ENGAGE

Working Paper Series
No. 10 | June 2022

Developing Assessment Criteria for Security and Intelligence Cooperation in the EU

Viktor Szép, Ester Sabatino & Ramses A. Wessel

ENVISIONING A NEW GOVERNANCE ARCHITECTURE FOR A GLOBAL EUROPE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 962533.

Executive Summary

This working paper proposes a set of assessment criteria for security and intelligence cooperation at the EU level and presents the limits that prevent more effective cooperation in this field. The research team conducted interviews with experts and officials involved in this work, which lends the report rare insights into the area of security and intelligence cooperation. The working paper first provides a summary of the current institutional architecture and presents an analysis of the main bodies involved in the provision of analysis, early warning and situational awareness at the EU level, like the Satellite Centre, or the Intelligence and Situation Centre and the EU Military Staff Intelligence Directorate working under the Single Intelligence Analysis Capacity. Moreover, this paper discusses matters relating to the EU's Area of Freedom, Security and Justice (AFSJ) and their relationship with external security. Since cooperation in this field also occurs outside the EU institutional framework, it considers other relevant European frameworks on intelligence cooperation and cooperative agreements with non-EU actors.

For More Information

EsadeGeo-Center for Global Economy and Geopolitics
ENGAGE
Avenida Pedralbes, 60-62
08034, Barcelona
Email: marie.vandendriessche@esade.edu

engage-eu.eu @ENGAGE_Europe ENGAGE_Europe

Table of Contents

1 Introduction

In the European Union (EU), cooperation in security and intelligence matters has always been a significant challenge. Although the EU's Common Foreign and Security Policy (CFSP)[1] would greatly benefit from more shared resources and capabilities, Member States have often been concerned about exposing methods and sources, being deceived or loosing national autonomy in intelligence matters. The fear of sharing information explains the dominance of the individual Member States rather than the collective EU in intelligence matters: most of the competences and capabilities to collect and analyse sensitive pieces of information are kept by EU capitals and are considered central in the maintenance of national security. Apart from legal competences, sharing also requires mutual trust and a similar understanding of the main security threats. Given the differences between EU Member States in terms of their national approaches to security and defence, their relations with third states, their historical perspectives on security challenges and their intelligence traditions and cultures, it seems sometimes particularly difficult to harmonise 27 views on matters related to foreign, security and defence policy.

However, despite the reservations of Member States that further integration in intelligence matters may threaten their core national interests, in the last decades there have been some steps to further strengthen cooperation in this field. Indeed, the EU has developed a number of capabilities to collect and analyse information, including the potential to gather imagery and geospatial intelligence (EU Satellite Centre), information on international crime (Europol and Frontex), cyberthreats (CERT-EU, ENISA), open source and social media analysis (EU Joint Research Centre and EU Intelligence Analysis Centre, INTCEN) or information on third states' activities (around 140 EU Delegations). INTCEN and EU Military Staff (EUMS) Int also support EU foreign, security and defence policymaking through the "deliverables" from Member States (Conrad, 2021, pp. 62–63), or the provision of intelligence information, which is given on a voluntary basis. Recent events and tendencies in international relations, such as a more assertive China or Russia's invasion of Ukraine in 2022, are expected to contribute to further intelligence cooperation due to the recognition that the EU's security is threatened in the short and medium term and may also lend urgency to the need to improve the situational awareness.

In this working paper we use the term intelligence to refer to a broad range of activities performed to reach information superiority. According to the type of information collected, it is possible to include signal intelligence (SIGINT), open-source intelligence (OSINT), human intelligence (HUMINT), imagery intelligence (IMINT), geospatial intelligence (GEOINT) or measurement and signature intelligence (MASINT).

[1] See our previous studies on the EU's CFSP and CSDP: Szép, V. & Wessel, R. A. (2021). *Mapping the Current Legal Basis and Governance Structures of the EU's CFSP*. ENGAGE Working Paper; Szép, V. Wessel, R. A., Sabatino, E., Gebhard, C. & Simon, E. (2021). *The Current Legal Basis and Governance Structures of the EU's Defence Activities*. ENGAGE Working Paper.

Table 1: Categorisation of the Types of Intelligence Sources

SIGINT	Data collected from electronic systems, i.e. communication systems, radars, weapons systems
OSINT	Data collected from publicly available data, i.e. radio, news, social media, television, or official reports
HUMINT	Data collected from human sources, either openly, or through espionage
IMINT	Data collected via images, i.e. photographs, radars
GEOINT	Data collected from satellites, drones
MASINT	Data collected from sources that do not fall under SIGINT or IMINT, i.e. radio frequencies

Source: own elaboration

Moreover, according to the type of sources used, it is possible to define an analysis as single source, or multi-/all-source analysis. It can be focused on one or more types of intelligence collection or comprehend a general agreement for the sharing of a specific information, regardless of the way this information is gathered. While intelligence sharing is limited to the deliberate distribution of gathered and analysed intelligence, intelligence cooperation might also involve the production or procurement of necessary information.

The degree of information sharing, and cooperation can vary from topic to topic, and from one framework of cooperation to another. Nonetheless, generally, "States and their national services are reluctant to share sensitive, classified information with international organizations and favour cooperation on a more controllable, bilateral, case-by-case basis. In fact, intelligence is shared only when there is a common threat perception, mutual trust, a demonstrable added value, the right type of diplomatic relationships or a combination of incentives" (Ballast, 2017). The various levels of specificity of the shared information are also a factor to consider when addressing intelligence cooperation. When cooperation occurs at the politico-strategic level, the "strategic information" gathered is usually meant to be used by policymakers and is generally an assessment of foreign policy developments. When turning to the operational level, it entails the sharing of threat assessment information, or information on specific armed forces or non-state actor groups. Lastly, this type of cooperation can occur for the exchange of tactical information relevant for operational investigations or for the performance of a mission/operation (Born, Leigh & Wills, 2015, pp.18–19).

This working paper is structured as follow. First, it offers a brief legal and policy context for EU level security and intelligence cooperation and presents the basic pre-conditions for effective cooperation. It also shows the challenges of multilateral cooperation in this particular area. Then it turns to the EU institutional architecture and shows how different units have developed over time and their current responsibilities in this area. The working paper has a clear external focus but due to the strong synergies between "internal" and "external" security issues, to a certain extent it also discusses matters relating to the EU's Area of Freedom, Security and Justice (AFSJ) and their relationship with external security. With a focus on the

European environment, it also examines institutions or bodies outside the EU framework where cooperation in intelligence matters also takes place, such as the Club of Berne or the Counter-Terrorism Group (CTG). The working paper then presents, mostly based on interview results, the main factors contributing to an effective intelligence cooperation. Finally, based on these findings, it proposes a set of assessment criteria that could be used to evaluate and improve EU security and intelligence cooperation.

2 Methods

The working paper is mainly based on an extensive mapping of existing literature on EU security and intelligence cooperation and, quite exceptionally in this field, on interviews made with officials and experts involved in EU intelligence cooperation. The use of qualitative methods is rare in this field (Arcos & Palacios, 2020). In our understanding, data from interviews with (current and former) intelligence officials are key to gain a better understanding to the logic behind EU intelligence sharing, mainly because the majority of information is inherently "hidden" from third parties, and generally scarce. However, thanks to the involvement of officials and experts, we were able to gather data which otherwise would have been hard to access. We conducted 11 interviews with professionals who work/worked for relevant EU agencies, bodies, directorates, representatives at the EU level, as well as people who work/worked for national security services but who coordinated national inputs with the EU. Further information on their affiliation is not provided due to the very sensitive nature of security and intelligence matters. All our interviewees accepted our request on the condition that their identity would be removed from this paper. Therefore, every interviewee is marked with a "#" (hashtag) sign and a number (for instance, an interviewee can be: #1, #2 and so on).

To analyse our dataset (the interviews) we created several codes that were used to follow similar patterns in the interviews. For example, the notion of "trust" was given a particular code and every time we came across this notion in different interviews – which is key for the establishment of a truly European intelligence – we indicated that "trust" is present in *x* number of interviews. These elements are then embedded within our main text to underpin an argument or to expand existing knowledge. If an argument is made by multiple interviewees, the study indicates, for example, that "there is a widespread belief that (#1, #2 and #4)", implying that three interviewees shared the same understanding of a given topic.

Given that the H2020 ENGAGE project has an overall objective of creating a more effective and sustainable EU external action, this working paper cannot be regarded in isolation from other ENGAGE works. In particular, the assessment criteria were developed in close coordination with ENGAGE Working Paper 9 (Sabatino et al., 2022). It should be noted, however, that given the very limited information available on intelligence matters, the potential number of assessment criteria are limited. The conceptual framework of the working paper followed the suggestions laid down in ENGAGE Working Paper 3 on the understanding of effectiveness, coherence and sustainability of cooperation (Sus et al., 2021).

3 The Limits and Opportunities of EU Intelligence Cooperation: General Legal and Policy Considerations

The creation of intelligence structures within the EU has always represented a significant challenge, despite the potential benefits it can bring to EU external actions. Among these, the collection of additional information contributing to gaining a better situational awareness on ongoing or potential crisis, or a possible reduction of costs related to intelligence gathering are particularly evident.

From a legal perspective, competences in intelligence activities inside the EU are largely in the hands of Member States. Article 4(2) TEU provides that "national security remains the sole responsibility of each Member State". In addition, Article 72 TFEU provides that Title V does "not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security". Article 73 TFEU further adds that it is "open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security". Indeed, as the former Counter-Terrorism Coordinator confirmed: "[y]ou can't get closer to the heart of national sovereignty than national security and intelligence services" (EurActiv, 2005).

To cooperate in this field, a secure management of relevant and/or classified information is particularly important. At the EU level, the securitisation of information follows the basic principles and minimum standards set in the Council Decision 2013/488/EU (Council of the EU, 2013), replacing Council Decision 2011/292/EU. According to this decision, the classification of information at the EU level follows the categorisation presented in Table 1.

Table 2: Types of Classified Information in the EU

- TRÈS SECRET UE/EU TOP SECRET is information and material the unauthorized disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of the Member States; - SECRET UE/EU SECRET is information and material the unauthorized disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States; - CONFIDENTIAL UE/EU CONFIDENTIAL is information and material the unauthorized disclosure of which could harm the essential interests of the Union or of one or more of the Member States; - RESTREINT UE/EU RESTRICTED is information and material the unauthorized disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States.

Source: own elaboration

The decision also defines the ways the EU classified information (EUCI) should be managed and shared, how a breach of security should be dealt with, and the cases in which personnel security clearances should be assigned. However, according to #1, #10 and #11, there are some factors negatively affecting the EUCI system, that mainly pertain to outdated IT and physical infrastructures, the very low number of personnel with security clearances, and the procedures to access information classified CONFIDENTIAL or above. Additionally, according to a former official "these regulations are from another time and another world" (#3) and a different system for security clearances is not possible, given the current legal constraints.

In case there is the need to share EUCI with third countries and international organisations, Council decision 2013/488/EU requires the establishment of a framework to do so, that takes the form of a security of information agreement. So far, the EU has signed a total of 17 Agreements on the security of classified information with third countries (Eurlex). Moreover, in the case of third countries' participation in Common Foreign and Security Policy (CSDP) missions and operations, in case of absence of such an agreement, provisions for a secure exchange of information shall be included in the Framework Participation Agreement regulating the third-country contribution to CSDP missions/operations.

In 2021, a total of 255 classified documents were referenced in the Council register, while 564 classified documents were not included in the public register (Council of the EU, 2022c). The non-inclusion of information in the public register means that the originator of the information did not provide the necessary authorisation to include reference to the document. This procedure is allowed by Article 9 of Regulation (EC) No 1049/2001 (Official Journal of the European Union, 2001). Even if the numbers might appear to be high, #11 stated that there is "no tendency in the EU to overclassify relevant information" and that there is a widespread understanding of the necessity to enhance and facilitate access to classified information to relevant persons, bodies and institutions, particularly in the presence of the need-to-know or eventual threat.

Coming to what the EU can do in intelligence, it does not do "spycraft" in a sense that it does not gather secret information held by other states but largely relies on various "deliverables" or voluntary contributions from Member States (Gruszczak, 2016, p. 68). In mid-2010s, former INTCEN director said that "for the moment I do not see real need nor will on the part of the Member States to take any steps towards that kind of integration" (Palacios, 2020, p. 485). Or, as an EU diplomat confirmed, "[t]here's not much appetite for [EU intelligence sharing] since we have difficulties to agree on a common perception and or categorisation of threats" (EurActiv, 2022).

At the very same time, as the Council of the EU (hereinafter: the Council) also recognised, "[t]he aim of preserving peace, preventing conflicts from erupting into violence and strengthening international security is an important element of the external action of the [EU] as laid down in the Lisbon Treaty […]. Preventing conflicts and relapses into conflict, in accordance with international law, is therefore a primary objective of the EU's external action" (Council of the EU, 2011a, p. 1). Despite reservations from Member States and the fear that sensitive data could be misused, the EU has experienced a considerable progress in building an intelligence

community within its institutional framework. After all, as Björn Müller-Wille argued, "sharing knowledge is a first step towards harmonising views, formulating and implementing common policies, and exploiting potential synergies in the fight against new threats" (Müller-Wille, 2004, p. 13). Indeed, the demands for more EU cooperation in this field also results from the increased number of transnational challenges that can be tackled successfully if information and resources are shared in a well-organized and secure structure (Fägersten, 2014, p. 94). Intelligence sharing would also become a more pressing priority if the EU were to become a major security actor. As Eveline R. Hertzberger argued, "the fact that the EU formulates and implements its own security policy means that a credible EU intelligence structure has to be put in place to support this security policy" (Hertzberger, 2007, p. 12). Similarly, in his famous article on capability-expectations gap, almost thirty years ago Christopher Hill already argued that if the EU were to acquire its own foreign policy, it would need, among other things, a single intelligence service (Hill, 1993, p. 317).

One of the pre-conditions for successful international intelligence cooperation is a set of common interests. As confirmed by Stéphane Lefebvre, "[c]lose allies routinely exchange intelligence through various bilateral and multilateral means. But the depth and breadth of these exchanges very much depend on their sharing a common perception of a threat or sets of interests" (Lefebvre, 2003, p. 529). One clear historical example of that is NATO's large amount of intelligence sharing and information activities in the face of the Soviet threats during the Cold War. However, as Lefebvre argued, "common threat perceptions and shared interests necessary to fruitful relationships among intelligence agencies are not sufficient" (Lefebvre, 2003, p. 529). Different intelligence cultures or the lack of trust may complicate or impede (effective) intelligence cooperation. Apart from common understanding of threats, common culture and trust can indeed enhance intelligence cooperation: NATO's Nordic countries (Denmark, Estonia, Iceland, Norway) find intelligence cooperation with non-NATO members Finland and Sweden, "natural and a question of geography, culture, and values […] We speak the same language. We feel closer to each other than most other people […] There is already a very good cooperation between intelligence services in the Nordic countries. It was like this even in the Cold War. There are close contacts at a personal level. It's an issue of trust, of joint interests" (Seagle, 2015, pp. 558–559). Similarly, in the Five Eyes (composed of the US, UK, Australia, Canada and New Zealand), SIGNAL intelligence sharing is facilitated by common language, historical experience and common culture (Seagle, 2015, p. 563).

