generals of the European Commission, the JRC falls under the responsibility of the Commissioner for Education, Culture, Youth & Sport, with the mission to carry out research in order to provide independent scientific advice and support for EU policies.
the Copernicus programme, and has for instance developed a Global Human Settlement Map in order to identify all populated areas on the globe. Furthermore, it carries out automatic analysis of satellite data to provide information products and analyses for disaster risk reduction, conflict prevention and assessments for post-disaster responses, recovery and reconstruction planning.\textsuperscript{21} This information is used, among others, by Commission services such as DG DEVCO and DG ECHO, and by Member States’ civil protection services, in order to support their work.

In sum, Earth observation geospatial information gives near real-time information over areas of difficult access, which serves to confirm or refute information obtained from other sources. New technologies and the use of constellations of satellites provide faster communication and improve the image resolution. The fact that geospatial information only detects physical signs of tension or a change to a situation is one of its weaknesses, as well as the requirement of experienced staff to interpret and analyse the data coming from this tool. Cyberattacks along the whole production chain of GEOINT, and the lack of knowledge of the potential use of geospatial information and GEOINT products for early warning and conflict prevention, are some of the threats. As discussed above, one of the main recommendations in this area is to ensure that potential users of geospatial products are trained and informed about the potential and capacities that such products have for conflict prevention applications.

2.2 INFORMATION ANALYSIS AND MEDIA MONITORING TOOLS

Analysis of data is a process of inspecting, cleansing, transforming and modelling data with the goals of discovering useful information, suggesting conclusions and supporting decision-making. Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, in different business, science and social science domains.

National governments, multilateral organisations, universities, non-governmental organisations and think tanks have created many different models designed to predict conflict and instability, with a diverse set of methodologies. As an example, the Fund for Peace (FFP), by combining social science techniques with information technology, has produced the
patented Conflict Assessment System Tool (CAST), which the FFP uses annually to elaborate
the Fragile States Index (FSI). Based on comprehensive social science methodology, data from
three primary sources is triangulated and subjected to critical review to obtain final scores for
the FSI. Millions of documents are analysed every year. By applying highly specialised search
parameters, scores are apportioned for each country based on 12 key political, social and
economic indicators (which in turn include over 100 sub-indicators).\textsuperscript{22}

The EU can of course access different open-source databases in order to extract useful
information for its EWS and conflict analysis. However, it appears that, as mentioned in
section 1.2 of this report, the EU EWS uses an information analysis model as a tool for
assessing the global situation with regard to violent conflict in the first step of the early
warning system (risk scanning), the GCRI, developed by the JRC together with experts,
academics and scientific organisations. Based on quantitative indicators, it uses a linear
regression model to calculate the risk and probable intensity of a violent conflict in a country
within one to four years, collecting 25 variables in 5 structural dimensions (social, economic,
security, political and geographical/environmental). It is based on open-source data and is
accessible for anyone to consult. The construction of the GCRI builds on the work of the
InfoRM index, an open-source global risk assessment of humanitarian crisis and disaster,
using an interactive platform for data analysis.

It has to be taken into account that the model for the GCRI only considers the data, so there
is no expert judgement or analysis used in the six-monthly updates of the GCRI. The index is
based on the ‘data in, data out’ principle, so if the source data have errors, are not updated
or are missing, the outcome will reflect that. In its use for a first assessment, it nonetheless
helps with an evidence-based analysis for EU external action towards ‘at risk’ countries.\textsuperscript{23} Yet
the contemporary academic and policy literature on conflict early warning and response
argues for a more people-centred approach.\textsuperscript{24} Perception-based data, i.e. data indicating a
population’s sentiment or reaction towards an event, as well as potential triggering events,
are missing from this kind of information analysis. Furthermore, the GCRI only measures
internal conflict; interstate conflicts are excluded due to lack of data.\textsuperscript{25}

The European Media Monitor (EMM) incorporates software that provides a 24/7 monitoring
of international news. It gathers and filters the information coming from thousands of
different sources and is able to take charge of up to 70 languages. The EMM not only provides
a database for analysts and decision-makers, it is also able to extract key information on each
source and to classify it into more than 500 different topics. The EMM highlights the main
trends in the news by providing real-time statistics. These products are easily available on the
EMM’s website, called News Brief,\textsuperscript{26} displaying the hottest topics discussed in the world
during the last minutes or hours. The image below is an example of what can be found on the

