Bossong, Raphael

Research Report

Intelligence support for EU security policy: Options for enhancing the flow of information and political oversight

SWP Comment, No. 51/2018

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bossong, Raphael (2018) : Intelligence support for EU security policy: Options for enhancing the flow of information and political oversight, SWP Comment, No. 51/2018, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/256539

SWP

SWP Comment

NO. 51 DECEMBER 2018

Intelligence Support for EU Security Policy

Options for Enhancing the Flow of Information and Political Oversight

Raphael Bossong

Since 2015, security cooperation between European Union (EU) member states has progressed at an accelerated pace. For the Union's foreign, security, and defence policy, there is the prospect that increased cooperation and enhanced arms cooperation will create more international capacity to act. As far as internal security is concerned, the continuing threat of terrorism is spurring the establishment of a "European Security Union" based on an intensive exchange of information between security authorities. In the shadow of these developments is the question of the extent to which European intelligence cooperation should also be promoted. In this particularly sensitive area, no steps towards integration that would attract public attention are to be expected. However, existing approaches to intelligence support for EU security policy should be deepened and better monitored.

According to the Lisbon Treaty, national security is solely the responsibility of the member states (Art. 4 (2) TEU [Treaty on European Union]). For this reason alone, the idea of a common European secret service, which has been repeatedly floated since the mid-2000s, remains out of the question. It is also clear that the EU cannot play a direct role in particularly sensitive areas of intelligence work, such as large-scale technical reconnaissance, the management of human sources, or the execution of covert operations. However, EU security policy allows for indirect access to intelligence. Particularly in the fight against terrorism, the intersections between European Police Office (Europol) or EU data systems and information from domestic intelligence services are growing. Meanwhile, the EU can draw on strategic risk and situation analyses for its foreign policy action — analyses that are synthesised in the European External Action Service (EEAS) from reports by various national services. These procedures should be made more transparent and discussed more openly to support a gradual and proportionate development of intelligence capabilities for the internal and external security of the EU in the coming years.

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Confidential analyses for European foreign and security policy

In 2002, the exchange of national intelligence information began in the so-called Joint Situation Centre (SITCEN) of the EU Council Secretariat. Its primary purpose was to support EU missions abroad and to contribute to a common assessment of terrorist threats. The methods established informally at the time are still valid today: Member states voluntarily transmit finished intelligence reports to the EU. A common situation analysis and options for European action are then derived from the range of national contributions. Openly accessible information, reports from European delegations, and findings from the EU Satellite Centre complement this work of analysts seconded to the EU by their national intelligence services.

In addition, the EU Military Staff, which emerged from the Western European Union, was able to maintain its access to military intelligence. Its internal Intelligence Directorate prepares confidential military situation analyses, which are especially needed to plan and conduct EU missions in high-risk theatres of operation, such as the Democratic Republic of Congo and Somalia. For the purposes of an integrated European foreign policy, cooperation between the Intelligence Directorate and the civilian SITCEN was formalised in 2007 and has since been run as the EU's Single Intelligence Analysis Capacity (SIAC). In 2011, the Joint Situation Centre SITCEN was renamed the EU Intelligence Centre (INTCEN) and integrated into the then newly established EEAS. INTCEN now has around 100 employees, approximately 60 of whom are involved in intelligence analysis. Together with the Military Intelligence Directorate, the EU-SIAC has around 80—90 intelligence liaison officers and analysts.

The EU-SIAC evaluations are made available to both EU bodies and decision-makers in national capitals. They provide a more comprehensive security picture than most EU member states could develop on their own. However, it can be assumed that member states often keep operationally relevant or particularly valuable intelligence to themselves. Therefore, the value of the EU-SIAC lies, above all, in its strategic and longer-term analysis. In the best case, however, a joint confidential assessment can also be drawn up in acute crises. Examples would be the occupation of the Crimea or the nerve gas attack in Salisbury, UK. Such common European intelligence analyses can have a direct impact on the foreign and security policy responses of the EU and its member states.