In accordance with the growing expectations that the EU should play an increased role in global affairs, one does observe a transformation in EU intelligence cooperation, especially after the entry into force of the Lisbon Treaty. The INTCEN and the EUMS INT, working nowadays under the auspices of the Single Intelligence Analysis Capacity (SIAC) in the EEAS, represents a clear sign of integration efforts. The reasons behind these efforts are numerous. Individual information-gathering is relatively costly and sometimes Member States might not have the necessary resources to collect intelligence on all topics, and thus there has been an incentive to cooperate at the EU level (Dijkstra & Vanhoonacker, 2011, p. 544). Also, the effectiveness and credibility of the CFSP cannot be guaranteed without proper information gathering and analysis among EU Member States (Gruszczak, 2016, p. 151). In particular in the area of justice

and home affairs, issues ranging from criminal intelligence early warning to situational assessment of territorial security have been incorporated in the EU. Especially since 11 September 2001, when terrorist activities were increasingly combined with cross-border crime, EU Member States had strong incentives to increase intelligence cooperation. In the face of these shared threats, multilateral cooperation in intelligence matters nonetheless remained a challenge despite regular meetings between counter terrorism units (Hill, 2004, p. 150).

Access to sensitive pieces of information is therefore among the reasons to engage in intelligence sharing and cooperation, as it constitutes a way to gain an advantage. Information superiority can lead to more influence at the international level and may also contribute to conflict prevention. Cooperation with other like-minded states can potentially also be economically beneficial: the price of expensive technologies (such as satellites) may be reduced by a joint acquisition of GEOINT and duplication of capacities may be reduced. Despite these general gains, the reasons for the low level of EU cooperation in the field of intelligence are manifold.

First and foremost, while the existence of common policy objectives may indeed enhance the likelihood of international cooperation in intelligence, states are often concerned about exposing methods and sources, being deceived or losing national autonomy. The disclosure of a country's methods and sources contribute to its vulnerability and sharing information with others is particularly worrying when the retention of information can generate political or commercial advantage for another states. Moreover, states are less willing to share intelligence information if, by sharing it, there is the risk that information will end in the hands of hostile countries, thereby relinquishing information superiority or potentially putting the country itself in danger. The loss of autonomy may also occur when a security policy measure is heavily dependent on others or when a state is involved in activities where it has no interest. Thus, in certain cases, cooperation may simply run contrary to essential state interests.

Second, those Member States having greater resources usually seek to secure special treatment within intelligence communities. The imbalance created by the preferences of these Member States should be accepted by other, less influential Member States. On this point, it is relevant to specify that Member States holding a particularly important information, or with a particular intelligence gathering capacity over a specific topic, are not necessarily those countries with higher intelligence capabilities in general. Therefore, a state, with relatively small intelligence capacity might still provide intelligence on a topic which is particularly relevant from its national perspective.

Third, bureaucratic self-interests may also hamper effective cooperation which can manifest in many different forms: different organisational or professional cultures, or even a resistance by bureaucrats may impede cooperation. Fourth, missing infrastructures can also hamper cooperation in certain areas despite actions are taken to mitigate this problem (Fägersten, 2015, pp. 2–4, 2016, pp. 2–3). Moreover, when receiving an intelligence information, the recipient state may need to verify the information, without having access to the primary source.

In general, the EU leans towards 'soft intelligence' and relies on open sources or information (e.g. social media, diplomatic reports, etc.). 'Hard intelligence', whereby highly skilled agents are involved in covert actions, is forbidden at the EU level. If hard intelligence "deliverables" are nevertheless received by the EU from Member States, these must be properly secured, classified and protected. 'Human intelligence', as a form of open or cover action to possess information from other persons or groups, is not conducted by the EU. During an EEAS mission to Libya in early 2011, some staff members of INTCEN (named SITCEN until 2012) were on location. The former director of INTCEN, Ilkka Salmi, denied the allegations that Centre's staff members took operational related actions and described the presence of INTCEN as only technical support for satellite phones and related services. Director Salmi reiterated at later stages that INTCEN "does not have any intelligence officers anywhere around the world. No operations" (Gruszczak, 2016, pp. 68–77; 78).

Table 3 shows areas of convergence and divergence among EU Member States: on the left-side, agreements have been expected to be concluded, whereas on the right-side issues still divide Member States. Paradoxically, EU intelligence has so far picked up issues that fall in the right column, which in turn has prevented the creation of a common European intelligence. The reason for this paradox is that matters falling in the right column did not compromise valuable sources, the sharing of which is easier due to their less sensitive nature. The challenge is that national intelligence services will certainly rule out possibilities where they would be required to bring pieces of evidence that would run contrary to their own countries' interests (Palacios, 2020, pp. 487–488).

Table 3: Political Preferences of Different EU Member States

Areas of Agreement	Areas of Disagreement
Counterterrorism	Policy toward the Israeli–Palestinian conflict[a]
Counterproliferation	Policy toward Russia[b]
Cybersecurity	Policy toward China
Control of common borders	Enlargement policy
Postconflict stabilization	Transatlantic relations
Support for EU crisis management missions	

Source: Palacios (2020, p. 488)

Internal and external shocks (e.g. terrorist attacks in 2001 in the US, 2004 in Spain or 2005 in the UK, but also following the 2014-16 terrorist attacks in France, Belgium, Germany, etc.) have always revived the question of more effective intelligence cooperation at the EU level. Pre-9/11, the European intelligence community was quite fragmented and communicated with each other in different settings both within and outside the EU institutional framework, including for example the long-standing Club of Berne, Europol or the Western European Union (WEU). The Club of Berne and Europol, to varying extents, were both preoccupied with the fight against terrorism, but barely coordinated their actions on this matter (Fägersten, 2010, p. 505). The vast majority of the intelligence data gathered comes from contributing Member States, with the exception of the SATCEN, that relies on commercially available satellite information.

The European Commission seems to be committed to further strengthening EU powers in that regard. In her 2021 State of the Union speech, President Ursula von der Leyen talked about the necessity to reinforce EU intelligence structures: "we need to build the foundation for collective decision-making – this is what I call situational awareness. We fall short if Member States active in the same region, do not share their information on the European level. It is vital that we improve intelligence cooperation. But this is not just about intelligence in the narrow sense. It is about bringing together the knowledge from all services and all sources. From space to police trainers, from open source to development agencies. Their work gives us a unique scope and depth of knowledge. It is out there! But we can only use that, to make informed decisions if we have the full picture. And this is currently not the case. We have the knowledge, but it is disjoined. Information is fragmented. This is why the EU could consider its own Joint Situational Awareness Centre to fuse all the different pieces of information. And to be better prepared, to be fully informed and to be able to decide" (von der Leyen, 2021).

A further integration of EU intelligence structures is also promoted by some members of the European Parliament. Following President von der Leyen's State of the Union speech, MEP Sánchez Amor advocated to develop the EU's own foreign intelligence services and argued that the Joint Situational Awareness Centre proposed by President von der Leyen may indeed contribute to overcome certain suspicions among Member States. MEP Sánchez Amor has also been working on a pilot project proposal that would allow the Union to increase its information gathering capacity for diplomatic purposes (EurActiv, 2022). But given that the European Parliament has marginal role in the EU foreign, security and defence policy, MEPs can just keep the issue on the agenda and draw EU policymakers' attention to the need of strengthening the EU's intelligence structures.

The willingness to increase intelligence cooperation among EU Member States to reach higher levels of situational awareness and perform better strategic foresight, was also identified in the Strategic Compass, adopted by the Council in March 2022.[2] A better sharing of intelligence among Member States and other non-EU countries and international organisations would also profit the higher success rate of CSDP missions and operations, but the main impeding aspects seems to be the treaty provisions and Member States preference to maintain the status quo.

[2] For further details on the modifications proposed in the Strategic Compass, please refer to section 4.2 EU Intelligence and Situation Centre of this paper.

4 The Institutional Architecture of EU Intelligence Cooperation

As of 2022, European intelligence cooperation entails three main branches: foreign and security policy (the main focus of this working paper), internal security, and law enforcement. From a formal and practical point of view, intelligence support is weakened by the voluntary character of Member States contributions and the impossibility for EU relevant structures to collect primary sources, nor do they have access to raw intelligence material. Nonetheless, activities are also supported by SATCEN which, quite uniquely in the EU, has the capacity to gather primary geospatial data. Intelligence in law enforcement is best represented by the Europol, but it is less integrated in the sense that it mainly supports Member States' individual rather than collective actions. Finally, internal security measures are mostly taken by units that are outside of the EU framework, such as the Club de Berne or the Counter-Terrorism Group (Fägersten, 2016, pp. 1–2).

This chapter will focus on the foreign, security, and defence policy aspects but it will also present all the involved units, mainly because of the increasing nexus between "internal" and "external" of security threats. In fact, it is hard, if not impossible, to artificially separate these areas. Clearly, civilian intelligence can hardly be credible without military intelligence and vice versa. Also, since mid-2000s, counterterrorism is an area where Europol and INTCEN have closely worked together. For a clear understanding, however, the paper will keep the separation of different EU intelligence units but will always draw the attention that nexuses between the different areas of intelligence (civilian-military; internal-external, etc.) exist. As our interviewees also confirmed, the civilian and military intelligence are still often regarded as two separate entities despite equally contributing to the processing of SIAC products. Indeed, civilian and military intelligence are structures that should work together in order to enhance the EU's intelligence capabilities (#4, #6, #10). In addition, sometimes even law enforcement agencies have relevant information to national security and defence (#4).

4.1 European Union Satellite Centre

SATCEN was established in 1992 and inaugurated in 1993 as a body of the WEU. The main reason for its establishment was the realisation that European security lacked intelligence capabilities, especially geospatial information and knowledge. In the early 1990s, SATCEN's main objective was to compile and process commercially available imagery data and provide them to WEU Member States. With the establishment of the ESDP, SATCEN was incorporated in the EU (Gruszczak, 2016, p. 80). The CFSP Joint Action 2001/555/CFSP establishing SATCEN provides that the Centre is "essential for strengthening early warning and crisis monitoring functions within the context of the [CFSP], and in particular of the [ESDP]". According to Article 2 of this Joint Action, its mission is to "support the decision-making of the [EU] in the field of the CFSP, in particular of the ESDP, including EU crisis management operations, by providing, as appropriate, products resulting from the analysis of satellite

imagery and collateral data, including aerial imagery, and related services" (Council of the EU, 2001b).

With the entry into force of the Lisbon Treaty, SATCEN became an EU agency that has continued to support CFSP/CSDP with satellite imagery analysis and collateral data, including aerial imagery and related services (Gruszczak, 2016, pp. 80–81). Council Decision 2014/401/CFSP, as modified by Council Decision (CFSP) 2016/2112, provides that "the HR […] direct[s] SATCEN to provide products or service" to the Member States, the EEAS, the Commission, Union agencies or bodies, certain third states or international organisations. The increasing relevance of GEOINT is referenced in the EU Strategic Compass, which stated that by 2025, autonomous GEOINT capacity should be boosted via the strengthening of the SATCEN. The direct reference to the need to strengthen the EU intelligence-based situational awareness, also through the strengthening of SATCEN budget, personnel, bases, and infrastructures, should be considered a positive development in the view of #9, despite the already close communication with Member States, who "got the message they need to invest increasingly into EU capacity because of the need of a shared situational picture" (#9). Also #2, #3, #10, #11 stressed the importance of the Centre and of an improved satellite imagery data gathering.

From a procedural point of view, the Political and Security Committee (PSC) exercises political supervision and issues political guidance on SATCEN's priorities. The HR/VP gives operational direction to SATCEN and reports every six months to the Council on the implementation of political guidance and operation direction. SATCEN's Board is chaired by the HR/VP or by the HR's representative and is composed of one representative by each Member State, one representative by the Commission and is attended by the Director of SATCEN. They could be joined by the Chairman of the EU Military Committee, the Director General of the EUMS and the EU Civilian Operations Commander. Decisions are taken by qualified majority voting.

On a recommendation from an advisory panel, the Board appoints the Director for a period of three years, which can be extended by two years (Council of the EU, 2014). Located in Spain, SATCEN is staffed by imagery analysts, geospatial specialists and supporting personnel and remains the only EU body to produce original intelligence data (Fägersten, 2015, p. 8; Seyfried, 2017, p. 2). The assigning of the tasking to SATCEN to perform any of its activities can also include the tasking for delivering a service to third countries and/or international organisations. The work programme of the Centre is defined every year and is accompanied with "a draft long-term work programme" (Council of the EU, 2014, Article 9). Nonetheless, as #9 highlighted, the tasking of the Centre to support also non-members requests, or requests from third organisations, is "dependent on Member States willingness" to approve the specific task. The tasking of SATCEN can occur with different timelines. It can foresee a monthly or annual mandate, or, for activities related to contingent situations, the tasking of activities can be assigned on a daily basis (#9).

The work of SATCEN in 2020 was performed by a total of 144 personnel. As Table 4 shows, the total staff number slightly increased during the years, with a predominance of permanent over temporary posts. According to the latest available annual report (SATCEN, 2020), 18

nationalities are represented among SATCEN personnel, leaving nine Member States not represented at all in the Centre. According to #9, Brexit had an impact in terms of loss of experienced staff, but this has been mitigated by the provision of additional personnel and funding from other Member States to cover the former British contribution.

Table 4: Evolution of SATCEN Human Resources in the Period 2014–2020

Evolution of SATCEN human resources 2014–2020								
		2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Posts	Permanent	87	90	90	89	90	90	89
	Temporary	12	25	30	36	43	43	50
Staff	Local	3	1	2	1	1		1
	SNEs	5	5	7	5	7	7	4
	Trainees			3				4
	Total	107	121	132	131	141	140	148

Source: elaboration of data taken from Council of the EU (2019), SATCEN annual reports (2019; 2020)

In the delivery of its products and provision of services, SATCEN shall apply Council Decision 2013/488/EU on the exchange of classified information. With specific reference to the proportion of classified products over unclassified ones, in the period 2014–2019, there has been a preponderance of restricted over unclassified products, except for the year 2017, when the unclassified deliverables outweighed more than 30 percent the restricted category (Council of the EU, 2019, p. 12). It also occurs with respect to any third state or organisation willing to receive SATCEN support: According to Article 15 of Council Decision 2014/401/CFSP they have to satisfy the minimum requirements mentioned in Council Decision 2013/488/EU.