\textsuperscript{22} See \url{http://fsi.fundforpeace.org/methodology}, last accessed on 3 November 2016.
\textsuperscript{23} See \url{http://conflictrisk.jrc.ec.europa.eu/}.
\textsuperscript{24} Emmanuel Letouzé, Patrick Meier and Patrick Vinck, “Big Data for Conflict Prevention: New Oil and Old Fires”,
Institute, New York, April 2013, p. 7.
\textsuperscript{25} See \url{http://conflictrisk.jrc.ec.europa.eu/Methodology}, last accessed on 10 November 2016.
\textsuperscript{26} See \url{http://emm.newsbrief.eu/NewsBrief//web/html/EMMAlertsHelp.htm}, last accessed on 10 November
2016.
News Brief. On the left side there are various filters that can be applied in order to quickly find information. Each curve of the graph corresponds to a specific topic and highlights the evolution of its presence in the news during the last hours. The headlines and latest information are presented as shown in Figure 6 below.

Figure 6. Example graph from EMM.NewsBrief.eu


EMM’s applications are also available on all mobile devices. Updated every ten minutes, this tool allows analysts and decision-makers to be up to date with the latest events and developments at any time. This is particularly helpful during crises that require effective monitoring. In addition to News Brief, the EMM has two other web platforms: News Explorer,27 which presents a summary of the most recent and main topics, but also finds further automatically derived information and lists of related persons and organisations; and MediSys,28 which stands for ‘Medical Information System’, which only displays articles related to public health. It is unclear if the EMM is actually used in the EWS and conflict analysis; however, it appears to be a useful instrument, especially combined with other early warning tools such as the GCRI and other technologies discussed in this report.

To conclude, the information analysis and media monitoring tools developed by the JRC take into account social, economic, political, security and environmental factors, extracting key information from thousands of different sources. The systems are frequently updated and are open to everybody. The EMM is also a useful tool for following the latest news and developments around the world. The GCRI can be a valuable tool for scanning potential areas of conflict, giving evidence-based data and structural indicators. The main weakness of the system is that it is based on ‘data in, data out’; if the data source is erroneous or if data are missing, this will be reflected in the output. There is no expert judgement or analysis of the data, as the system uses a quantitative method based on data processing. Nevertheless, it

can be very useful combined with other tools and methodologies for completing an analysis of the risk of conflict in a country (see Figure 7).

**Figure 7. SWOT for information analysis and media monitoring tools**

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Give an evidence base, quantitative global view of potential risks of conflict (GCRI)</td>
<td>- Data in, data out; only based on existing data, and if the source data have errors, are not updated or are missing, the outcome will reflect this (GCRI)</td>
</tr>
<tr>
<td>- Take into account social, economic, security, political and environmental variables (root causes of conflict)</td>
<td>- There are no perception-based or triggering events data included (GCRI)</td>
</tr>
<tr>
<td>- Extract key information from thousands of different sources</td>
<td>- No qualitative analysis of the data provided by these tools</td>
</tr>
<tr>
<td>- Frequently updated (EMM)</td>
<td>- Only includes internal conflict risk indicators (GCRI)</td>
</tr>
<tr>
<td>- Ease of use and open to everybody</td>
<td></td>
</tr>
</tbody>
</table>

**Opportunities**

- Leading academic and scientific organisations and experts are part of the methodology reference working group (GCRI)
- Combination with qualitative analysis

**Threats**

- Lack of human resources to maintain, update and extract information from these tools
- Accuracy of data, sometimes less 'exciting' data are missing or are not provided, which can be crucial for an accurate outcome (GCRI)
2.3 HORIZON 2020 TECHNOLOGICAL SUPPORT IN EU EARLY WARNING AND CONFLICT PREVENTION

Some projects developed within the framework of Horizon 2020 could also improve the conflict prevention and early warning processes of the EU. This section discusses in more detail the thematic focus of each of these projects.

The Reaching Out project (“demonstRation of EU effective IArge sCale tHreat and crlisis maNaGement OUTside the EU”) proposes an innovative multidisciplinary approach to conflict prevention, based on the development of a collaborative framework, with distributed platforms of functional services, and 78 new connectable and interoperable tools.

EU-CIVCAP (“Preventing and Responding to Conflict: Developing EU CIVilian CAPabilities for a sustainable peace”) will provide a comprehensive, comparative and multidisciplinary analysis of EU civilian capabilities for external conflict prevention and peacebuilding in order to identify “the best civilian means to enhance these capabilities”. Several deliverables, including this one, examine in more detail the role of technologies in conflict prevention and peacebuilding as well as identify capability shortfalls in this area.29

For its part, WOSCAP (“Whole of society Conflict Prevention and Peacebuilding”) is a project aiming at enhancing the capabilities of the EU to implement conflict prevention and peacebuilding interventions through sustainable, comprehensive and innovative civilian means.30 Among other things, the project will investigate opportunities, barriers and ethical dilemmas presented by the use of ICT in order to assess EU capabilities and provide a more complete picture of technology needs and how these can serve the operational goals of the EU.