Coalitions of the willing to enhance the intelligence supply

The standards that have hitherto applied to intelligence work tend to stand in the way of a deepening of this voluntary cooperation. Already at the national level, sensitive intelligence is mostly passed on when this is absolutely necessary (need to know), not when it is available (need to share). However, the larger changes in Europe's wider security situation mean that the structural need for more intelligence exchanges must be reassessed. Brexit will exert additional pressure for reform, since the expertise of British staff in the EU-SIAC will be lost.

In concrete terms, a coalition of EU member states could embark on the path of closer cooperation in the field of Common Foreign and Security Policy (CFSP) under Article 329 of the Treaty on the Functioning of the European Union (TFEU). Since the EU-SIAC is already regarded as a component of the CFSP and the EEAS, a deepening of these structures would not have to come into conflict with national prerogatives in the area of national security (Art. 4 (2) TEU). The participating member states could commit to a division of labour and direct their respective national intelligence services to work on jointly agreed thematic and regional priorities. Furthermore, they would also commit to feeding related intelligence assessments reliably into the EU-SIAC. This enhanced cooperation could lead to a European circle of intelligence analysis: The

planning and prioritisation of intelligence resources (first phase) would be more intensively coordinated at the European level. The collection of raw intelligence (second phase) and its first processing (third phase) would remain at the national level. The final secondary evaluations in the EU-SIAC and the dissemination of finished intelligence reports to decision-makers (fourth phase) could, therefore, be of higher quality — and, in turn, shape future intelligence priorities in a new iteration of the cycle.

In parallel, political forums could be strengthened in order to improve the use of intelligence for policy-makers. At the working level, this would mean expanding the role of the Political and Security Committee. The idea of a high-level European Security Council, as repeatedly proposed by Chancellor Angela Merkel, is also under discussion. Such a Security Council would offer particular advantages when it comes to intelligence issues. The services of the member states, which are generally assigned to different line ministries, could be brought together at the level of the Heads of State and Government. At the same time, such a Security Council could operate with a high degree of confidentiality and enhance strategic decision-making.

However, at the level of Heads of State and Government, as with most CFSP issues — including authorisation for enhanced cooperation — the principle of unanimity applies. If this were to result in political blockades with regard to the proposed increase in intelligence cooperation, member states would be free to embark on intergovernmental cooperation independent of the EU. This approach would also be in line with the provisions of Article 73 TFEU on cooperation in the field of national security. However, such an approach risks a further fragmentation of the European security architecture. There is already tension between Permanent Structured Cooperation (PESCO), in which 25 member states want to participate, and the more recent French European Intervention Initiative (EI2), which is currently comprised of 10 European states, including the United Kingdom. The EI2 is meant to increase the operational capabilities of European military forces in the neighbourhood. If this ambition materialises, it will lead to a common interest of the EI2 states in high-quality intelligence information on potential or actual areas of operation. The more exclusive membership of the EI2 supports the necessary confidentiality for increased intelligence exchanges, while the United Kingdom can throw in its leading capacities for technical reconnaissance and security relationship with the United States. In order to prevent the EI2 from splitting PESCO and to keep from losing sight of the importance of the civilian CFSP, the EU-SIAC should therefore be supported by the broadest possible coalition of member states within the framework of enhanced cooperation under EU law. From the perspective of PESCO, joint projects for technical reconnaissance and intelligence analysis could also be envisaged in the medium term.

Personal data for the purposes of combating terrorism and enhancing internal security

As far as internal security is concerned, the terrorist attacks of 13 November 2015 in Paris boosted the level of intelligence exchanges in Europe. France sent sensitive intelligence leads to Europol, especially to obtain cross-checks by using the US Terrorist Finance Tracking Program, for which Europol has served as the central European interface since 2010. Other EU member states that had previously been reluctant to cooperate with Europol subsequently shared their data on so-called foreign fighters. As part of this dynamic, the European Counter Terrorism Centre (ECTC) was set up within Europol at the beginning of 2016; together with a new version of Europol's legal mandate, this opened up new opportunities for cooperation. Article 2 of this reformed regulation keeps it open as to which national "competent authorities" responsible for combating and preventing

serious crimes can be involved in Europol working processes. At least some member states have taken steps to further involve their national security authorities that exercise both police and intelligence functions.