SATCEN's products include geospatial intelligence, satellite imagery analyses, topographic surveys, or briefing notes for situational awareness, early warning and crisis monitoring. However, SATCEN receives data mainly through the intermediate commercial providers since it lacks its own satellite sensors. It also receives collateral materials from open sources and government agencies (Gruszczak, 2016, p. 81). Moreover, Member States who have the capacity to collect their own images and recognise the potential presence of an EU interest in monitoring or collecting further analysis on a certain area, can request SATCEN to do so (#9).

Since 2015, the Centre has contributed to the EU Space Surveillance and Tracking (SST) according to the terms agreed to in the SST Implementing Arrangement of September 2015. Thanks to the 2016 Delegation Agreement signed between SATCEN and the European Commission, SATCEN enlarged its capacity to support EU security and defence policy. The agreement entrusted SATCEN with coordinating the Copernicus Service in Support to EU External Action (SEA) to provide" rapid, on-demand geospatial information for the detection

and monitoring of events or activities outside the European borders that may have implications for European and global security" (Copernicus).

SATCEN products are to be considered an important support for the recipient entities. Once a product or analysis is delivered to the recipient, "they decide how to divide it and use it. Sometimes they request further processes and analysis, some other times they just use the document as it arrives to them" (#9).

The support SATCEN provides to EU missions and operations through the its services to the EUMS, the Military Planning and Conduct Capacity (MPCC), and the Civilian Planning and Conduct Capacity (CPCC), increased over time and more than quintuplicated between 2019 and 2020: in 2020 the services provided to EU missions and operations represented around 17 percent of the total SATCEN services, against a 3 percent portion in 2019 (SATCEN, 2020, p. 30). Nonetheless, the aforementioned 2019 five-year report underlined a general scarce knowledge about SATCEN activities and its potential support in the performance of CSDP missions and operations, which might not have sufficient budget to task SATCEN to provide them with IMINT and GEOINT.

Among the operations to which SATCEN provides support, there is operation EUNAVFORMED IRINI. Its mandate already included the reference to the need to use satellites images. According to the mission's Commander, SATCEN provides "essential element of Operation IRINI as it provides us with the necessary satellite imagery and analysis" and the relevance of cooperation "has been already proved by the detection of illegal activities in some ports and airports in Libya in coordination with the other assets assigned to IRINI (SATCEN), thanks to the provision of 444 reports during 2020 (SATCEN, 2020, p. 32).

In addition to the provision of intelligence analysis and data, SATCEN also works on capability development and on the testing of new technologies and platforms. In this regard, SATCEN cooperates with the EU Commission and profits from funding on R&I initiatives under the H2020 programmes and funding for Copernicus (#9). The centre also cooperates closely with companies (#9) and with the EDA, like in the case of the machine-based algorithms and tools for enriched imagery intelligence exploitation (MATRIX) joint initiative aiming at delivering a study on the possible application of AI solutions in support of IMINT products (SATCEN, 2020, p. 54). Particularly important for the purpose of this working paper, is the training activity SATCEN delivers to national and EU agencies' personnel, as joint training helps in integrating the personnel and in establishing a certain level of trust among experts which might then facilitate the exchange of information or the interoperability of approaches. Given the specificities of the sector, "there are not many institutions that train specifically personnel, so there is a little number of analysts that can be employed" (#9), which highlights the importance of this kind of activities performed by the Centre.

4.2 EU Intelligence and Situation Centre

Since the mid-1990s, the EU has sought to achieve progress in early warning capacities. One of the earliest manifestations was the creation of the Policy Planning and Early Warning Unit

in 1997 when EU Heads of State and Government realised the need of using confidential information in CFSP policymaking. This new unit was established in the General Secretariat of the Council. It was HR/VP Javier Solana's personal think tank which provided policy options for the EU (Hemmer & Smits, 2011, p. 9).

Table 5: The Remit of the Policy Planning and Early Warning Unit

- monitoring and analysing developments in areas relevant to the CFSP;
- providing assessments of the Union's foreign and security policy interests and identifying areas where the CFSP could focus in future;
- providing timely assessments and early warning of events or situations which may have significant repercussions for the Union's foreign and security policy, including potential political crises, and
- producing, at the request of either the Council or the Presidency or on its own initiative, argued policy option papers to be presented under the responsibility of the Presidency as a contribution to policy formulation in the Council, and which may contain analyses, recommendations and strategies for the CFSP

Source: European Parliament (2010)

During the 1990s, the EU increasingly gave priority to analytical intelligence capabilities that are outward looking to support a developing CFSP. The crisis in the former Yugoslavia, in particular, was an incentive for the EU to develop intelligence capabilities that contributed to the establishment of the Joint Situation Centre (SITCEN). The latter took over the task of the Policy Planning and Early Warning Unit after it became operational in 2003 (Aldrich, 2012; Hemmer & Smits, 2011, p. 10).

In 2002, SITCEN was established as the EU's Joint Situation Centre and was attached as a department to the office of the HR/VP within the General Secretariat of the Council. SITCEN was created as a body that "monitors and assesses events and situations worldwide on a 24-hour basis with a focus on potential crisis regions, terrorism and WMD proliferation" (Cross, 2013, p. 389). It was an idea originated from the French, British and German security services (#5). Initially, it started with only seven seconded analysts, one each from France, Germany, Italy, the Netherlands, Spain, Sweden and the UK. They were joined by two diplomats from the Policy Planning and Early Warning Unit, three military officers from the EUMS and a police officer from the police Planning Team (Müller-Wille, 2008, p. 62). SITCEN was not established through the adoption of a (CFSP) Council Decision but rather on the initiative of the HR. It enjoyed political endorsement from the Council without the adoption of a formal legal act or a publicly available document on its mission and tasks (Van Buuren, 2009, p. 12). The lack of legal basis is partly explained by the fact that in the early 2000s all personnel of SITCEN was seconded and therefore it did not formally qualified as an organisation of the General Secretariat. At the same time, SITCEN was understaffed and therefore could not fully deliver the external intelligence support for EU institutions (Müller-Wille, 2004; Norheim-Martinsen, 2012, p. 96). After 9/11, it could, however, contribute on which individuals need to be added to the EU's anti-terrorist sanctions list and could provide further feedback based on open sources and inputs from national intelligence services (Gruszczak, 2016, p. 110). It also contributed to

a confidential early warning document called "the Watchlist" which listed countries where potential crises were expected to erupt (Gruszczak, 2016, p. 130). SITCEN was widely accepted by every Member State given that its products were distributed amongst all Member States irrespective of the number of inputs they provided to the common intelligence community (Norheim-Martinsen, 2012, p. 97). Indeed, nowadays 23 out of 27 Member States participate in the work of INTCEN but all of them receive INTCEN's output, also through the EEAS and the Commission (#1).

Table 6: The Remit of the Situation Centre

- to contribute to the early warning work of the Council and the High Representative;
- to undertake situation monitoring;
- to undertake situation assessment;
- to provide facilities for crisis task forces, and
- to provide Brussels-based support and a point of contact for Council field activities, the High Representative, crisis-management operations, fact-finding missions, EU Special Representatives

Source: European Parliament (2010)

With the entry into force of the Lisbon Treaty in 2009, SITCEN came under the authority of the HR/VP. Although the Council has never adopted a secondary legislation establishing SITCEN, the Council Decision establishing the EEAS acknowledged, in the third indent of Article 4(a), that SITCEN became part of the EEAS under the authority of the EEAS (Council of the EU, 2009). As a change in its place under EU framework, in 2012 SITCEN was renamed INTCEN and a public document was also released on its functioning. According to a factsheet, INTCEN "is the exclusive civilian intelligence function of the [EU], providing in-depth analysis for EU decision makers" (EEAS, 2015). By monitoring international events and particularly sensitive geographical areas, its tasks include intelligence analysis, early warning and situational awareness to the HR/VP. INTCEN's main functions and tasks are defined as follows:

Table 7: INTCEN's Main Functions and Tasks After Institutional Re-Shuffling

- Providing exclusive information that is not available overtly or provided elsewhere to the [HRVP] and the PSC, based on contributions from Member States' intelligence and security services;
- Providing assessments and briefings and a range of products based on intelligence and open sources to the [HRVP] and to the EEAS, to the various EU decision making bodies in the fields of CFSP/CSDP and CT as well as to the Member States;
- Acting as a single entry point in the EU for classified information coming from Member States' civilian intelligence and security services;
- Supporting and assist the President of the European Council and the President of the European Commission in the exercise of their respective functions in the area of external relations;
- Giving ad-hoc briefings, e.g. to the HRVP, EU Special Representatives, various Council bodies and the European Parliament.

Source: EEAS (2015)

The integration of INTCEN into the EEAS, however, does not mean that it now works with raw intelligence or operational information. According to former SITCEN Director William Shapcott: "[t]he information shared with us is generally not designed to help with that sort of [urgent] warning. SITCEN can write a respectable analysis of the overall threat in Europe and the types of features that it has, but it will not help you much in judging what next week's threat in Paris or London will be. There are other people better placed to do that" (Jones, 2013, p. 5). Given the lack of collection capabilities of its own, INTCEN is a purely analytic centre which heavily relies on open sources information but also sends requests for information to national intelligence authorities. At the same time, it struggles to receive information on some dossiers, especially information on Middle East countries. Thus, INTCEN is specialised in medium- and long-term products which are evaluated to provide accurate predictions on future events (Arcos & Palacios, 2020, pp. 78–80). Its main added value is not new information but rather "the collective effort and shared and common information base that it represents" (Korteweg, 2022). After the 2014 Ukraine crisis, a Hybrid Fusion Cell (HFC) was formed in INTCEN to contribute to situational awareness on hostile hybrid policies (Conrad, 2021, p. 60) by putting together information and intelligence from different sources. However, the usual criticism has been that Member States do not share enough and there is always a dilemma of how to incentivise them to routinely share (#6). Sharing, therefore, is not only the question of trust but also a question of routine (#6, #7).

Another important question is the extent to which intelligence information can be politicised. According to an EU official involved in information sharing, once an information is influenced by political considerations, the whole intelligence process loses its significance. The role of the intelligence is, indeed, to provide objective information on a certain topic, thus Member States have to accept some realities even if they dislike the results. EU intelligence units need to de-politicise intelligence briefings (#1, #3). Similarly, another former official confirmed that INTCEN and EUMS Int need to work out their assessments and how they manage them because the main question is "how you incorporate challenge and dissent, especially in the multinational domain. We are always thinking about how you challenge assessments and how you register dissent in a way that is not completely destructive" (#6).

With the establishment of the EEAS, an Intelligence Support Architecture (ISA) was also created (HR Decision, 2012). After the entry into force of the Lisbon Treaty, the tasking of EU intelligence resources was tied more closely to the HR/VP and in general to the EEAS. The establishment of ISA aimed to strengthen inter-agency coordination within the EEAS and the Commission and to connect more closely national and international intelligence authorities and partners, as well as EU military and civilian intelligence structures. Administratively, the ISA is divided in the Intelligence Steering Board (ISB) and the Intelligence Working Group (IWG). The ISB is chaired by the HR/VP or the EEAS Executive Secretary-General while its Board also consists of senior officials from the relevant Managing Directorates of the EEAS, representatives of the General Secretariat of the Council, the Commission and the EU Counter-Terrorism Co-ordinators. The IWG, co-chaired by the heads of INTCEN and EUMS INT, is a preparatory body for the ISB and its monthly meetings are attended by the representatives of the relevant Managing Directorates of the EEAS. The Prioritised Intelligence Requirements

(PIR) are the cornerstone of ISA which, on the proposal of the IWG, is adopted by ISB. They set out the areas of priorities, focus areas and requirements for joint intelligence production (Fägersten, 2015, p. 7; Gruszczak, 2016, pp. 237–238; Kozlowski & Palacios, 2014, p. 11).

Table 8: INTCEN Products

- Intelligence assessments: long-term strategic papers, mainly based on intelligence.
- Intelligence reports: follow-up of a crisis or an event, or a thematic paper focusing on a specific topic of current interest.
- Intelligence summaries: focusing on current important events with a short intelligence based analysis.
- Threat assessments: focusing on risks for EU personnel in a given country.

Source: EEAS (2015)

The INTCEN is not the only unit that came under the authority of the EEAS. In mid-2011, EU foreign ministers agreed that "early warning needs to be further strengthened within the EU, by better integrating existing early warning capacities and outputs from all sources, including from Member States, and drawing more extensively upon field-based information from EU Delegations and civil society actors, in order to provide a more solid foundation for conflict risk analysis" (Council of the EU, 2011a, p. 2). Subsequently, the Lisbon Treaty provided other elements and capabilities in the EEAS that supported early warning and conflict prevention. Then HR/VP, Catherine Ashton, created crisis response capabilities within Crisis Response and Operational Co-ordination Department (MD VII) of the EEAS. This modification aimed at mobilising EU institutions and Member State to manage civilian crises and consolidated within the EEAS organisational and human resources around all-source analytical capabilities (Gruszczak, 2016, p. 134). In 2013, the EU Integrated Political Crisis Response (IPCR) was also created which is the EU's framework for the coordination of cross-sectoral crises at the highest political level (Council of the EU, 2022b). The political control and strategic direction of IPCR is under the leadership of the Presidency of the Council.[3] As a result of these rearrangements, a multi-level system was created whereby the IPCR served as a "super-structure" and MD VII as a coordinator for external crises that managed the Crisis Response System (CRS), formed in 2011, and cooperated with different EEAS units, INTCEN, EUMS and SATCEN (Gruszczak, 2016, p. 134; Vimont, 2014, p. 36).

The EU Situation Room, which complements the analytical work of INTCEN and EUMS Int, is the EU's crisis centre that provides worldwide monitoring and situation awareness 24/7. It was created in 2011 and is a result of a merger of staff from SITCEN and the Commission's DG RELEX Crisis Room. As part of the EU's CRS and as permanent stand-by body, the Situation Room is the first contact point for all information on crisis situations. Thus, it closely monitors events relevant for the EEAS and for the EU in general, liaises with CFSP/CSDP missions and operations, supports the HR/VP, the EEAS, the Council, and the Commission and plays a role in the EU IPCR arrangements (EEAS, 2019). According to a Council's report, in 2014 the

[3] Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements.

Situation Room forwarded more than 650 of its monitoring products, all accessible to Member States (Council of the EU, 2015, p. 11). The Situation Room also includes the Watch-Keeping Capability which works on a 24/7 basis and is run by police and military officers tasked with supporting CSDP with specific information. Most background information reaches the Situation Room, which can alert the EEAS, the Commission, the General Secretariat of the Council, and the Member States and can draw their attention to cases of emerging crisis situations (Gruszczak, 2016, pp. 135; 140; Pawlak, 2014, p. 87; Vimont, 2014, p. 36).

The EU Crisis Platform is the second important element of the CRS (Gruszczak, 2016, p. 136). Chaired by the HR/VP, the EEAS Executive General or the EEAS Managing Director, the Crisis Platform is convened when there is an urgent need for the EU to respond to an external crisis. It provides clear political and strategic guidance for the EEAS and the Commission for possible crisis management responses. Depending on the nature of the crisis, the Crisis Platform can be composed of different units (EEAS, 2019). By 2014, it responded to various crises, ranging from challenges located geographically mostly in Africa and Asia (Gruszczak, 2016, p. 136).