The CIVILEX (“Supporting European Civilian External Actions”) project results will identify, characterise and model the communication and information systems in use among EU civilian missions, understand stakeholder requirements and provide possible solutions to meet them by a future interoperable situational awareness, information exchange and operational control platform.31

iTRACK (“an integrated system for real-time TRACKing and collective intelligence in civilian humanitarian missions”) will provide an integrated, intelligent real-time tracking and threat identification system to improve protection of responders and assets, and provide information management and logistics services, such as real-time information updates and analyses as well as navigation, routing and scheduling.32

Several of the above-mentioned projects might lead to further developments of pre-commercial procurement projects, also funded by the Horizon 2020 framework programme, for example CIVILEX, as seen above. Consequently, it is very important to get effective support from users as well as the involvement of institutional actors, as these projects are designed

to improve technological capabilities and bridge gaps in crisis management, including early warning and conflict prevention.

The SWOT analysis shows that the technical support from Horizon 2020 projects can facilitate a comprehensive, comparative and multidisciplinary analysis and development of EU capabilities in this area (see Figure 8). Horizon 2020 projects take into account user requirements in various policy areas of the EU and bring together key actors in the private and public domains to address new technologies. The weaknesses identified include the complexity of financial rules and agreements, which could discourage smaller organisations, structures and innovative small and medium-sized enterprises (SMEs) from participating in a project, and in some cases the formation of very big consortia make it difficult to manage a project in working to reach the expected outcomes. Nevertheless, among the opportunities are the support received from users and institutional actors, and the potential development of new tools and services for early warning, conflict analysis and prevention. The threats identified are the risk that the project results are not endorsed by decision-makers or the industry, and thus remain in the ‘scientific community’. Another threat is that the users are not fully involved in the projects, with the result that the project outcomes do not reflect their requirements.
Figure 8. SWOT for Horizon 2020 technological support

**Strengths**
- Enables a comprehensive, comparative and multidisciplinary analysis and development of EU capabilities
- Collects user requirements in the various EU policy areas, including CFSP/CSDP and external action
  - Provides multidisciplinary and new approaches to conflict prevention
- Brings together the key actors in the private and public domains to address new technologies and tools to support EU policy
  - Supports the development of EU flagship programmes

**Weaknesses**
- Very big consortia can be difficult to manage in working to reach the expected outcomes
- Results from capability development projects do not always lead to new tools and applications, particularly in the absence of sustainable funding
- Complexity of financial rules, reporting and consortium agreements could discourage innovative SMEs and smaller structures from participating in a project

**Opportunities**
- Support from users and institutional actors
- Development of new tools and services for conflict prevention and conflict management
  - Development of pre-commercial procurement is an asset for facilitating the emergence of new technologies and tools

**Threats**
- Project results are not endorsed by decision-makers or industry and remain in the 'scientific community'
- Users are not engaged in the projects and project results do not reflect their requirements (technology push)
2.4 INFORMATION AND COMMUNICATION TECHNOLOGIES

New technologies, such as mobile phones and smartphones, and the incorporation of digital social media in our daily lives are changing how and when we learn about events and how these are communicated. Today, 95% of the global population lives in an area that is covered by mobile networks, while mobile broadband networks (3G or above) reach 84% of the global population. Hence, the sources of information are multiplying and becoming multi-directional, stemming from the classical top-down channels, from state and governmental-influenced information sources, as well as from a bottom-up flow of information from individuals and from actors at the grassroots level. Allan Dafoe and Jason Lyall call this a democratisation of ICT, and suggest that we are standing at the threshold of an ICT-driven transformation of politics that will rival the introduction of earlier technologies, such as the telegraph, newspaper, radio and television.

Figure 9. Mobile network coverage and evolving technologies

Note: LTE – Long Term Evolution; a standard for high-speed wireless communication for mobile phones and data terminals.
Source: International Telecommunication Union.

These changes in ways of communicating events put greater responsibility on the consumer to be able to classify and sort the flow of information with a critical mind. New technologies allow information and news to reach a large amount of the population faster, which on the one hand raises the accountability of a state towards its citizens, while on the other hand they...

---

become the perfect instrument to spread propaganda and false information fast and efficiently.