Looking at the operational dimension, the number of entries on Islamist terrorism and foreign combatants in the Europol Information System (EIS) increased significantly. In parallel, a closed user group for national anti-terrorist authorities was created inside the SIENA (Secure Information Exchange Network Application) data network between Europol member states. This closed group should allow for more confidential communication and can also contribute to an increased exchange of more sensitive intelligence. At the initiative of Germany, an additional steering group of national anti-terrorist authorities was set up within the ECTC to improve cross-border investigations and information processing.

Meanwhile, Europol is seeking access to particularly useful biometric information that American services and armed forces collect on suspected terrorist fighters around the world. Such data can be cross-checked in the context of external border controls as well as in the so-called EU hotspots for registering irregular immigrants and asylum-seekers. In the summer of 2018, the EU also agreed that all member states have to upload alerts for suspected terrorists into the common Schengen Information System (SIS). The SIS has served as a central information network for police and border control authorities since the mid-1990s and has long been supplemented informally with inputs from intelligence services. In the future, Europol should participate in the analysis of Passenger Name Records (PNR) data and support the management of a pan-European warning list. This list is to prevent third-country nationals who do not require a visa, but who are suspected of committing serious crimes, from entering the Schengen zone. The "no-fly list" and related border control practices of the United States, which serve as a model for the EU, are based on a common data platform between police and intelligence authorities. Finally, Europol is in the process of negotiating agreements on the exchange of personal data with the Maghreb states of Egypt, Tunisia, Algeria, and Morocco, as well as with Jordan and Israel. All these countries maintain close links between intelligence services and police structures in the fight against terrorism.

On the part of the European domestic intelligence services, cooperation in the context of the so-called Counter Terrorism Group (CTG) was significantly deepened. The CTG comprises all EU member states as well as Norway and Switzerland, and was established in 2001 as a working group of the Bern Club, which has served as an informal platform for combating international terrorism and countering espionage since the 1970s. Despite these long-standing intelligence relations, the CTG initially worked on a case-by-case basis and engaged in rather sporadic consultations with the EU. In 2016, however, the CTG opened permanent headquarters in The Hague. There, liaison officers of the participating intelligence services can access their respective national information systems as well as edit a common database. This should provide for a much more comprehensive picture of terrorist networks in Europe. In addition, the permanent liaison officers in the CTG should help to carry out cross-border investigations and surveillance measures as seamlessly as possible.

Strengthening the links between police authorities and intelligence services

In view of the parallel growth of Europol and the CTG, one can pose the question whether there is potential for structural mutual cooperation. Since 2001, many Western states have established procedures for the exchange of intelligence between police and intelligence services. In Germany, the Joint Counter-Terrorism Centre (GTAZ) is an example of this development. In the summer of 2018, the governing

German Christian Democratic Party (CDU) proposed a European data platform comparable to the GTAZ for combating terrorism, organised crime, and illegal migration.

Apart from the lack of EU legal competence, there are numerous practical obstacles to such a proposal for permanent intelligence fusion. Europol has not yet been able to guarantee the full intelligence standard of secrecy in its information systems, while it is also subject to a strict data protection regime. This collides with the classic approach to intelligence cooperation, in which the transmitting state retains control over shared information (Third-Party Rule). Data entries can indeed be marked in Europol's databases in order to restrict their further use. However, this technical system of handling codes does not replace the higher level of confidentiality and interdependence in bilateral intelligence relations.

Moreover, among the 30 member states of the CTG, there are differing views on its role and status. For example, the German government was initially extremely reluctant to respond to parliamentary questions about the group with reference to the core national security interests of the state. The Dutch supervisory authorities, in contrast, dealt with the CTG's working methods in publicly accessible reports. In other European countries, international intelligence cooperation is often conducted without an explicit legal basis. Meanwhile, the participating intelligence services argue that mutual trust is still being built up and that the principle of voluntary and flexible cooperation must be maintained. In this respect, despite growing support for the CTG, it is not yet possible to speak of a consolidated institution that could be formally integrated into a European platform for intelligence fusion.