After the INTCEN moved from the Council to the EEAS, approximately 70 people were employed out of 3500 in the EEAS. The number of people working in the INTCEN was largely seven times higher compared to its 2002 beginning (European Parliament, 2010). INTCEN has two main divisions. The Analysis Division provides strategic analysis based on the inputs received from Member States whereas the General and External Relations Division focuses on the legal, administrative and IT issues and undertakes open-source analysis (Jones, 2013, pp. 2–3). By 2017, INTCEN's size grew to approximately 100 personnel but its responsibilities continued to be the same: INTCEN also keeps open the channels of communication with NATO and other international organisations (Seyfried, 2017, p. 2), as also EUMS Int is mandated to do. INTCEN produced 166 documents in first half of 2012 of which 17 were SECRET, 129 CONFIDENTIAL, 20 RESTRICTED, but no one received the TOP SECRET classification (Jones, 2013, p. 5).

The role of the European Parliament in foreign and security policy issues is marginal but, under certain circumstances, it may be granted access to some types of sensitive information. MEPs may only consult information up to the level RESTREINT UE/EU RESTRICTED without security clearance. EU CONFIDENTIAL, SECRET and TOP SECRET classified information can be accessed in the cases and modalities explicated in a 2013 Decision of the Bureau of the European Parliament (European Parliament, 2013).[4]

Being part of CFSP and of CSDP, MEPs do not have the possibility to substantially influence the way intelligence cooperation is performed. Nevertheless, some of the MEPs are increasingly interested in fostering EU intelligence structures. Following Ursula von der Leyen's 2021 State of the Union speech in which the President of the Commission foresaw the further

[4] Interinstitutional agreement of 12 March 2014 between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters than those in the area of the common foreign and security policy.

integration of EU intelligence structures, MEP Sánchez Amor asked the HR/VP to clarify the EU's plans on the future of EU intelligence. In particular, he asked three questions: (1) would the Joint Situational Awareness Centre, as proposed by the President of the European Commission, have intelligence collection powers; (2) how does the EU envisage forging closer intelligence cooperation between itself and the Member States; and (3) how does the EU plan to create its own intelligence service (Sánchez Amor, 2021)? In a reply, the HR/VP clarified that (1) the President of the Commission seeks to encourage Member States to share more information at the EU level, and although the establishment of the Joint Situational Awareness Centre is currently given full consideration, intelligence is a Member State competence and some of the Member States are even legally constrained to disseminate information at the EU level; (2) INTCEN acts as gateway for intelligence and security services in the EU and the Member States are committed than ever to share voluntarily strategic intelligence and seconded experts; (3) the establishment of the Joint Situational Awareness Centre will develop in the context of the Strategic Compass (Borrell, 2022).

Table 9: Intelligence and Secure Communication in Pillar 2 of the Strategic Compass

- "By the end of 2022, the [SIAC] will review the EU Threat Analysis in close cooperation with Member States' intelligence services. Such regular and structured reviews will be conducted at least every 3 years or sooner if the changing strategic and security context calls for it.
- By 2025, we will strengthen our [SIAC] by enhancing the resources and capacities. By 2025, we will also strengthen the EU [SATCEN] to boost our autonomous geo-spatial intelligence capacity.
- To facilitate exchange of information, including classified information, we call upon EU institutions, agencies and bodies to adopt in 2022 additional standards and rules to ensure cybersecurity and security of information.

Source: Council of the EU (2022a)

4.3 EU Military Staff

Military intelligence refers to intelligence on threats coming from an external security environment, be it a national or non-state actor. It usually informs the planning and conduction of a military operations, by providing a situational picture and an analysis of actual and potential risks on the ground, or of changing situations.

The first embryonic forms of military intelligence cooperation at the EU level started in the framework of the WEU in the early 1990s. The 1992 Petersberg Declaration recognised the necessity for the WEU to have a Planning Capacity Cell for the performance of WEU missions and operations. The necessity to have a cooperation with national authorities and NATO on intelligence cooperation, by means of specific intelligence agreements, was a feature considered to be of importance by the Assembly of the WEU, if the planning capacity and operational activities of the WEU were to be taken seriously (WEU, 1994). After the completion of the first organisational setting of the Cell and the initial definition of its roles, the permanent

council of the WEU decided in 1994 to establish a fact-finding mission, to propose a possible WEU intelligence structure.

The resulting structure saw the division between the civilian and the military side of intelligence gathering (Politi, ed., 1998, p.20). The necessity to divide the structures was due to different memberships of the organisation's civilian and military branches. In May 1995, the WEU Council of Ministers, declared the establishment of "a Politico-Military Group, to set up a Situation Centre, and an Intelligence Section in the Planning Cell as well as the adoption of preliminary conclusions and transitional arrangements for the financing of WEU operations, are designed to facilitate and expedite WEU's decision-making and its ability to plan and conduct Petersberg operations" (Extraordinary Council of ministers, 1995, point 168). Later that year, an Extraordinary Council of Ministers further re-confirmed "[t]he need for WEU to establish or to have access to an adequate observation capability and to develop an intelligence processing capability which are decisive for the conduct of operations in complex, shifting politico-military environments" (Extraordinary Council of ministers, 1995, point 175). Given the different memberships and roles, the Situation Centre and the Intelligence Section worked with different sources: while the former worked with open sources, the latter was given classified sources directly from Member States. The dependence of the intelligence section on the Member State's willing contribution, limited the work of the section to the analysis and interpretation of intelligence reports and information passed by those member states with an interest in sharing the specific information.

Council Decision 2001/80/CFSP, as modified by Council decisions 2005/395/CFSP and 2008/298/CFSP, signed "the start of military intelligence cooperation. And very strongly based on British and NATO experience. The structure of the EUMS was mainly inspired by NATO structures: EUMS division of operation etc. is a 'military-light' structure" (#3). Among the EUMS' tasks, there are the monitoring of "potential crises by relying on appropriate national and multinational intelligence capabilities" and the collaboration "with the Joint Situation Centre in the field of information exchange in accordance with the arrangement on the Single Intelligence Analysis Capacity". Additionally, in crisis management situations, the EUMS "requests and processes specific information from the intelligence organisations and other relevant information from all available sources" (Council of the EU, 2001a).

The structure of the EUMS comprised five divisions (now directorates): Policy and plans (now concepts and capabilities), Intelligence, Operations and exercises (now operations), Logistics and Resources (now Logistics), Communication information and security (now Communication and Information Systems & Cyber Defence). To the initial structure, the current one also includes liaison cells at NATO (SHAPE) and the UN, an EU cell at SHAPE, as well as others dealing with external relations and synchronisation with other bodies and entities at the EU level.

In 2005, the intelligence division had personnel of 33 people coming from 19 Member States and constituted the largest division (Maj. Gen. Vaz Antunes J.N.J., 2005). Nowadays, almost every Member State contributes with personnel, which also reflects a positive trend in the level of shared information from Member States (#10). Positive considerations over the shared

information are also confirmed by another interviewee, according to whom "by its nature, [EUMS Int] it's a bit more disposed to share intelligence amongst military members because they have shared experiences on operations, missions and training, etc." (#4).

Inside the intelligence directorate, the intelligence policy branch is responsible for the division coordination with other branches of the EUMS and for development of intelligence related concepts, doctrines and procedures, which are specifically developed also for EU missions/operations. The intelligence support (former requirement branch) encourages the relationship with national defence intelligence structures and coordinates with SATCEN. Lastly, the production branch produces the classified EU Watchlist in coordination with other EUMS bodies. Despite the name of the latter branch, the EUMS Int does not produce in-house intelligence but relies exclusively on Member States contribution. According to the contingent situation, the EUMS Int can request those Member States who might have intelligence on the subject to share that information to then send it to SIAC and issue an EU-approved summary and interpretation of the information received.

When it comes to EU engagement abroad, the Implementation Plan on Security and Defence recognised that "[p]reventing conflicts from erupting or escalating remains of paramount importance. We need to improve our ability to respond early and effectively to conflicts and crises. To support anticipation and situational awareness, enhanced civil/military intelligence and strategic foresight is required" (Council of the EU, 2016).

The sharing of intelligence necessary for the reaching of a situational awareness supporting the performance of the mission, is of paramount importance in all phases of the mission itself, from the monitoring of the situation on the ground, toward the conceptualisation of the operation, and to its performance.

The reliance on Member States' contribution and coordination with third non-EU states, and actors needs to be taken into account in the evaluation of an effective intelligence sharing system. According to a European Parliament study (2012), lessons learned from previous CSDP missions highlighted the necessary to have an increased intelligence support from Member States and an increased EUMS effort in collecting information and intelligence from non-EU intelligence agencies, NGOs, think tanks, and other relevant actors, with knowledge of the situation, or with personnel on the ground. Therefore, possible additional ways to assess the effectiveness of intelligence cooperation in deployment, could be to look at the actual contribution of Member States to the EUMS and to the presence of eventual additional intelligence sharing agreements with relevant actors on the ground. Brexit also meant the exclusion of the country to the EUMS Int. According to #10, Brits officials were particularly active in sharing intelligence with the EUMS Int. The exchange of information between the two entities is still possible and can be considered a way for the UK (and the Five Eyes) to influence EU Member States (#11), given the country enjoys the reputation of a highly capable intelligence actor. What is not possible, though, is the provision of intelligence to the UK without the prior consensual approval of Member States.

Nonetheless, when it comes to the EUMS Int support to CSDP missions and operations, some legal and practical important limitations need to be considered. Currently, the EUMS Int is not mandated to provide intelligence reports on missions/operations, but just to deliver a six-month threat assessment. As a former official said, in "CSDP missions you have a lead nation and accountability is handed to them. This is the then nationalized tactical intelligence. Aside from the youngest developments, the EU has never had military, operational responsibilities. They had executive operations, with lead nations and a commander who will be summoned to Brussels to discuss, but accountability continues to lie with the national government" (#3). Therefore, the eventual collection and sharing of intelligence on the ground is up to Member States with personnel deployed and there is also no system in place to share operational specific intelligence between the EUMS Int and Member States (#10, #11). Such a lack of intelligence sharing questions the role the EU wants to play in the international arena, as well as the effectiveness, coherence, and sustainability of the CSDP structure. As #11 pointed out, once there will be a clearer political definition of the level of ambition of the EU, then it would be possible to consider what this implies for CSDP and missions/operations. Moreover, it would be necessary to "consider defining joint standards and procedures for information management for CSDP missions/operations, as well as improving (IT) infrastructures".

4.4 Single Intelligence Analysis Capacity

An early experience in EU intelligence cooperation was that the civilian and military intelligence needed to be combined. Already during its creation in 2002, SITCEN included staff from the EUMS Intelligence Division and Operations Division, which in itself showed an increased interaction between the military and civilian intelligence (Müller-Wille, 2008, p. 62). However, SITCEN and EUMS Int continued to work as two different entities. Subsequently, then HR/VP Javier Solana proposed "to bring together, in a functional way, analytical capacities from both the [SITCEN] and EUMS Int, thus benefiting from a wide EU knowledge base for producing enhanced and reliable intelligence" (Kozlowski & Palacios, 2014, p. 11). "While they couldn't change structures and join the entities, they could change procedures" (#3) and so "SIAC had been created by Solana in 2007. This was, in the end, the best possible thing he could have done" (#3). The cooperative scheme between SITCEN and EUMS Int in SIAC was a response to the need for a comprehensive approach in EU security policies. Both the SITCEN and the EUMS Int sought to advance synergies by a joint civilian-military approach. However, regardless of this new format, SIAC's products largely remained dependent on Member States willingness to forward pieces of information to the two bodies. As two of the interviewees put it, "within the EU there is no intelligence cooperation, there is a concerted support to INTCEN and EUMS Int" (#3) and the good outcome of the cooperation and coordination between INTCEN and EUMS Int can be evaluated to be "as good as the willingness of the directors to work together" (#10). As a matter of fact, the total absence of any legally binding minimum requirements to be satisfied limits the potential improvement of the cooperation.

The SIAC receives inputs from civilian and military sources which are compared and analysed against open-source information (Gruszczak, 2016, pp. 235–236; Kozlowski & Palacios, 2014, p. 11). In practice, the two entities coordinate the requests for information sent to the Member

States and, once they receive States' contribution, they produce joint reports, a process often led by the INTCEN (Fägersten, 2014, p. 97). The SIAC receives finished intelligence products from Member States which are fused with information from the EEAS and the Commission into all-source intelligence products which are then disseminated to all Member States, the EEAS and the Council (Political and Security Committee, 2017, p. 14).

The SIAC, however, has remained a virtual entity with no secretariat – i.e. no human being involved – but this virtual arrangement still contributes to a better synergy between INTCEN and EUMS Int. As Ilkka Salmi, former Director of INTCEN put it: "[w]hen we produce our products, most of them are joint production anyway – probably 90 percent" (Mondial Nieuws, 2014). As the Implementation Plan on Security and Defence of 2016 underlined: "[i]mproving CSDP responsiveness requires enhanced civil/military intelligence to support anticipation and situational awareness, through the [SIAC] as the main European hub for strategic information, early warning and comprehensive analysis. This includes horizon scanning, updated situational assessment in support of political/strategic decision-making, and granular civil/military 24/7 situational awareness for the planning and conduct of missions/operations (Council of the EU, 2016, p. 26). Or, as the EU's Global Strategy also emphasises on the need of timely information sharing and situational awareness: "[i]n security terms, terrorism, hybrid threats and organised crime know no borders. This calls for tighter institutional links between our external action and the internal area of freedom, security and justice […] Member State efforts should also be more joined-up: cooperation between our law enforcement, judicial and intelligence services must be strengthened" (EEAS, 2016).

Despite the establishment of SIAC, intelligence officers are to a certain extent sceptical as to whether the bringing together of SITCEN and EUMS Int has been efficient. Generally, expert opinions are not favourable to completely separate civilian and military intelligence (#3, #4, #5, #6, #10, #11). Despite the creation of SIAC, a former intelligence officers argued that "you are still starting from two different organisations. I can't believe they have so many people that they can afford to have two different organisations" (#6). Another former official also emphasised the need of a complete fusion between SITCEN and EUMS which did not happen in 2015 "when I had a close connection with the EUMS […] I have seen in NATO to fusing the military and civil intelligence operators and analysis and it brings a lot of added value and really improves the quality of the output" (#4). A third former official added that "probably SITCEN and EUMS are doing quite a lot of the same things" (#5). A fourth official affirmed that the merge of intelligence structures could solve the coordination problems currently present between INTCEN and EUMS Int (#10). A fifth added that to do so there is first the "need to define what they want and need" (#11).