An example of how these technologies can be used to influence society is illustrated by the project “Political information technology and political Islam”, carried out by the University of Washington, which analysed the use of mobile phones and social media in the North African countries touched by the events of the Arab Spring. The project showed evidence that “suggests that social media carried a cascade of messages about freedom and democracy across North Africa and the Middle East, and helped raise expectations for the success of political uprising”. Data for the project came directly from immense digital archives the team built over the course of several months. The research included data about technology use and political opinion from before the revolutions. It assembled data about blogging in Tunisia one month prior to the crisis in that country, and had special data on the link structure of Egyptian political parties one month prior to the crisis there.35

In view of these events and the decisive influence that mobile phones, smartphones and social media had in creating a sphere of political organisation and debate, these tools should be considered useful for the prevention of violent conflict by various means. The most evident use would be the collection of better data to feed the Conflict Early Warning System.36 These tools would also allow researchers, along with early warning and conflict prevention actors to access perception-based data, something that the information analysis tools presented in the section above are lacking.

Software such as Frontline SMS collects data through SMS or smartphones (Magpi, KoBoToolbox) and captures social media data (Geofedia). For instance, Ushahidi, an open-source software platform for information collection, visualisation and interactive mapping, was originally created in the aftermath of the Kenyan presidential elections in 2007 with the purpose of collecting eyewitness reports of violence communicated by email and SMS, placing them on a Google map. The organisation uses the concept of crowdsourcing37 for social activism and public accountability, serving as an initial model for what has been coined ‘activist mapping’ – the combination of social activism, citizen journalism and geospatial information. Ushahidi offers products that enable local observers to submit reports using their mobile phones or the Internet, while simultaneously creating a temporal and geospatial archive of events. The software has since been used in various settings, ranging from humanitarian crises to natural disaster management.38

Mobile phones and social media are also used to alter a prevailing discourse and to spread alternative narratives. This process could be applied to conflict prevention and peacebuilding in order to create an alternative discourse enabling the turn of a situation away from tension

35 O’Donell (2016), op. cit.
37 Merriam Webster gives the following definition of crowdsourcing: “the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers” (merriam.webster.com/dictionary/crowdsourcing).
38 See https://www.ushahidi.com/, last accessed on 15 November 2016.
and the set-up of a dialogue for peace.\textsuperscript{39} As shown in the section below, Big Data applications for the analysis and extraction of information from ICT can further expand the opportunities for enhanced early warning and conflict analysis (as well as for conflict prevention in general). However, the digital divide\textsuperscript{40} should not be overlooked when talking about the opportunities and applications of ICT for early warning and conflict analysis, and data extraction and analysis of ICT data also provokes concerns regarding personal privacy and data protection.

The EU does not have a policy on the use of ICT for peacebuilding, conflict early warning or conflict prevention. Still, the very recent Council Conclusions on “Mainstreaming digital solutions and technologies in EU development policy” call for digitalisation to be properly mainstreamed “across all policy areas, including the EU’s development and foreign policies, while addressing cyber challenges and assuring promotion and protection of human rights, including privacy, data protection and freedom of expression”.\textsuperscript{41} More importantly for the EWS and conflict analysis, the “Council insists on the importance of using ICT as an enabler for sustainable development, inclusive growth and inclusive societies. To this end, the Council encourages the Commission to develop its capacities in this regard and the High Representative of the Union for Foreign Affairs and Security Policy to raise awareness at headquarters level and in country delegations.”\textsuperscript{42}

The Council also calls for the rapid launch of pilot initiatives in selected priority areas, including support for formulating appropriate policies and strategies for digital development.\textsuperscript{43} These conclusions should open up many possibilities for improvement and prioritisation of ICT when it additionally comes to early warning and conflict analysis.

It is nonetheless unclear the extent to which ICT is used in the collection of information for the EWS, at which stage and by whom. In principle, EU delegations, providing information and input to the EWS and the conflict analysis process, could use ICT for the collection of information in-country. Furthermore, it is possible that civil society working in conjunction with the delegations and the different EEAS services with regard to early warning, conflict analysis and conflict prevention are using different software, smartphones and other ICT in their work. Nevertheless, at the time of writing this report (December 2016), there does not appear to be a systematic and direct use of ICT for early warning and conflict analysis at the EU level. For instance, out of 292 projects funded by the instrument on contributing to stability and peace, only 12 have an ICT component and most of these only focus on the media in general, including radio, with only 1 project specifically having reference to ICT.\textsuperscript{44}