Nevertheless, sporadic contacts with the EU level could be intensified, for example by placing CTG liaison officers at Europol's ECTC. Members of national security authorities with both police and intelligence tasks, for example from Sweden or Austria, could act as a bridge. In this way, information from the CTG platform could be regularly fed into the EIS and contribute, for example, to the screening of irregular immigrants in EU hotspots. On the other hand, the same liaison officers could ensure that relevant entries from EU databases for police cooperation or migration control are relayed back to the CTG.

If such a regular exchange of information proves its worth through the increased reporting of hits at EU external borders or through other measures for the prevention of terrorism, a stepwise expansion of mutual cooperation can be considered along the lines of the German GTAZ. This model implies that police and intelligence services can jointly discuss and assess individual suspects and cases. Despite intermittent and unavoidable intelligence failures in the fight against terrorism, such direct consultations are widely considered to be indispensable at the national level. Transposed to the European level, this would mean that Europol and the CTG would hold joint discussions and recommend concrete measures on persons of interest to national security authorities. A refusal to act on such recommendations would require an explicit justification by national security authorities. Thus, even without a direct EU-competence to coordinate operations in the field of national security, such a platform and cooperation model would in all likelihood boost cross-border cooperation.

For other forms of serious crime, the foundations for similar data platforms are already in place. Since 2016, Europol has been operating the European Migrant Smuggling Centre (EMSC), which contributes to confidential risk assessments and law enforcement measures. The European Cybercrime Centre (EC3) at Europol works with both a police and an intelligence agency from the United States as well as with the Federal Bureau of Investigation and the Secret Service in the context of the so-called Joint Cybercrime Action Taskforce (J-CAT).

Rule of law and democratic supervision

The National Security Agency (NSA) scandal made it clear that the international activities of the intelligence services are often beyond the control of national supervisory authorities. Since then, controversial political debates and the actions of European courts have led to the first reforms. In Germany, for example, the legal foundations and supervisory bodies of the Federal Intelligence Service have been reorganised. The European Court of Justice urged Sweden and the United Kingdom to apply more restrictive rules to the retention of mass communication data for the purposes of threat prevention and law enforcement. Similarly, in September 2018, the European Court of Human Rights called for a more precise definition of the powers of British intelligence services to collect and analyse mass communications data. In principle, all European states face major challenges in ensuring effective control over their intelligence services under the conditions of technical progress and globalisation. The debate on the rule of law within some EU member states underlines the importance of preserving fundamental rights in core areas of national security.

The EU does not play a direct role in mass surveillance, nor is personal data processed in the EU-SIAC. Nevertheless, one needs to ask critical questions about the supervision and democratic legitimacy of this aspect of the EU's foreign and external security policy. Mistaken or wrongful policy decisions, which may be made on the basis of common intelligence assessments, can erode the EU's legitimacy. Just as at the national level, it must remain possible to attribute political responsibility in this context. This means, for example, that representatives of other democratic institutions, such as Members of the European Parliament, must be given the power to review confidential documents in the Council (or a future European Security Council).

In the field of internal security, further questions arise about the legality of intelligence cooperation. Any answers must take into account the EU Charter of Fundamental Rights, recent EU data protection laws, as well as national constitutional traditions, such as the German requirement for separations between police and intelligence services. These legal challenges cannot be avoided by flexible forms of cooperation with intelligence services. Rather, the greatest possible transparency is required when using low-level or informal procedures, such as the use of liaison officers. Only in this way can problematic developments be addressed at an early stage instead of having them emerge through scandals afterwards, as in the case of the NSA leaks.