The Strategic Compass is an important step to further the potential enhancement of EU intelligence structures. Adopted in March 2022, it was based on the first-ever joint threat analysis, produced by the SIAC and created to provide a "comprehensive, 360-degree independent analysis of the full range of threats and challenges the EU currently faces or might

face in the near future".[5] The fact that the Strategic Compass had to be approved by all 27 EU Member States diminished the level of details on the threats and according to some officials it failed to foresee a Russian stronger attitude toward conventional conflict. Nonetheless, the threat analysis was an important process in defining a common understanding of the main threats the EU faces and could be considered the "most meaningful intelligence document ever produced by an international framework" (#10), thanks to the low level of politicization of the document. Indeed, the process leading to the threat analysis started from contributions from Member States to INTCEN and EUMS Int, followed by a phase of internal analysis and report drafting inside SIAC. The analysis was then re-sent to the national intelligence services for the provision of feedback prior to the finalisation of the document that occurred at SIAC.

The Strategic Compass aims, among other things, to enhance the EU's intelligence capacities, including the SIAC framework. Its primary objective is to improve the EU's situational awareness and strategic foresight, building on the Early Warning System and horizon scanning mechanism. The further strengthening of the SIAC and the SATCEN is expected to bring Member States closer to a common strategic culture and to give the EU more credibility as a strategic actor. As #8 put it, "we have vocal statements that we want to be a global actor with the necessary means, [but] we will never be a global actor if we do not have the means. And one of the means to be a global actor is intelligence".

With the further reinforcement of the SIAC, there is a prospect of facilitating the exchange of strategic intelligence to better respond the many challenges the EU is facing now as well as the opportunity to provide improved services to EU institutions and Member States. As part of a response to increased cyber-attacks, there is also a recognition of the need to strengthen secure communication to protect information, infrastructure, and communication systems as well as to guarantee the protection of EU classified information and sensitive non-classified information. A strengthened cyber intelligence sharing and EU posture in the cyber domain has also been hoped for in the Council conclusions on the development of the European Union's cyber posture (Council of the EU, 2022d).

The SIAC will be also expected by the Compass, through the work of the Hybrid Fusion Cell, to detect, identify and analyse hybrid threats and their sources and will also be designed to provide foresight and situational awareness in that regard. The Strategic Compass also recognises the importance of the need to strengthen cyber intelligence capacities to enhance cyber resilience and to support civilian and military CSDP missions and operations (Council of the EU, 2022a, pp. 21–23). Nonetheless, the strategic compass needs a follow up from Member States and requires a leader "who steers the process" (#10). A further possible improvement of SIAC could be "to create terms of reference for the EU and its Member States concerning the role and function of SIAC in creating situational awareness in all the decision-making processes, foreign and internal [...]. That puts situational awareness as a constituent

[5] EEAS, Memo, Questions and Answers: Threat Analysis – A Background for the Strategic Compass, 20 November 2020, https://www.eeas.europa.eu/sites/default/files/2020_11_20_memo_questions_and_answers_-_threat_analsysis_-_copy.pdf

in the decision-making process [and there is] [n]o decision-making without situational awareness" (#3). an alternative restructuring could be done with the creation of an entity, outside the EEAS, that puts together all branches of intelligence cooperation. According to #11, the exact structure of such an entity is difficult to foresee, as it will mainly depend on the role the EU wants to play and on the scope for intelligence cooperation. "Should intelligence continue to be used in support of policymaking, then there is little that can be done, but if the goal is to support CSDP more substantially, there should be a discussion on how to structure a possible different architecture" (#11).

4.5 The External Dimension of the Area of Freedom, Justice and Security

This working paper focuses on the external aspects of EU intelligence. Undeniably, however, EU internal affairs can also have an external dimension. Internal and external security, although technically separated in the EU, cannot be always neatly disconnected from one another. In particular, the development of the EU's counter-terrorism policy shows how the INTCEN and the Europol have worked together in intelligence matters. In 2004 after the Madrid bombings, two important changes occurred in the relationship between INTCEN and Europol. First, INTCEN's Civilian Intelligence Cell created a counter-terrorist analytical capacity and its focus on the CFSP shifted slightly to Justice and Home Affairs (JHA) matters. Indeed, INTCEN originally focused on external threats, but as part of the comprehensive approach, the EU gradually removed the artificial divide between internal and external security (Cross, 2013, p. 394). It was also decided that the Counter-Terrorism Group should be the interface between the EU and the internal security services on terrorist issues. In 2005 a team of counter-terrorist experts seconded from the Member States joined the INTCEN (EEAS, 2015). INTCEN was also envisaged to have a central position in the General Secretariat of the Council and thus was expected to bridge the gap between the CFSP and JHA matters by providing internal and external security analysis. The recommendation at that time was to better streamline the activities of counter-terrorism groups (e.g. Terrorism Working Group or Article 36 Committee) but leave intact Europol's margin to conduct intelligence-led criminal analysis. Gilles de Kerchove also argued that "[t]he [INTCEN] has developed into a unique platform where strategic intelligence produced by the intelligence, security and military services, police information collected by Europol and open sources are integrated and summarized." William Shapcott, similarly stated that "[w]e are all trying to make sure that the interior ministries see [INTCEN] as something that they own jointly and that works for them […] We are not exclusively a [CFSP] body" (Gruszczak, 2016, pp. 231–232).

Second, interrelated to the first change, INTCEN did not receive intelligence only from foreign intelligence agencies of the Member States but also from counter-terrorism hubs. This latter included Germany's Joint Counterterrorism Centre, the UK's Joint Terrorism Analysis Centre and the Dutch General Intelligence and Security Service. Already in mid-2005, the EU Action Plan on Terrorism was considered to be a document that crossed the line between domestic and international security. It also reflected the broader trend of understanding security as encompassing the protection of national infrastructure or analysing trends in terrorist

financing (Aldrich, 2012; Norheim-Martinsen, 2012, p. 96). In the mid-2000s, it was estimated that approximately 40 per cent of INTCEN's reports dealt with terrorism assessments (Cross, 2013, p. 393). As the Council's 2008 annual report on the CFSP confirmed, the INTCEN contributed to early warning and conflict prevention. It undertook situation and risk assessments and issued 150 reports to the Council and to Member States (Council of the EU, 2008, p. 98).

At the same time, even after the terrorist attacks in the US and Europe in the 2000s and despite several calls to establish a stronger counterterrorism policy, national authorities and security and intelligence services failed to agree on a mechanism for passing more information to Europol. INTCEN was also expected to deepen its cooperation with Europol, but this cooperation did not materialise to the extent hoped for by many policy makers. There have been three principal reasons why the effort to strengthen EU intelligence cooperation failed. First, in the field of security intelligence, Member States favoured pre-existing arrangements which had been established outside the EU framework. Europol simply could not compete with long-established informal networks that were trusted by the Member States. Second, bureaucratic interests clearly contributed to less effective cooperative formats: disagreements over which Member State had the greatest competence in counter terrorism precluded a high degree of cooperation, and INTCEN aimed to marginalise Europol in this respect. Third, different ideas and cultures prevail in the internal and external intelligence spheres: Europol is primarily seen as a police organisation whose competence in terrorism is often called into doubt. More importantly, information gathered by intelligence services may be shared with partner organizations but less with internal intelligence services that may have different culture and secrecy policies (Fägersten, 2010, pp. 515–519).

The blurred boundaries between internal and external aspects of terrorism are reflected in a number of EU policy documents, including in the 2011 Council Conclusion "on enhancing the links between internal and external aspects of counter-terrorism". Indeed, after the entry into force of the Lisbon Treaty, the EU yet again realised the need of ensuring consistency between the different areas of EU external action and the area of freedom, security, and justice (formerly JHA area). It also recognised the requirement of developing synergies between the different institutions and units dealing with counterterrorism. Interaction between the internal and external aspects of security is perhaps best demonstrated by the document's reference to INTCEN which continues to provide "assessments both on the internal and external aspects of [counterterrorism], serving Member States, Commission, EEAS, and other EU bodies" (Council of the EU, 2011b, p. 3). The Council also encouraged the "[INTCEN] and Europol to work together, in a complementary manner, to comprehensively analyse the terrorist threat to the EU" (Council of the EU, 2011b, p. 3). The EU Terrorism Situation and Trend Report (TE-SAT), established after 9/11, is produced annually by Europol to provide an overview of the terrorism situation in the EU from a law enforcement perspective. TE-SAT is shaped by a number of EU institutions and units, more prominently by the INTCEN.

The position of the EU Counter-Terrorism Coordinator, created by the European Council after the 2004 bombings (European Council, 2004, p. 14), has also ensured that threats analyses

and reports produced by EU bodies and the Europol are synthesised and are translated into policymaking. The idea behind the Counter-Terrorism Coordinator was that someone in the EU needs to have an overarching view of all the policies regarding radicalisation and terrorism. This includes the competence to oversee the coordination of several stakeholders, involving law enforcement, diplomatic services or ministries of finance or defence. The Counter-Terrorism Coordinator is located within the Council, but its role is seen as serving all EU institutions (International Review, 2022). Indeed, the overall task of the EU Counter-Terrorism Coordinator, currently led by Ilkka Salmi, is to coordinate counter-terrorism activities within the EU and to present recommendations and areas of priority for action to the Council. In his daily job, the Counter-Terrorism Coordinator coordinates the relevant preparatory bodies of the Council, the Commission, and the EEAS (Council of the EU, 2021).

The EU's actions against cyber-related activities also fall in the grey zone between EU internal and external actions. Internally, for instance, the European Cybercrime Centre was set up by Europol in 2013 to strengthen the law enforcement to cybercrime and has since been involved in many high-profile operations. The Centre mainly focuses on cyber-dependent crime, child sexual exploitation and payment fraud. It provides operational support to national authorities, including criminal information or intelligence in cybercrime cases (Pawlak, 2018, p. 26). It works together with a number of EU units, such as the EU cybercrime Task Force (EUCTF) or the Joint Cybercrime Action Taskforce (J-CAT) (Europol, 2022). From a judicial perspective, in 2016 the Council formalised the European Judicial Cybercrime Network (ECJN), supported by Eurojust, to "facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace" by sharing information and best practices (Pawlak, 2018, p. 34).

Externally, the EU has adopted many tools to tackle cyber-related activities. In 2017, for instance, the EU established a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the so-called cyber diplomacy toolbox), which allows the Union to use CFSP measures to prevent, deter or respond to different cyber activities. The Council recognised that cyberspace "poses continuously evolving challenges for EU external policies, including for the [CFSP], and affirms the growing need to protect the integrity and security of the EU, its Member States and their citizens against cyber threats and malicious cyber activities (Council of the EU, 2017, p. 3). As part of this cyber diplomacy toolbox, in mid-2020 the EU imposed its first ever sanctions against six individuals and three entities involved in various cyber-attacks (Council of the EU, 2020).

Cyberspace is also protected by EU defence measures. The first such element was the EU Cybersecurity Strategy adopted in 2013 with a focus on developing cyber defence capabilities and technologies, cyber defence policy framework to protect CSDP missions and operations, a civil-military dialogue and a dialogue with international partners, such as NATO. In 2014, the Cyber Defence Policy Framework was also adopted with the aim to develop cyber defence capabilities for CSDP and its communication and information networks. In 2016, the EU and NATO adopted a Joint Declaration to enhance coordination on hybrid threats, including the sharing information and intelligence in these matters (Pawlak, 2018, p. 40). In 2020, the

Commission and the HRVP presented a new EU Cybersecurity Strategy which is expected to allow the Union to step up leadership on international norms and standards in cyberspace and to strengthen both the capacity to react to cyber threats through the Joint Cyber Unit and the cooperation with international partners. In parallel, the Commission also proposed two pieces of legislation that aim to "address current and future online and offline risks, from cyberattacks to crime or natural disasters, in a coherent and complementary way" (European Commission, 2020). Moreover, the EU Military Vision and Strategy on Cyberspace as a Domain of Operations recognises the importance of cyber in "providing situational awareness, early warning, advance and crisis response planning, while strengthening the EU autonomous analysis capacity in order to better inform the decision-making processes" (EEAS, 2021). Its relevance has been further recognised also for the civilian intelligence sharing, advising a "strengthening [of] EU INTCEN's capacity in the cyber domain, based on voluntary intelligence contributions from the Member States and without prejudice to their competences and of exploring the proposal on the possible establishment of a Member States' cyber intelligence working group" (Council of the EU, 2022d).

5 Intelligence Sharing with External Actors

For decades, European national intelligence and security services have cooperated with several multilateral organizations. Clearly, one of the most developed multilateral cooperative frameworks in that regard is the Club de Berne. It remains mostly a blackbox for outsiders as its discussions are subject to 30 or sometimes even 50-year retention periods. Established in the early 1970s, the Club de Berne brings together European security services – currently, the 27 EU Member States, Norway and Switzerland. Given the successful exchange of information that takes place within its framework, several attempts have been made to bring the Club de Berne closer to EU institutions, but EU Member States have always resisted, partly due to the Club's secretive framework and the fear of exposure of sensitive data. Despite the continued deliberate separation of the Club de Berne from the EU, its presidency follows the rotating presidency of the Council. Its biannual meetings are attended by experts in the fields of counter-espionage, counterterrorism or the proliferation of weapons of mass destruction (Fägersten, 2014, p. 98; Jirat, 2020; Seyfried, 2017, p. 3).

As a recent leak clearly demonstrated, however, non-European services are also active in the work of the Club of Berne. Thus, the long-standing belief that the Club of Berne is only composed of some European intelligence services is now seriously called into doubt. In fact, as a leak by the Austrian Newspaper "Oesterreich" showed, the FBI, the CIA and the Israeli foreign intelligence service Mossad were also involved in exchanging information. Moreover, as other pieces of evidence point out, already in the 1970s – when the Club of Berne was only composed of nine Western European secret services – Mossad and the FBI had been already involved as part of coordinated efforts against Palestinian terrorists. Still today, this larger network is present: a list in the Club's communication network is called "Capraccio" which is the group exchanging information on Islamic extremism and is composed of non-European services, such as Mossad (Tel Aviv), CSIS (Ottawa), FBI (Washington), ASIO (Canberra), NZSIS (Wellington), CIA (Brussels) and ISA (Tel Aviv). Another list is called "Toccata" which is used for the exchange of information on non-Islamic terrorism but that is seemingly composed only of European services (Jirat, 2020).