\textsuperscript{39} Kahl and Puig Larrauri (2013), op. cit., p. 5.
\textsuperscript{40} The digital divide entails economic and social inequality with regard to access to use of, or impact of information and communication technologies; see for example “ICT Facts and Figures 2016”, International Telecommunication Union (available at http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx).
\textsuperscript{42} Ibid. p. 7.
\textsuperscript{43} Ibid. p. 7.
As seen in Figure 9 above, ICT tools are widely used for human communication (mobile phones, smartphones, the Internet and software) through which a huge amount of data can be extracted and analysed in order to monitor an event, get perception-based knowledge or engage and create common spaces for social and political dialogue. Even though they do not figure among the current tools for the EU’s early warning and conflict analysis processes, the Council Conclusions on mainstreaming digital solutions and technologies open a door to its future inclusion in the EU’s crisis management structures. At the same time, the analysis here notes that the utilisation of such data for extracting information would need to carefully consider issues of personal and digital privacy, and data protection.
**Figure 10. SWOT for ICTs**

**Strengths**
- Almost at worldwide connectivity (mobile connection and mobile broadband networks)
- Real-time connections
- New spaces for political dialogue and organisation
- Possibilities for information sharing
- Collection of data since ICT habits are traceable (SMS, social media usage) making it possible to collect perception-based data
- Software for data analysis and organisation, data fusion

**Weaknesses**
- Digital human activity produces a large amount of unstructured data
- Digital divide

**Opportunities**
- Raised awareness of the influence of ICT in our society and more specifically on conflict early warning and conflict analysis
- Software for data analysis and organisation, data fusion

**Threats**
- Intrusive if personal privacy and data protection are not respected
- Adverse usage of ICT
- Cyber threats
2.5 BIG DATA

Big Data refers to an accumulation of data that is too large and complex for processing by traditional tools for database management.\(^{45}\) However, as mentioned earlier, it is crucial to distinguish between Big Data as a field of practice and big data as data.

As a field of practice, Big Data refers to Big Data analytics, i.e. methodologies leveraging advanced computing techniques as well as the actors and institutions using them to gain insights for decision-making purposes.\(^{46}\) As data, the big data is commonly characterised by five key attributes, the so-called 5 Vs: volume (a great amount of data), variety (diverse data from multiple sources), velocity (a rapid influx of the data stream), veracity (uncertainty of the data) and value (information extracted from the data).\(^{47}\)

Big Data technologies can be used for processing data faster as well as for extracting knowledge (analysing) data in a distributed manner. Big Data technologies and analytics can be applied to any of the tools for early warning and conflict analysis discussed in this report, except perhaps for the information and communication exchange tool, due to its classified character. Concerning geospatial information, Big Data can facilitate the access to huge data sets (imagery), speed up the processing and assist in their storage. This would enable the access and processing of the large number of images that are or will be provided by the Copernicus Sentinels and future microsatellites. By the end of 2016, the Sentinels are expected to produce more than 6 terabytes of data per day, open and free of charge as per its data policy. It can also be applied to the analysis of satellite imagery in order to perform statistical analysis and extract information from time series of Earth observation imagery. Big Data technologies are also more and more related to data fusion: the integration of data and knowledge from sources, which is also useful for the elaboration of GEOINT products.

In the case of analytical tools, traditional databases could be replaced by Big Data systems, by integrating different data sources, extracting and analysing information from endlessly more data than a traditional database management tool is capable of. ICT technologies are probably those that are going to benefit the most from Big Data technologies, since they allow for the access, classification, fusion, extraction and analysis of massive streams of complex real-time data that are produced daily by mobile phones, smartphones, the Internet and social media. For actors dealing with early warning and conflict analysis, Big Data would make it possible to get a quick overview of complex situations with inputs from various sources and data sets, to


\(^{46}\) Letouzé, Meier and Vinck (2013), op. cit., pp. 8-9.

\(^{47}\) Ibid., p. 10.
build data patterns and do change detection. Big Data could provide the perception-based data that is not offered by tools such as the GCRI.

Emmanuel Letouzé, Patrick Meier and Patrick Vinck have also shown how Big Data could help reveal key insights into the drivers, triggers and early signs of violent conflict in order to support and improve conflict prevention initiatives. They have coined the concept of ‘Big Data for Conflict Prevention’, built on the application of Big Data for the purposes of development put forward by the UN Global Pulse initiative, and have identified three categories of big data for conflict prevention:

1. “digital breadcrumbs”, i.e. traces of human actions picked up by digital devices, or the digital translation of human actions (making a phone call, making a purchase, online research, sending a tweet, updating a Facebook profile or posting a blog);
2. open web data (social media, blogs, online news, etc.), most of which is unstructured; and
3. remote sensing data using satellite imagery.