According to Article 43 (4) of Europol Regulation (EU) 2016/794, the European Data Protection Supervisor has, in principle, access to all data, including classified information. This is a cornerstone of the constitutional supervision of Europol. Intelligence services should accept this external control and, more generally, adopt less restrictive interpretations of the so-called Third-Party Rule in the context of exchanges with European oversight bodies. In addition, a Joint Parliamentary Scrutiny Group (JSG) on Europol was established in 2017. The practical experience with this new body of national and European parliamentarians, which meets every six months, is still too limited to draw meaningful conclusions. Due to the mixed nature of the supervisory body, however, one possible priority area could be to monitor the intelligence interfaces at Europol. National parliamentarians can assert information rights in the area of national security, rights to which European representatives are not entitled because of the EU's competence restrictions under Article 4 (2) TEU. The JSG on Europol could therefore act as a building block for a more comprehensive or networked supervision of the EU's indirect interactions with intelligence services.

The Dutch supervisory authority published a first report on the reformed CTG in February 2018. The report stressed the need to strictly examine the proportionality of data processing and underlined that the

participating services hold collective responsibility. However, a follow-up project on networking the supervisory authorities of five European countries (Belgium, Norway, Denmark, the Netherlands, Switzerland) showed that national legislation makes it largely impossible to discuss matters of common interest, which are mostly highly classified. National supervisory authorities have, in any case, hitherto rather divergent powers to access intelligence databases, or to acquire information about the working methods, techniques, and international cooperation of their respective national intelligence services.

Even though the EU will not be given the competence for legal harmonisation in this area in the foreseeable future, European member states should gradually reduce these obstacles and cross-national divergences. As a first step, the national legal bases for international cooperation between intelligence services should be clarified and subjected to regular supervision. At the same time, the objective should be to guarantee a higher level of legal protection if it is not a question of general reconnaissance abroad but of intelligence surveillance of EU citizens. In the case of persons suspected of serious crimes or terrorism, there are numerous other instruments available within the EU for police cooperation, information gathering, and the preservation of evidence that are linked to criminal proceedings under the rule of law. Therefore, consideration should not only be given to the continued expansion of intelligence-led policing when it comes to cooperation between domestic intelligence services and police authorities. Instead, the other direction should also be considered, that is, a return as far as possible to the more narrowly defined area of law enforcement and prosecution.

Conclusions and outlook

The role of intelligence services in the further development of EU security policy must be given greater consideration. This particularly sensitive aspect of national sovereignty will not be able to be directly integrated into the EU institutional structure in the foreseeable future. Beyond the EU, there are numerous multilateral forums and traditional relationships between intelligence services. Examples are the European partners (SIGINT Seniors Europe) of the transatlantic Five Eyes Alliance, NATO's military intelligence, and the Police Working Group on Terrorism, also decades old, for the European fight against terrorism. These overlapping as well as functionally differentiated networks of European intelligence services, which branch out further on a bilateral level, will largely have to be preserved due to the equally complex transnational threats and risks they are intended to counter.

However, the EU member states should not only follow old path-dependencies, but also develop their own ideas about what kind of intelligence support is needed for an effective EU security policy. The impending Brexit and increasingly volatile transatlantic relations are increasing the pressure for reform. Rather than holding fruitless and symbolic debates about a common intelligence service, member states should make the collection of intelligence and its transmission to the EU much more reliable, while also maintaining the coherence of the EU's foreign and security policy. In the context of voluntary coalitions and PESCO, enhanced cooperation in the medium term may also include joint research and procurement projects for signals intelligence.

European intelligence cooperation in the fight against terrorism is comparably more advanced already. Nevertheless, it remains necessary to strengthen the established channels in a stepwise manner. Once a systematic and controlled rule-of-law deployment of liaison officers between Europol and the CTG has proved its worth, one could conceive of a more advanced platform for police and intelligence services at the EU level.

In any event, member states should promote both the powers and cross-border networking of their national supervisory authorities. At the very least, the reformed CTG and Europol's evolving interfaces must be monitored as closely as possible by administrative supervisory or data protection authorities as well as parliamentary bodies. Traditional standards for intelligence work, such as the Third-Party Rule or strict classification rules, must be reviewed. In the long term, a European convergence of supervisory regimes should be pursued in order to create a resilient basis for all forms of European and international intelligence cooperation.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

(English version of SWP-Aktuell 66/2018)

Dr Raphael Bossong is an Associate in the EU/Europe Division at SWP.