As a former working group of the Club of Berne, the CTG emerged as a separate forum after 9/11, mostly as a recognition of the need to increase security service cooperation on counter-terrorism issues. The CTG thus became a "forum for experts to develop practical cooperation a better understanding of terrorist threats" and produces "threat analyses for leading politicians at the EU level" (Jirat, 2020). Interestingly, the CTG is also an autonomous body, but it has presence in the form of a team working within the INTCEN. The CTG's presidency also rotates along with the presidency of the Council. It receives data from national intelligence services and its analyses are provided mostly to the Commission and the HR/VP. Thus, since the early 2000s, the CTG has played an important role in terrorist threat analysis conducted by European security authorities (Fägersten, 2014, p. 98; Jirat, 2020; Seyfried, 2017, p. 3). "After the London bombings, Solana said we have to have other capabilities for situational understanding and arranged that with the member states governments and respective bodies governing their intelligence services. This was quite interesting and merely due to the intense

feeling of imminent terrorist threats at that time. CTG agreed on that and they seconded another half a dozen analysts" (#3). In 2018, the CTG also welcomed Europol on two occasions where the latter delivered presentations on women and children joining the ISIS, "focusing on their use of internet and social media for terrorist-related purposes" (Europol, 2019, p. 43). While cooperation between the CTG and EU institutions in general could be seen as a welcome development, Austrian historian and intelligence expert Thomas Riegler has critical views on that: "[s]ince [the Club de Berne and CTG] are not officially embedded in the institutional architecture of the EU, nor are they based on a contractual agreement, both […] are merely bound by the national laws of their respective states. There is no uniform regulation on this […]. The Club and CTG do not follow any overriding rules. And since the national laws differ greatly, control becomes impossible" (Jirat, 2020).

The exchange of classified information also occurs with NATO.[6] The first official legal basis for this exchange is represented by the 2003 Agreement between the European Union and the North Atlantic Treaty Organisation on the security of information, which builds upon the 2000 Interim Security Arrangement between the General Secretariat of the EU Council and the North Atlantic Treaty Organisation (Official Journal of the European Union, 2003, p. 36–38). Additionally, thanks to the arrangements under the Berlin Plus Agreement the EU CSDP missions and operations can take advantage of the NATO structures and support. For the performance of a mission/operation, information sharing is particularly relevant for an effective and coherent cooperation. In the case of the transition from NATO's Allied Harmony operation to the EU Operation Concordia, modalities for intelligence sharing were not agreed upon in the beginning, causing challenges. Additionally, the establishment of direct contacts between Concordia and NATO peace keeping forces in Kosovo were prevented by structural and procedural differences between the organisations (European Parliament, 2012).

In case of deployment foreseeing the involvement of various (non)NATO and (non)EU contributing countries, there are "different levels of information exchange" (#2, #11) according to the membership of the different countries. There usually is a "core central group of States which basically share everything but also do collection jointly or processing jointly. Then you have these outline layers [...] and those on the outlines have different levels of information and exchange. [...] So you would end up [...] in a NATO-led operation hav[ing] these EU Member States that are not NATO Member States in one of those outline circles where the level of information sharing is not as intense as it is with core NATO members. But still, this facilitates information sharing between those" (#2). Moreover, NATO operates shared military capabilities collecting shared data, which are also used in the performance of a mission/operation (#11). At the EU level "there have been attempts to build something similar with some PESCO projects" (#11) but no "meaningful commitment" can be seen at the moment (#10).

[6] The presentation of the NATO structures for intelligence sharing and cooperation is beyond the scope of this working paper. Therefore, only considerations on the exchange of information between NATO and the EU are taken into account.

In the exchange of classified information, the Turkey – Cyprus issue also prevents proper classified information sharing. Turkey vetoed the exchange of intelligence with the EU, particularly when NATO intelligence could land in the hands of non-NATO EU members (Dursun-Özkanca, 2019). As an interviewee pointed out, "Turkey might be an obstacle in greater intelligence sharing and if that is the case then they have to do with (other) allies. [...] It is mostly Turkey but not always just Turkey. Other nations sometimes reject to share intelligence for one reason to another; France, or Greece, have been sometimes one of the impediments of intelligence sharing from the EU to NATO. It's a bit of a two-way street" (#4).

Nonetheless, to improve effective mutual consultation, both organisations have permanent military liaison officers at the respected premises: NATO has its officials at the EUMS and vice-versa (Latici, 2020). Although liaison officers do not exclusively focus on intelligence sharing, the presence of permanent personnel can be considered a positive step forward towards the improvement of trust, coordination and cooperation among parties, despite a divergent view from our interviewees (#10).

Based on the 2016 Joint declaration, EU and NATO perform the Parallel and Coordinated Assessment, which is based on the national intelligence made available to both organisations. The purpose of the assessment is to ensure "a shared vision of the threat landscape" (Joint progress report, 2019), although sometimes NATO and the EU have different, sometime complementary, views on the same issues (#11). In the period June 2020 – May 2021 three Parallel and Coordinated Assessments were developed, and particular effort was concentrated on the reform of security and intelligence services (Joint progress report, 2021). Nonetheless, a proper joint threat assessment is missing, as is an immediate channel for classified information sharing or enough trust between the two organisations (Lindstrom & Tardy, 2019).

"[T]echnological fragmentation, decentralization, and the lack of a common culture are among the weaknesses that hamper NATO's intelligence sharing practices" (Seagle, 2015, p. 560). These factors impede the flow of intelligence sharing within NATO, to which additional ones should be considered in exchanging intelligence with the EU. The different classification systems between the two organisations force NATO to "sanitize" the information shared with the EU or to not share certain information, as it happened in the case of the sharing of military requirements for military mobility (Drent, Krujver, & Zandee, 2019). This limited intelligence and information sharing demonstrates that NATO and the EU are "not able to optimise efforts. This is acceptable in peace time, but not in other situations" (#10). The improvement of the intelligence and information sharing systems was among the proposals included in a European Parliament (2018) resolution, in which the parliament hoped for an increased number of clearances provision for the EU personnel, as well as an improved intelligence sharing on the basis of the need-to-know principle.

Another forum that could further enhance the development of a common intelligence culture is the Intelligence College in Europe. In 2017, French President, Emmanuel Macron, called "for a European intelligence academy to strengthen links between our countries". It is noteworthy

that Macron did not use the notion of “intelligence” or “European FBI” but referred to the creation of an “academy” (Politico, 2017b).

Despite some reluctance, the Intelligence College in Europe (ICE) was founded in Paris in 2019 as “a platform for reflection, engagement and outreach” (Intelligence College, 2020, p. 3) to facilitate cooperation at a non-operational level between the different intelligence authorities, practitioners and academics. The Letter of Intent at the basis of the intergovernmental entity was signed by 23 European states, while others (such as Bulgaria, Greece, Ireland, Luxemburg, Poland, Slovakia and Switzerland) are expected to join at a later stage. The ICE is not a top-down organisation where decisions are made above the participants. It is instead shaped by the intelligence officers (civilian, military, homeland security, external security, and signals intelligence services) through regular interaction with their peers. The ICE also includes security experts and academics who participate in webinars, seminars and research on intelligence issues, to contribute to a common understanding of external threats, to enhance a common intelligence culture and to improve joint situational awareness (Intelligence College, 2022; Korteweg, 2022; Pronk & Korteweg, 2021, pp. 19–21). Such initiatives can be considered positive for the non-specialist personnel, a benefit for non-specialist personnel but according to #10 the added value of such initiatives is very limited without a binding mechanism that allows the translation of the goals into practical and tangible outcomes. However, “having a common understanding what intelligence is, what it can do, how it functions [...] [can] further common understanding and culture” (#2). Similar efforts are also put forward in the EU framework, like the Joint EU Intelligence School Pesco project. While the initiative is commendable, the project targets the “reconnaissance squats and not the strategic level and there is no strategic, common, standard available” (#10).

6 Factors Contributing to an Effective EU Intelligence Cooperation

Trust and shared culture are key issues in sharing sensitive pieces of information (#3, #4, #5, #6, #7). When the EU's intelligence capabilities are compared to other organisations, such as the Five Eyes, it is often emphasised that the members of the Five Eyes "have developed a very-very high level of trust amongst themselves. They are able to share and keep safe classified information. Frankly, it's all about trust among EU Member States that would allow that sharing." (#4). Or, as another former intelligence officer said: "the basis of the Five Eyes is a level of trust that builds over years and years, working together in conflicts, and being on the same side" (#6). The Five Eyes, however, is composed of five independent intelligence agencies who are not *mandated* to share because sharing cannot be prescribed politically – sharing of intelligence must be *organic* (#5, #7).

Against this background, members of an intelligence community also need to guarantee that information is secured, including through internal security measures to prevent the loss of information superiority. Apart from potential institutional re-structuring, the EU is therefore also expected to develop more secure, faster communication channels to lay the basis for a more trusting environment where intelligence information cannot be leaked in relation to third parties (#1, #3, #4, #10, #11). Concerns about how the intelligence information will be treated are among the reasons why EU Member States do not share intelligence. The more they are convinced of effective internal security handling, the more they are willing to share quite a bit of private information on certain issues. The EUMS is a bit more disposed to share intelligence amongst military members because its members have shared experiences on operations, missions, and training (#4).

Deriving from the aforementioned factors, another key issue is that many of the sharing takes place bilaterally or in minilateral formats. As confirmed by a former national intelligence official, meetings were organised between national intelligence authorities and INTCEN/EUMS Int but "the real meetings were in small groups or bilaterally anyway […] I had a decent relationship with INTCEN and EUMS Int and we shared information whenever I went to Brussels but I did not get a huge amount back. It was pretty much one way […] I was much more incentivised to speak to a Latvian who would tell me their perspective on what Russia is up to than a fairly bland EU assessment that does not really add anything to what I already knew" (#6). In addition, geographical proximity and/or culturally aligned states (e.g. Nordic states) are more willing to share intelligence with one another given the shared historical legacy, a similar understanding of security threats and mutual trust they have developed over years.

In the field of intelligence cooperation, the main reason for the controversial and unequal integration process is that EU Member States have different interests and capabilities in intelligence matters (#1, #2, #3, #4, #6, #8, #10). For instance, the reason why there has been increased sharing of intelligence related to terrorism is that "interests align and there is a

common interest and also a common threat perception" (#2). In general, "large" Member State have more capacity due to their long traditions in intelligence matters and may therefore be able to put forward more deliverables compared to "small" Member States (#4). However, as confirmed by one of our interviewees, there is an apparent divide between quantity and quality of information. According to the experience of #1, who is heavily involved in the current EU intelligence sharing, "small" Member States may provide more important information on a particular region than "large" Member States. In other words, it is not always necessarily the size of the Member States that determines the importance of a given information (#1). Similarly, another former official argued that "if you want to know about Kaliningrad, you would ask the Baltics but you would not ask the Baltics about a certain part of Africa" (#7).

External threats may be catalysts for further improvements. Indeed, as confirmed by some of our interviewees, Russia's decision to invade Ukraine could contribute to additional discussions within the EU on the conditions for further integration. Before 24 February 2022, EU Member States far from the Eastern neighbourhood could have argued that the EU's foreign policy priorities were focused elsewhere other than Russia. After the invasion, the EU's unity is stronger than ever and although we cannot expect/claim a complete harmony of views on Russia, there is now a recognition that there should be a transatlantic exchange of information on Moscow. Before the 2022 invasion, the US was constrained from sharing information with the EU but it could share a "two-line assessment that said: we assess that Russia is going to invade Ukraine. We could not provide any more detail" (#7). Sharing information with everybody meant that there was a higher risk that it could be picked up by the Russians (#5, #7). Despite all these reservations, recent Russian actions may be a wakeup call that will lead to a greater intelligence sharing on challenges ranging from malign efforts, cyber or hybrid attacks. Additionally, the fact that relevant information was shared by the US intelligence on the possibility and expected date of a Russian invasion to Ukraine in March 2022 is something unusual for the intelligence community. Moreover, according to some newspapers, the US provided operational and tactical intelligence to Ukraine in support of the country (Bertrand N. and Bo Lillis K., 2022).

In the longer term, China is also a challenge for both the EU and NATO. However, China is not only a security challenge but there are also other concerns, such as supply chain security, pharmaceuticals, microchips, foreign direct investment, state-owned enterprises, 5G, software or hardware (#2, #3, #4, #7). One of our interviewees added that "this is where the senior leaders could say 'we have a real common interest here and we've got different intelligence capabilities that we could share'. Both the EU and NATO would benefit from them. The EUMS has a liaison element inside the SHAPE, Ally command operations. But the sharing is not really strong. It's very, very limited" (#4). One of the reasons why cooperation is difficult is that it is easier to share intelligence either bilaterally or in a smaller subset of nations rather than in the EU where sharing means that information is spread between 27 Member States (#5).

A further factor influencing cooperation attains to the capacity in collecting intelligence. EU Member States are still dependent, at least in part, on US and UK inputs. Since Brexit, EU Member States certainly continue to receive intelligence via bilateral agreements and the

potential exchange of classified information is regulated by an ad hoc agreement dating from April 2021. Nonetheless, the UK inclusion in the European Intervention Initiative framework further facilitates the exchange of information on potential or actual areas of operations (Bossong, 2018). However, the preference for bi- or minilateral formats hinders the potential of EU structures. Considering the intra-EU perspective, there appears to be a tendency in which the less the country is capable of collecting intelligence autonomously, the more it might want to be included in collaborative frameworks, as highlighted by #3, #10.

The success of cooperation also depends on how success itself is defined and how intelligence cooperation is approached. On the one hand, as argued by an interviewee, the intelligence structure in the EU is already a success, especially given that the EU – and its predecessors – was not created to become an intelligence sharing hub "but here we are at the EEAS and we are part of the EU intelligence community" (#1). Similarly, another interviewee argued that intelligence cooperation means different things to different people. "One layer is intelligence judgements [...] that can be shared in one particular way, and sitting beneath that is assessing intelligence, single source, multisource. If you go down is single source intelligence. Then you go down, another layer and there's cooperation on capability building. Then you get another layer, which actually is joint operations" (#5).

Finally, particularly in the field of intelligence cooperation, the sense of ownership over cooperation is a relevant factor in determining an effective, coherent and sustainable sharing mechanism. Starting from the assumption that a binding commitment in this field is not possible given the current legal limitations, and that unbinding or voluntary commitments usually results in missed opportunities for cooperation (#3, #10), an increased sense of ownership of the initiatives could help increasing the willingness of Member States to be involved in the cooperation. Nonetheless, this sense of ownership should also be complemented by internal coordination, at the national level, of all actors involved in intelligence and in the different branches of the State, to avoid or reduce any misalignment of positions (#10).

7 Assessment Criteria for a Peculiar Area of EU Cooperation

Similarly to ENGAGE Working Paper 9 (Sabatino et al., 2022), this working paper proposes a set of assessment criteria to evaluate security and intelligence cooperation in the EU. However, contrary to the aforementioned working paper, developing such criteria is not without methodological challenges. EU intelligence cooperation is an area where public information can hardly be accessed. Outsiders, including researchers or analysts, struggle to access fundamental, comprehensive information on EU intelligence activities, thus reducing the possibility to produce assessment criteria that are based on knowledge of the main and most important characteristics of cooperation: understanding the functioning and main impediments of intelligence cooperation should be considered a prerequisite for the development of appropriate assessment criteria.

The unique nature of EU intelligence cooperation, however, does not prevent us from developing a set of assessment criteria for EU security and intelligence cooperation. Based on the literature and the interviews with officials and experts involved in EU security and intelligence cooperation, we have determined a set of criteria that can be applied to evaluate intelligence cooperation. Proposing assessment criteria that evaluate the effectiveness, coherence and sustainability of the cooperation required the definition of these concepts, which are presented in ENGAGE Working Paper 3 (Sus et al., 2021).