Furthermore, Big Data may serve the following objectives in conflict prevention:

1. early warning, i.e. the early detection of anomalies in how populations use digital devices and services, which can enable faster response in times of crisis;
2. real-time awareness, i.e. how Big Data can paint a fine-grained and current representation of reality, which can inform the design and targeting of programmes and policies; and
3. real-time feedback, i.e. the ability to monitor a population in real time makes it possible to understand where policies and programmes are failing and make the necessary adjustments.

However, to benefit from Big Data technologies and analytics and to set up a Big Data system for conflict prevention or early warning, appropriate expertise is necessary. Expertise in Big Data architecture and expertise in the field of the subject to which Big Data technologies and analytics will be applied is also crucial. With the constant inflow of real-time big data, a completely different approach to integrating and communicating the information extracted by Big Data is required as well. This could be a challenge for some organisations and could lead to the remodelling of previous decisions, plans and strategies. If an organisation is not used to handling data at a rapid rate, it could lead to incorrect analysis, which could cause larger problems. Other caveats of Big Data are the protection of personal data and personal privacy. Big Data raises the challenge that, while extracting information from an incredible

---

48 Change detection when applied to remote sensing techniques refers to the process of identifying differences in the state of land features by observing them at different times. More generally, change detection also includes the detection of anomalous behavior (of a statistical pattern for example).
49 Ibid., p. 4.
50 Global Pulse is a flagship innovation initiative of the United Nations Secretary-General on big data. Its vision is a future in which big data is harnessed safely and responsibly as a public good (www.unglobalpulse.org).
51 Letouzé, Meier and Vinck (2013), op. cit., p. 11.
amount of data sources, this information and the analysis of it should not violate privacy and data protection rights. In relation to this, the Commission adopted the Communication on the data-driven economy as a response to the European Council’s Conclusions of October 2013, which focused on the digital economy, innovation and services as drivers for growth and jobs and called for EU action to provide the right framework conditions for a single market for big data and cloud computing. In addition, the Horizon 2020 programme has ongoing projects on Big Data, for example BigDataEurope (“Integrating Big Data, Software & Communities for Addressing Europe’s Societal Challenges”) This project aims at evaluating possible tools that could improve the operational capacity for the timely and efficient management of extremely large and complex data sets.

The EU EWS and its conflict analysis process would most certainly benefit from Big Data as described in sections 1.2 and 1.3. A Big Data system for conflict prevention fusing (integrating) different data sources and types, classifying them while constructing statistical patterns, based not only on data sources like those used by the GCRI, but also on data from ICT, would on the one hand facilitate the work of the EU’s conflict prevention structures, while providing better data. On the other hand, the question regarding whether the current organisational and decision-making structure of the EU would be able to follow the pace of the information obtained from such a system remains. Moreover, the digital divide (the economic and social inequality with regard to access to, use or impact of information and communication technologies) and gender-related issues should be taken into consideration while analysing data obtained from ICT, since the obtained data will most probably to a higher degree represent the urban, male population.

In conclusion, Big Data has the widest possible application of the tools discussed in this report. Big Data can help speed up and facilitate the processing of huge data sets of satellite imagery that new generations of satellites will provide (Sentinels and microsatellites), improve the analysis and create statistical patterns out of unstructured data from ICT. Furthermore, it could serve as a tool for conflict prevention (including early warning and conflict analysis) by constructing an integrated system combining and integrating different tools and data from different sources in order to provide Big Data for conflict prevention, which in turn would provide early warning, real-time awareness and real-time feedback. Big Data might, however, challenge an organisation such as the EU, which will probably have to change its current IT architecture, data handling policy and data analysis. If the large amount of data that can be extracted by Big Data analytics is not correctly handled or analysed, it is likely to have a negative impact on the organisation.