Based on the literature review and the interviews, we propose the following 15 assessment criteria to evaluate EU security and intelligence cooperation:

To assess effectiveness:

- Are there institutions or other processes in place for trust-building among cooperating actors?

It is relevant to examine whether there are ad hoc forums and/or institutions that can (directly or indirectly) increase the level of trust and common understanding of security threats and how intensively and frequently are used by Member States. As confirmed by literature and by our interviews, trust and common understanding of security threats are necessary pre-conditions for effective intelligence cooperation (Seagle, 2015). Organising common trainings and workshops for officers and other staff may enhance the effectiveness of EU level cooperation.

- Is there continued support to further integrate the EU's security and intelligence cooperation?

The success of cooperation could be measured by evaluating whether, over the last years, more integration has taken place and whether there is continued support to improve security

and intelligence cooperation within the EU. As confirmed by our interviews, internal demand for more cooperation in security and defence may lead to further EU intelligence cooperation.

- To what extent do the Member States have a sense of joint ownership over EU intelligence cooperation?

Despite being aware of the difficulty in measuring perceptions, we propose to investigate the degree of the sense of ownership over the cooperation and its resultant effect on increased willingness to cooperate. This could be assessed by looking at both national declarations of support and commitment, and actual provision of intelligence products to the pertinent EU structures.

- Are procedures, roles and goals of actors involved in the cooperation clearly defined?

The assessment of the effectiveness of cooperative frameworks can be performed through the assessment of the clarity of the process. Without a clear definition of procedures and roles of the entities involved, it is difficult to assess whether cooperation is performing well or whether cooperation opportunities are being missed.

- Have communication channels been secured? Is there continuous improvement of the system to guarantee the uninterrupted and/or increased level of intelligence cooperation within the EU?

A secure and fast communication channel is a necessary pre-condition for effective cooperation. Given the fear that information may be leaked, securing those channels is essential for the sharing of intelligence. The presence of secure channels affects both the cooperation among States and cooperation between EU bodies and external actors, like NATO. The more secure the communication channels are, the faster and easier cooperation in this field would be. An example in this regard is represented by the improved cooperation between SATCEN and SIAC experienced in 2020, thanks to improved IT interlinkage through the EU OPS WAN secure connection (SATCEN, 2020, p.19). Nonetheless, further improvement of the standards and rules at the basis of intelligence sharing are advised in the Strategic Compass and by some of our interviewees.

- Are new units or processes in place to enhance the EU's situational awareness?

The literature has pointed out the need to be able to rely more on adequate and timely situational awareness (Conrad, 2021). In the EU, the European Commission indicated that it would be useful to fuse all the different pieces of information (von der Leyen, 2021). The new Strategic Compass has also emphasised that situational awareness needs more attention (Council of the EU, 2022a). This new commitment could be measured by examining whether EU institutions create a specific unit for this purpose (e.g. in the form of the Joint Situational Awareness Centre, as proposed by Commission President Ursula von der Leyen) or take other steps towards the collection and development of adequate and timely situational awareness.

- Are the means to collect information adequate for an effective multilateral cooperation in intelligence matters?

In the case of collection of information, it is useful to assess the appropriateness of the means used to collect information. This pertains to the preparedness of the personnel, the adequacy and frequency of training, as well as updates of the technical and technological instruments used.

- Are there appropriate frameworks for intelligence cooperation between EU structures and Member States during deployment? Are these agreements complemented by intelligence cooperation agreements with non-EU countries and/or institutions?

In the case of missions and operations, effective intelligence sharing between the different actors involved can be a determinant for the good results of the activities. In this regard, it could be useful to see whether appropriate frameworks for intelligence sharing in operations are in place within EU bodies and whether contributions are directed from Member States to the EU bodies and vice-versa. Similarly, intelligence sharing agreements with relevant actors (local actors, NGOs, international organisations, third countries) should also be considered and, most importantly, there should be an assessment of the actual performance of intelligence sharing.

To assess coherence:

- Is there continued support to create and sustain the necessary synergies between the internal and external aspects of EU security?

It is necessary to examine whether the "internal" and "external" aspects of EU security issues, such as terrorism, continue to be treated as synergy areas between the AFSJ and EU external action. There is a risk that these inter-linked security issues are handled separately by respective national and EU bodies. As confirmed by the literature, there is a bureaucratic interest to keep different intelligence units separate. Also, different organisational cultures impede effective cooperation between internal and external security services (Fägersten, 2015, 2016).

- Do the latest foreign and security policy challenges lead to a recognition that the fight against common threats needs more shared information between the relevant actors?

It is useful to examine whether in (previous) areas of disagreements (e.g. EU policies on Russia) there is more convergence among Member States. The literature and our interviews have pointed out that once an issue becomes an area of agreement, Member States are willing to share more information with one another (Palacios, 2020, p. 488). Therefore, it would be useful to examine whether external crises could lead to higher convergence of views among Member States.

- To what extent does coherence of interests between the EU and its Member States prevail in intelligence cooperation?

Similarly to that proposed in ENGAGE Working Paper 9 (Sabatino et al., 2022), a criterion to assess the coherence of this field of cooperation is to look at the degree of convergence of national interests with the set EU ones. The more convergence there is, the more the

cooperation can be considered to be coherent between the EU and Member States, who will also presumably be more willing to participate. Please note that this criterion also affects the sustainability of cooperation. Should interests diverge, cooperation could result in being more of a burden, rather than an added value.

To assess the sustainability of intelligence cooperation:

- Are there any (economic or other types of) savings resulting from intelligence cooperation?

One should look at the sharing of capabilities, such as satellites or other instruments used for gathering of information for intelligence purposes. Sharing capabilities means that the Member States can save resources if they use collective instruments through the EU. In some cases, particularly if Member States do not own the necessary capabilities to collect and analyse certain types of information, undertaking cooperative efforts could result in gains, both in terms of input used and output obtained.

- Do EU policymakers take democratic legitimacy into account when further developing intelligence cooperation within the EU?

Democratic accountability of EU intelligence cooperation should be taken into account. The issue of democratic legitimacy is an evergreen question, especially in CFSP/CSDP matters where democratically elected members of parliaments have limited roles. We understand that many intelligence activities (must) take place behind closed doors. At the same time, the field of intelligence could potentially demonstrate some of the features that are expected in other areas of EU cooperation, such as a clear legal basis for transparency and accountability reasons that might be also required for upholding rule of law within EU context (Conrad, 2021, p. 65). A clear definition of legal basis and procedures would also help improve the sharing of information, thanks to streamlined processes.

- Is there an appropriate number of staff working in the different fields (civilian, military, etc) of EU intelligence cooperation?

The number of people involved in the collection and analysis of intelligence and the available budget for that cooperation are additional aspects to investigate. According to the mandate of the body or agency in question, a possible way to assess its sustainability is to look at the allocated resources and the continued support of relevant bodies and units. As an example, the INTCEN started with only seven analysts (Müller-Wille, 2008, p. 62). By 2017, INTCEN's size grew to approximately 100 personnel (Seyfried, 2017, p. 2), but the literature still points out the need for a significant increase of analytical manpower and technical capacity, both in the Hybrid Fusion Cell and regional desks (Conrad, 2021, p. 65). The number of people working at INTCEN and EUMS Int, and their technical expertise, are key for a sustainable intelligence cooperation.

- To what extent does the system for the classification of information contribute to a sustainable intelligence cooperation within the EU?

With reference to the classification of information, several aspects should be considered. First, the appropriateness of the security clearance system should be assessed against its capacity to provide a clear and smooth process for the management of information. Second, it should include a mechanism to verify that all personnel with a need to know have the appropriate security clearance according to the type of information they are supposed to deal with. Third, there should be an assessment of the physical and IT infrastructures to ensure the right balance between an appropriate level of security and speedy access to classified information. Fourth, bearing in mind the current legal limitations, potential areas of improvement of EUCI should be assessed.

8 Conclusion

The working paper has proposed, in close coordination with ENGAGE Working Paper 9 (Sabatino et al., 2022), a set of assessment criteria for security and intelligence cooperation in the EU. It has suggested fifteen criteria against which this area of cooperation could be evaluated. However, developing these assessment criteria has not been without challenges: as the working paper has argued, intelligence is a field which is hardly accessible to outsiders, including to researchers or policy analysts. By its very nature, intelligence authorities – irrespective whether they are at national or EU level – seek to keep their information and their channels of communication secured. Therefore, examining the effectiveness and the impact of intensified EU-level intelligence cooperation on Europe's security has its clear limits.

These strict boundaries, however, have not prevented us from analysing EU security and intelligence cooperation. This working paper has not only provided an extensive literature review but, quite exceptionally in this research area, involved interview data in an attempt to offer a better understanding of EU security and intelligence cooperation. The interviews were conducted with current and former national or EU intelligence officers whose involvement has proved to be indispensable to overstep our existing knowledge but also to develop assessment criteria. One could argue that the existence of current arrangements – INTCEN, EUMS Int, etc. – is already a success, given that the EU was not initially created to share sensitive pieces of information between the Member States. At the same time, short- and medium-term security threats – e.g. Russia, China but also foreign direct investments or the emergence of 5G – incentivise Member States to further integrate intelligence structures due to increased shared interests.

The lack of a shared culture, history, threat perception and interests often impede an effective multilateral cooperation in intelligence matters. The legitimate fear of EU Member States that some of their information will get leaked or will be misused is indeed hard to overcome. However, recent Russian actions have not only demonstrated that EU Member States have shared interests in Europe's security, but the Ukrainian war has also clearly showed the need for more intra-European and transatlantic coordination in intelligence matters. Seemingly, there are increasingly more areas of shared interests (in the short term: Russia; in the longer term: China) where the threat of non-cooperation comes at higher price compared to more sharing of relevant information among partners and allies. A framework for the evaluation of the EU intelligence cooperation is, therefore, more necessary than ever before.

This working paper corresponds to Deliverable 5.2 of the H2020 ENGAGE project.

Reference List

Aldrich, R. J. (2012). Intelligence and the European Union. In E. Jones, A. Menon, & S. Weatherill (Eds.), *The Oxford Handbook of the European Union* (pp. 627–642). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199546282.013.0044

Arcos, R., & Palacios, J.-M. (2020). EU INTCEN: A transnational European culture of intelligence analysis? *Intelligence and National Security*, *35*(1), 72–94. https://doi.org/10.1080/02684527.2019.1649912

Ballast J. (2017). Trust (in) NATO: The Future of Intelligence Sharing within the Alliance, NATO Defence College, Research Division, Research Paper n. 140.

Bertrand N. and Bo Lillis K. (2022). *US provided intelligence that helped Ukraine target Russian warship.* CNN. https://edition.cnn.com/2022/05/05/politics/us-intelligence-russian-moskva-warship-ukraine-target/index.html

Born H., Leigh J., Wills A. (2015), Making International Intelligence Cooperation Accountable, Norwegian Parliamentary Intelligence Oversight Committee., ISBN: 978-92-9222-375-5, https://www.dcaf.ch/sites/default/files/publications/documents/MIICA_book-FINAL.pdf

Borrell, J. (2022). *Answer for question E-004266/21*. https://www.europarl.europa.eu/doceo/document/E-9-2021-004266-ASW_EN.html

Bossong R. (2018). *Intelligence Support for EU Security Policy Options for Enhancing the Flow of Information and Political Oversight*. SWP. SWP Comment n.51

Conrad, G. (2021). Situational Awareness for EU Decision-making: The Next Decade. *European Foreign Affairs Review*, *26*(1). http://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.1/EERR2021006

Copernicus. *Copernicus Service in Support to EU External Action*. Copernicus Website. https://sea.security.copernicus.eu/about-copernicus-sea/ Council of the EU. (2001a) *Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02001D0080-20080407&qid=1652789886435&from=en*

Council of the EU. (2001b). Council Joint Action of 20 July 2001 on the establishment of a European Union Satellite Centre (2001/555/CFSP)

Council of the EU. (2008). *Annual report from the Council to the European Parliament on the main aspects and basic choices of the CFSP*. http://aei.pitt.edu/43165/1/CFSP_2007.pdf

Council of the EU. (2010). *Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0427&from=EN

Council of the EU. (2011a). *Council conclusions on conflict prevention—3101st Foreign Affairs Council meeting*. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/122911.pdf

Council of the EU. (2011b). *Council Conclusions on enhancing the links between internal and external aspects of counter-terrorism. 3096th Justice and Home Affairs Council meeting, Luxembourg, 9 and 10 June 2011*. https://www.consilium.europa.eu/media/52167/122505.pdf

Council of the EU. (2013). *Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN

Council of the EU. (2014). *Council decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre and repealing Joint Action 2001/555/CFSP on the establishment of a European Union Satellite Centre,* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0401&from=EN

Council of the EU. (2015). *Taking forward the EU's Comprehensive Approach to external conflict and crises—Action Plan 2015*. https://data.consilium.europa.eu/doc/document/ST-7913-2015-INIT/en/pdf

Council of the EU. (2016). *Implementation Plan on Security and Defence*. https://data.consilium.europa.eu/doc/document/ST-14392-2016-INIT/en/pdf

Council of the EU. (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')*. https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf

Council of the EU. (2019), *Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council on the functioning of the EU Satellite Centre (2014-2019)*. https://data.consilium.europa.eu/doc/document/ST-13699-2019-INIT/en/pdf

Council of the EU. (2020). *Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1127&from=EN

Council of the EU. (2021). *Counter-Terrorism Coordinator.* The EU response to terrorism. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

Council of the EU. (2022a). *A Strategic Compass for Security and Defence—For a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

Council of the EU. (2022b). *Crisis coordination in the Council (IPCR)*. https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/

Council of the EU. (2022c). Draft twentieth annual report of the Council on the implementation of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. https://data.consilium.europa.eu/doc/document/ST-8196-2022-INIT/en/pdf

Council of the EU. (2022d). Council conclusions on the development of the European Union's cyber posture - Council conclusions approved by the Council at its meeting on 23 May 2022. https://www.consilium.europa.eu/media/56358/st09364-en22.pdf

Cross, M. K. D. (2013). A European Transgovernmental Intelligence Network and the Role of IntCen. *Perspectives on European Politics and Society*, *14*(3), 388–402. https://doi.org/10.1080/15705854.2013.817805

Dijkstra, H., & Vanhoonacker, S. (2011). The Changing Politics of Information in European Foreign Policy. *Journal of European Integration*, *33*(5), 541–558. https://doi.org/10.1080/07036337.2010.546845

Drent M., Krujver K., Zandee D. (2019). *Military Mobility and the EU-NATO Conundrum.* Clingendael Report, https://www.clingendael.org/sites/default/files/2019-07/Military_Mobility_and_the_EU_NATO_Conundrum.pdf

Dursun-Özkanca, O. (2019). The Turkish Veto over the EU–NATO Security Exchange. In Turkey–West Relations: The Politics of Intra-alliance Opposition (pp. 63-82). Cambridge: Cambridge University Press.

EEAS. (2015). *EU INTCEN Fachtsheet*. https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf

EEAS. (2016). *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

EEAS. (2019). *Crisis management and Response* [Text]. EEAS - European External Action Service - European Commission. https://eeas.europa.eu/headquarters/headquarters-Homepage/412/crisis-management-and-response_en

EEAS. (2021). European Union Military Vision and Strategy on Cyberspace as a Domain of Operations. EEAS(2021) 706 REV4. LIMITE. https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf

EUobserver. (2016). *Europol in massive data breach on terrorism probes*. EUobserver. https://euobserver.com/justice/136097

EUobserver. (2017). *EU intelligence agency not a priority*. EUobserver. https://euobserver.com/justice/138939

EurActiv. (2005, March 4). *Gijs de Vries on terrorism, Islam and democracy*. Www.Euractiv.Com. https://www.euractiv.com/section/security/interview/gijs-de-vries-on-terrorism-islam-and-democracy/

EurActiv. (2022, January 21). *EU should advance foreign intelligence-gathering capacity, EU lawmaker says*. https://www.euractiv.com/section/justice-home-affairs/news/eu-should-advance-foreign-intelligence-gathering-eu-lawmaker-says/

Eurlex. *Agreements on the security of classified information*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4300998

European Commission. (2020). *New EU Cybersecurity Strategy* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Council. (2004). *Declaration on combating terrorism*. https://www.consilium.europa.eu/media/52165/st_7906_2004_init_en.pdf

European Parliament. (2010). *Answer to Question No E-5998/09*. https://www.europarl.europa.eu/doceo/document/E-7-2009-5998-ASW_EN.html

European Parliament (2012). CSDP Missions And Operations: Lessons Learned Processes. Directorate-general For External Policies Of The Union. April. https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/457062/EXPO-SEDE_ET(2012)457062_EN.pdf

European Parliament. (2013). *Decision Of The Bureau Of The European Parliament of 15 April 2013 concerning the rules governing the treatment of confidential information by the European Parliament (2014/C 96/01)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0401(01)&from=EN

European Parliament (2018). *European Parliament resolution of 13 June 2018 on EU-NATO relations (2017/2276(INI))*. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0257_EN.pdf

Europol. (2019). *Consolidated Annaul Activity Report (2018)*. https://www.europol.europa.eu/sites/default/files/documents/consolidated_annual_activity_report_2018.pdf

Europol. (2022). *European Cybercrime Centre—EC3*. Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Extraordinary Council of Ministers. (1995). *European Security : a Common Concept of the 27 WEU Countries*. http://www.bits.de/NRANEU/docs/WEU141195.PDF

Fägersten, B. (2010). Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol. *Intelligence and National Security*, *25*(4), 500–520. https://doi.org/10.1080/02684527.2010.537028

Fägersten, B. (2014). European intelligence cooperation. In I. Duyvesteyn, B. De Jong, & J. Van Reijn (Eds.), *The Future of Intelligence: Challenges in the 21st Century* (pp. 94–113). Routledge.

Fägersten, B. (2015). *Intelligence and decision-making within the Common Foreign and Security Policy* (SIEPS European Policy Analysis). https://www.sieps.se/en/publications/2015/intelligence-and-decision-making-within-the-common-foreign-and-security-policy-201522epa/

Fägersten, B. (2016). *For EU eyes only? Intelligence and European security* (EUISS Brief Issue 8). https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_8_EU_Intelligence_Cooperation.pdf

Gruszczak, A. (2016). *Intelligence Security in the European Union: Building a Strategic Intelligence Community*. Palgrave.

Hemmer, J., & Smits, R. (2011). *The early warning and conflict prevention capability of the Council of the European Union: A Mapping of the Pre-Lisbon Period* [Clingendael Conflict Research Unit]. https://www.clingendael.org/sites/default/files/pdfs/20100300_IfP-EW_report.pdf

Hertzberger, E. R. (2007). *Counter-terrorism intelligence cooperation in the European Union* / [UNICRI Report]. UNICRI. https://digitallibrary.un.org/record/784267

Hill, C. (1993). The Capability-Expectations Gap, or Conceptualizing Europe's International Role. *JCMS: Journal of Common Market Studies*, *31*(3), 305–328. https://doi.org/10.1111/j.1468-5965.1993.tb00466.x

Hill, C. (2004). Renationalizing or Regrouping? EU Foreign Policy Since 11 September 2001. *JCMS: Journal of Common Market Studies*, *42*(1), 143–163. https://doi.org/10.1111/j.0021-9886.2004.00480.x

Hill, C., & Smith, K. E. (2000). *European Foreign Policy: Key documents*. Routledge.

Intelligence College. (2020). *Letter of Intent*. https://www.intelligence-college-europe.org/wp-content/uploads/2020/03/LoI-English.pdf

HR Decision (2012). *HR Decision establishing the organization and functioning of the EEAS Intelligence Support Architecture No. HR DEC (2012)013 dated 22 June 2012* (classified)

Intelligence College. (2022). *The College*. https://www.intelligence-college-europe.org/presentation/

Intelnews. (2017, October 6). German spy officials dismiss calls to create European intelligence agency. *IntelNews.Org*. https://intelnews.org/2017/10/06/01-2191/

International Review. (2022). *Interview with Gilles de Kerchove*. International Review of the Red Cross. http://international-review.icrc.org/articles/interview-with-gilles-de-kerchove-916

Jirat, J. (2020). The Club de Berne: A black box of growing intelligence cooperation. *About:Intel*. https://aboutintel.eu/the-club-de-berne/

Joint progress report (2019). *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

Joint progress report (2021). Six*th progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.* https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

Jones, C. (2013). *Secrecy reigns at the EU's Intelligence Analysis Centre* [Statewatch analysis]. https://www.statewatch.org/media/documents/analyses/no-223-eu-intcen.pdf

Korteweg, C. (2022). *Closer EU intelligence cooperation: Four opportunities | Clingendael spectator*. https://spectator.clingendael.org/en/publication/closer-eu-intelligence-cooperation-four-opportunities

Kozlowski, J., & Palacios, J.-M. (2014). Single Intelligence Analysis Capacity (SIAC)—A Part of the EU Comprehensive Approach. *IMPETUS - Magazine of the EU Military Staff*. https://eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-military-staff/images/impetus_springsummer_14.pdf

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence*, *16*(4), 527–542. https://doi.org/10.1080/716100467

Latici T. (2020). *Understanding EU-NATO cooperation Theory and practice.* European Parliament Research Service. October. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659269/EPRS_BRI(2020)659269_EN.pdf

Lindstrom G. and Tardy T. (edited by) (2019). *The EU and NATO. The essential partners.* European Union Institute for Security Studies, DOI 10.2815/493939

Maj. Gen. Vaz Antunes J.N.J. (2005). Developing an Intelligence Capability :The European Union, Studies in Intelligence Vol. 49 No. 4, https://www.cia.gov/static/09e29d375bb05ff28a25fb8f0504ba1e/Developing-an-Intel-Capbility.pdf

Mondial Nieuws. (2014). *Ilkka Salmi, the EU's spymaster*. MO*. https://www.mo.be/en/interview/ilkka-salmi-eu-s-007

Müller-Wille, B. (2004). *For our eyes only? Shaping an intelligence community within the EU* [EUISS Occasional Papers No 50.]. https://www.iss.europa.eu/sites/default/files/EUISSFiles/occ50.pdf

Müller-Wille, B. (2008). The Effect of International Terrorism on EU Intelligence Co-Operation. *JCMS: Journal of Common Market Studies*, *46*(1), 49–73. https://doi.org/10.1111/j.1468-5965.2007.00767.x

Norheim-Martinsen, M. (2012). *The European Union and Military Force: Governance and Strategy*. Cambridge University Press. https://www-cambridge-org.proxy-ub.rug.nl/core/books/european-union-and-military-force/A3D566BCA0E1F0C6DADE0C9A99DC599C

Official Journal of the European Union (2001). *Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&from=en

Official Journal of the European Union (2003), *Agreement Between The European Union And The North Atlantic Treaty Organisation On The Security Of Information.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22003A0327(01)

Palacios, J.-M. (2020). On the Road to a European Intelligence Agency? *International Journal of Intelligence and CounterIntelligence*, *33*(3), 483–491. https://doi.org/10.1080/08850607.2020.1754670

Pawlak, P. (2014). Political and technical aspects of information sharing. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* (pp. 83–90). EUISS.

Pawlak, P. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building*. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

Politi A. (ed) (1998). *Towards a European intelligence policy, Chaillot Paper 34, Institute for Security Studies, WEU.* December. https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp034e.pdf

Political and Security Committee. (2017). *Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17*. https://www.statewatch.org/media/documents/news/2017/jul/eu-council-pace-crisis-management-exercise-plan-11256-17.pdf

Politico. (2017a, September 4). *Commissioner calls for European intelligence system*. POLITICO. https://www.politico.eu/article/commissioner-dimitris-avramopoulos-calls-for-european-intelligence-system/

Politico. (2017b, September 27). *How Macron's EU vision stacks up to reality*. POLITICO. https://www.politico.eu/article/how-emmanuel-macron-france-eu-vision-speech-stacks-up-to-reality/

Politico. (2017c, October 5). *Germany rejects creating European intelligence agency*. POLITICO. https://www.politico.eu/article/germany-rejects-creating-european-intelligence-agency/

Pronk, D., & Korteweg, C. (2021). *Sharing the Burden, Sharing the Secrets: The future of European intelligence cooperation*. Clingendael. https://www.clingendael.org/publication/future-european-intelligence-cooperation

Sabatino, E., Edouard, S., Breuer, F. & Renaut, J. (2022). *Developing Assessment Criteria for Defence Cooperation in the EU.* ENGAGE Working Paper. https://www.engage-eu.eu/wp9

Sánchez Amor, N. (2021). *The need for an EU intelligence service*. https://www.europarl.europa.eu/doceo/document/E-9-2021-004266_EN.html

SATCEN. *SATCEN supports EUNAVFOR MED Operation IRINI with geospatial intelligence services.* https://www.satcen.europa.eu/page/satcen-supports-eunavfor-med-operation-irini-with-geospatial-intelligence-services

SATCEN (2020). *Annual Report 2020.* Publications Office of the European Union, 2021, https://www.satcen.europa.eu/keydocuments/SatCen%20Annual%20Report%202020_WEB6090fe685f405a0001df8eaf.pdf

Seagle, A. N. (2015). Intelligence Sharing Practices Within NATO: An English School Perspective. *International Journal of Intelligence and CounterIntelligence*, *28*(3), 557–577. https://doi.org/10.1080/08850607.2015.1022468

Seyfried, P. P. (2017). *A European Intelligence Service?: Potentials and Limits of Intelligence Cooperation at EU Level*. Federal Academy for Security Policy. https://www.jstor.org/stable/resrep22196

Sus, M., Vandendriessche, M., Saz-Carranza, A., Gruni, G., & De Esperanza, C. (2021). *Towards Effective, Coherent and Sustainable EU External Action: Laying the Ground for the ENGAGE White Paper*. ENGAGE. https://www.engage-eu.eu/publications/towards-effective-coherent-and-sustainable-eu-external-action

Van Buuren, J. (2009). *Secret Truth: The EU Joint Situation Centre*. Eurowatch. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=46402A9AAFD8890AB2A159E28921B077?doi=10.1.1.366.3625&rep=rep1&type=pdf

Vimont, P. (2014). The European External Action Service and complex crises. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* (pp. 35–38). EUISS.

von der Leyen, U. (2021). *State of the Union Address by President von der Leyen* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

WEU (1994). *Assembly of the Western European Union, Fortieth ordinary session (First part), Document 1421*. 19th May. http://aei.pitt.edu/53126/1/B0873.pdf

WEU. (1995a). *Annex 13—Lisbon Declaration (excerpts)*. http://www.nzdl.org/cgi-bin/library?e=d-00000-00---off-0aedl--00-0----0-10-0---0---0direct-10---4-------0-0l--11-en-50---20-about---00-0-1-00-0--4----0-0-11-10-0utfZz-8-10&cl=CL1.3&d=HASH80329ac5344ee3d84b07fa.4.9&gt=1

WEU. (1995b). *European Security: A Common Concept of the 27 WEU Countries*. http://www.bits.de/NRANEU/docs/WEU141195.PDF

Authors

Viktor Szép is a postdoctoral researcher at the Faculty of Law at the University of Groningen. His research focuses on EU foreign and sanctions policy. Recent publications include: "New intergovernmentalism meets EU sanctions policy" (Journal of European Integration, 2020) and "EU sanctions policy and the alignment of third countries: relevant experiences for the UK?" with Peter Van Elsuwege (In. J. S. Vara, R. A. Wessel & P. R. Polak (eds.): The Routledge Handbook on the International Dimension of Brexit, 2020).

Ester Sabatino is a research analyst for the Defence and Military Analysis Programme at the International Institute for Strategic Studies (IISS), conducting research on the EU's Common Security and Defence Policy, as well as contributing to the programme's wider research projects. Before joining the IISS, Ester was a researcher in the defence programme at the Istituto Affari Internazionali in Rome. She previously worked in the private sector, in a consultancy firm. Ester is the author and editor of numerous reports, articles and papers on EU defence-industrial cooperation, military capabilities and defence policies.

Ramses A. Wessel is a professor of European Law and head of the Department of European and Economic Law at the University of Groningen. His research expertise is in EU external relations law, EU foreign and security policy, international organizations and the relations between legal orders. He published widely on the legal dimensions of the European Union as a global actor. Ramses is vice-president of the European Society of International Law (ESIL), and member of the Governing Board of the Centre for the Law of EU External Relations (CLEER) in The Hague. He is the editor of several international journals in the field, including the European Foreign Affairs Review.

ENGAGE

ENVISIONING A NEW GOVERNANCE ARCHITECTURE FOR A GLOBAL EUROPE

Working Paper Series

The ENGAGE Working Papers are peer-reviewed publications based on research from the EU Horizon 2020 funded project no. 962533, entitled *Envisioning a New Governance Architecture for a Global Europe,* which runs from January 2021 to June 2024.

ENGAGE examines how the EU can effectively and sustainably meet strategic challenges by harnessing all of its tools to become a stronger global actor. As a starting point, the project defines the challenges of global governance and international relations, as well as the acceptability of advancing EU external action among citizens and policymakers. Taking a comprehensive approach, ENGAGE also maps and assesses the EU's capabilities, governance structures and strategic objectives in the realms of CSDP, CFSP, external action and 'external action plus'.

Thirteen leading universities and think tanks work together within ENGAGE to facilitate knowledge exchange between researchers and foreign policy practitioners. Through this convergence of expertise and backgrounds, ENGAGE is uniquely placed to offer policy advice on how the EU can more effectively engage with strategic partners and neighbourhoods, support conflict prevention, mediation and resolution, and ultimately have a stronger voice in the world.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 962533.