54 See https://www.big-data-europe.eu/about/.
2.6 INFORMATION EXCHANGE TECHNOLOGIES FOR EARLY WARNING AND CONFLICT ANALYSIS OF THE EU

As can be seen, the EU EWS and conflict analysis are based on strong cooperation among multiple actors and agencies. The recent Global Strategy for Foreign and Security Policy highlighted the necessity to improve the interoperability between EU agencies. For example, Terri Beswick has identified various problems regarding internal communication, such as different lines of reporting within the EWS and conflict analysis structures.\(^{56}\) She noted that “each EU in-country actor appears to have their own reporting line to Brussels” and that information transmitted is not being automatically shared with the relevant actors within the EWS. Furthermore, she highlighted that there are “outstanding technical obstacles that undermine cooperation and information- and analysis-sharing between departments”,

---

notably encryption incompatibility between the different teams and sections within the EEAS, EU delegations and other actors in the EWS structure.\textsuperscript{57} This analysis was produced in 2012, but these issues still persist. The aforementioned difficulties can easily be understood by looking at the architecture of the EEAS classified systems. The EEAS is using a collection of classified systems inherited from two main sources: the Commission and the General Secretariat of the Council, with different actors within the EEAS using different classified systems.\textsuperscript{58} The EUMS, IntCen and the Crisis management and planning directorate (CMPD) directorates use a classified EU system called SOLAN. The EU Ops Wan is a permanent EU-SECRET network linking the Operational Headquarters and Force Headquarters in the EU Member States to the EU SatCen in Torrejón de Ardoz, Spain, and to the EUMS headquarters in Brussels. From Brussels, the system feeds the SatCen products further to other services, e.g. IntCen, via SOLAN. The EU Ops Wan network was initially intended for the planning of EU military operations and offers email, a collaborative tool (CAMÉO) and some video teleconference functionalities.

INTELLAN is the system used by the military intelligence, whereas the system used by the civil intelligence is SINTCENLAN. The EEAS headquarters and designated delegations have a secret EU system called CIMS, and the civilian CSDP missions have access to DEUS and its mobile extension NOMAD (systems stemming from the Commission). This multiplicity of systems is of course an obstacle to information sharing, which is a necessity for conflict prevention. Moreover, all of these systems are outdated, going back to 2003 and 2008 at the most recent. Consequently, there is a crucial need to replace these systems with a modern and centralised one.\textsuperscript{59}

It is to be hoped that this issue will be addressed by the EC3IS (EEAS Corporate Classified Communication and Information System) programme. The EC3IS will be a common platform protecting classified information used by the EEAS services. It will replace the above systems currently in use, integrating all functions that already exist, adding secure multimedia services as a common service. Its implementation will lead to better security for classified information and to greater efficiency in interagency collaboration. Some dedicated services will still exist, especially for the EUMS, but common services will include an electronic directory, office automation tools, email services (including electronic signature and calendar sharing tools), telephony via voice over IP (VoIP) functionality, videoconferencing in end-to-end and multi-point modes, an archiving and document management system, collaborative tools, a forum and chat. Nevertheless, although the initial steps of its implementation began during the first part of 2016, it is not yet operational.\textsuperscript{60}

In sum, in the case of information exchange technologies, the weaknesses seem to overshadow their strengths (see Figure 12). While there are networks for information exchange within the EU structures dealing with early warning and conflict analysis, they are highly fragmented, only connecting certain actors. The different systems seem to be

\textsuperscript{57} Ibid., p. 12.
\textsuperscript{59} Ibid., p. 5.
\textsuperscript{60} Ibid., p. 9.
outdated, dating back to the years 2003 and 2008. Still, EU institutions seem to be aware of these weaknesses, since a new system, EC3IS, is currently in its implementation phase. The EC3IS is a common platform for classified information, linking the different services within the EEAS. The support from various projects under Horizon 2020 also provides a potential opportunity for improvement in this area.

*Figure 12. SWOT for information exchange technologies*

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Networks for information exchange exist and are interlinking EU actors</td>
<td>- A fragmented system, with no common EU system</td>
</tr>
<tr>
<td>- The EU is developing cybersecurity capabilities to protect its infrastructure</td>
<td>- Low interconnectivity between different actors, services and divisions</td>
</tr>
<tr>
<td></td>
<td>- Outdated systems</td>
</tr>
<tr>
<td></td>
<td>- Information exchange capacities and effectiveness are often based on human relations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Creation of a common platform for classified information (EC3IS) will enhance the interagency communication and information exchange</td>
<td>- Cyberattacks</td>
</tr>
<tr>
<td>- Support from Horizon 2020, e.g. CIVILEX, Reaching Out and EU-CIVCAP</td>
<td>- Financial constraints</td>
</tr>
</tbody>
</table>
CONCLUSIONS AND RECOMMENDATIONS

As set out in this deliverable, the EU has created an EWS and conflict analysis structure with quite a few technological tools to support these activities. Information collection seems to come mainly from the SIAC and EU delegations, without clarity on the technological means through which EU delegations collect and extract information in-country. At the institutional level, the main tools used are Earth observation geospatial information – probably already ingested in the information produced by the SIAC – and the GCRI. By contrast, the systematic use of ICT for obtaining information, and Big Data to process and analyse this information, has not been incorporated into the EU EWS and the conflict analysis structure so far. However, recent Council Conclusions call for the mainstreaming of digital solutions and technologies in EU development and foreign policies, which could accelerate the possible use of ICT for early warning and conflict analysis. Ongoing EU projects on Big Data could also open further the possibility of its application in the conflict prevention domain (including the EWS and conflict analysis). Yet, technological applications and their use should be analysed against the institutional capabilities of the organisation and the policies they are supposed to support. New technologies such as ICT and Big Data could present great opportunities for the enhancement of EU early warning and conflict analysis capabilities, but they also raise the question of how the complexity of handling such tools will be tackled by the relevant EU institutions.

This report has also shown the lack of a unified system for information exchange, with almost every policy area and service having its own classified system (civilian, military, intelligence, etc.). Given the lack of interconnectivity both on a technological level and on a human as well as physical level – as the EU’s conflict prevention structures are based in different premises – good personal contacts and cooperation between different actors and services, willing to share information and cooperate, are key conditions for a smooth and effective exchange and sharing of information among the various Brussels-based bodies and EU delegations. At an organisational level, there is also a lack of knowledge and awareness of the available technological tools, their usability and how to best combine them for effective early warning and conflict analysis.61 Despite the implementation of a comprehensive approach of the EU, the need to enhance the interconnectivity between different services in order to avoid duplication and isolation, and to enhance the capacities and performance of the EU could be improved further.

Knowledge of the tools at hand is additionally crucial for assuring their optimal performance. As an example, the EU SatCen can provide imagery intelligence to support the early warning and conflict analysis of the EU, but it is up to the service or institution tasking the SatCen to ask for such a product and it is the final user who assures that such a product is used to this end. To achieve this, greater knowledge and awareness within the different institutions of the support that the EU SatCen can provide would be beneficial.

Another important question raised is how the EU, by adding more technologies, would practically benefit from them. Based on the findings of this report, it could be argued that the use of new technological tools would improve the EU’s early warning and conflict analysis by

---

providing more and better information faster, but the question remains as to whether this would enhance the (early) response of the EU. Terri Becker notes that “the speed of decision-making and implementation of responses is noted as a constraint to EU potential for early response to conflicts”.\textsuperscript{62} In other words, will the integration of new technological tools reduce the gap between early warning and early response?

To respond to the different shortcomings highlighted by this report, it can be recommended that the EU envisage the actions outlined below.

1. **Reflect on how new technologies such as ICT and Big Data could be added, in a sustainable manner, to the existing technological tools for early warning and conflict analysis.**

   The EU may wish to study how to make the best use of ICT and Big Data for early warning and conflict analysis. To do so, it could consider incorporating the possibilities of ICT and Big Data as applied to EU external action, including conflict prevention, in the next calls for Horizon 2020 projects and beyond.

2. **Update, mainstream and coordinate the various capacities and their use within different services dealing with conflict early warning and conflict analysis, in order to bridge gaps, improve interconnectivity and avoid duplication.**

   An updated and unified information exchange system is crucial for smooth communication, coordination and interconnectivity between actors dealing with early warning and conflict analysis at the EU level. Furthermore, the use of different technologies already available and the introduction of possible new tools should be mainstreamed at the organisational level to avoid duplication and isolation.

3. **Properly familiarise staff involved in the early warning and conflict analysis cycle with the available tools.**

   The EU should raise awareness and knowledge of the available technological tools, ensure their full use and understanding of how to best combine them for effective early warning and conflict analysis, by providing suitable training of its staff members.

4. **Assure that technological tools for early warning and conflict analysis are aligned with EU policies on conflict prevention and vice versa.**

   Finally yet importantly, the level of performance and usability of the tools studied in this report should go hand in hand with the policies that they are expected to support. In this regard, EU-CIVCAP DL 3.2. highlights that there is a positive trend within the EU institutions to mainstream conflict prevention. Yet, this has been accompanied neither by a common understanding among policy-makers of what conflict prevention entails in practice nor by a common view on what conflict prevention is or what should be done by whom.\textsuperscript{63} Hence, the effective use of technological tools for EU conflict prevention (and more precisely early warning and conflict analysis) would require a common agreement and a common view on how the EU should carry out and promote conflict prevention beyond its borders.

\textsuperscript{62} Beswick (2012), op. cit., p. 13.

REFERENCES


