Politeja
No. 4(79), 2022, pp. 131-150
https://doi.org/10.12797/Politeja.19.2022.79.08

Artur GRUSZCZAK
Jagiellonian University in Kraków
artur.gruszczak@uj.edu.pl

INTELLIGENCE FUSION FOR THE EUROPEAN UNION'S COMMON SECURITY AND DEFENCE POLICY

ABSTRACT The data fusion methods, techniques and tools are regarded as a remedy for shortcomings of information/knowledge management and intelligence production. They also address current needs of the holistic, all-source approach to intelligence. Their implementation means the creation of new organizational elements – 'fusion centers'. The concept of a fusion center has been introduced to and tested in the European Union for years. This paper examines data fusion processes and elements within the EU and focuses on intelligence fusion capabilities developed under the Common Security and Defence Policy (CSDP). The examples of the Single Intelligence Analysis Capacity (SIAC) and EU Hybrid Fusion Cell in the Intelligence and Situation Center (INTCEN) are examined to evaluate challenges, opportunities and limitations of EU intelligence fusion elements. This paper is also an effort to indicate that there are still many elements to be improved within the EU intelligence establishment, including the area of data and information fusion – with the overall aim to effectively and timely support CSDP. Intelligence sharing by Member States with the EU remains one of the main impediments.

Keywords: intelligence, intelligence fusion, SIAC, EU INTCEN, European Union, security, Common Security and Defense Policy

INTRODUCTION

Modern intelligence relies increasingly on technological solutions and professional skills applicable for the management and analysis of large volumes of information and data stored in databanks and repositories, also available on a commercial basis from private companies. The integration and processing of data/information to meet the requirements and needs of security and defence sectors still is a significant challenge for national intelligence and security services. This is mainly due to the fact that the data and information needed are available from many different sources, providers, and brokers. Numerous efforts have been expended to meet this challenge. This was accompanied by efforts to effectively manage and integrate big volumes of data ('Big Data'). This specific phenomenon can be defined as high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.

The invention and introduction of data fusion techniques, and subsequent establishment of fusion centers, was not an exclusive security phenomenon, responding to national security strategies and action plans. It also emerged at the level of international organizations having a strong security and defense agenda, elements involved in organization and launching international military operations, as well as crisis management, internal security and law enforcement activities.

The European Union is an interesting case in this regard. It has launched many efforts within the security domain, also involving elements of political, military, economic, social and cultural dimensions. The EU adopted and pursued a coordinated stance in order to be prepared for consequences of the rapidly changing security environment, and particularly to cope with new challenges and threats posed by political and criminal factors, extremism, radicalism, terrorism and transnational organised crime. Different EU initiatives and activities focused on increasing efficiency and reliability of decision-making mechanisms at the EU level. They depend increasingly on accurate, timely and trustworthy situational assessments, threat analyses and intelligence estimates.

The concept and models of a fusion center capable to integrate data/information collected, collated, retrieved from scattered sources, and then 'fuse' them by a single analytical unit in order to convert them into intelligence has been tested in relevant EU bodies already for years. With the advent of new technologies of data gathering, data and text mining, new analytical methods, techniques and tools, including Big Data, the European Union has made an effort to implement elements of data fusion and build more effective intelligence processes and procedures.

This paper examines the state of data fusion processes at the EU level, focusing on intelligence fusion capabilities developed under the Common Security and Defence Policy (CSDP). The EU Hybrid Fusion Cell, as part of the analytical capabilities of the EU Intelligence and Situation Center (INTCEN), and the Single Intelligence Analysis

Capacity (SIAC) serve as case studies to examine opportunities and limitations of EU-based data/information fusion. It aims at answering questions which address the most tangible aspects of intelligence fusion in the EU: How is this process embedded in the EU's institutional setting, especially in the field of CSDP? What kind of cooperation between the EU institutions and Member States' civil and defense intelligence organizations has been worked out thus far? Which determinants have been critical for the effectiveness of data/information fusion at the EU level?

The main argument developed throughout this paper holds that efforts to implement data/intelligence fusion for the EU's Common Security and Defence Policy have been limited and achieved a reduced impact on international security. This is mainly due to ineffective data/information sharing system by national authorities, as well as supranational agencies and bodies supporting CSDP. This continues to be a problem despite political decisions and efforts at building an institutional framework at the EU level, as well as creating processes, procedures and IT systems able to secure delivery of information and intelligence by EU Member States.

This article was framed by the concept of intelligence fusion as an element proving advantages and necessity of all-source analysis. This concept was juxtaposed with legal and institutional design of intelligence cooperation system in the EU. The research process was based on a deductive strategy focused on the critical exploration of knowledge, content analysis of primary sources and the logic of causality. Desk research was utilized as a technique to process data extracted from a variety of sources: documents, reports, academic literature and the web repositories. Anonymized qualitative data acquired from interviews with EU officials and national intelligence officers conducted by the author in the past ten years served as an important reference.

The article is organized in four main sections. The first contains the theoretical framework, explaining the concept of intelligence fusion. The next section presents the role of intelligence in the shaping of the CSDP. It is followed by a section dedicated to the Single Intelligence Analysis Capacity (SIAC), analytical setup for pooling contributions provided by Member States' civilian intelligence organizations (CIO) and defense intelligence organizations (DIO) contributions. The last part discusses the Hybrid Fusion Cell and opportunities and limitations of intelligence support to the EU's CSDP.

INTELLIGENCE AND DATA FUSION

Intelligence fusion has already established itself in local security environments, community policing, and national security systems. Terrorist attacks on Washington, D.C. and New York City, which shook the world on the 11th of September 2001, generated a strong impetus to massive development of fusion centers and refinements of data/information fusion methods, techniques and tools. 20 years after 9/11, 80 fusion centers certified and accredited by the US Department of Homeland Security, employing nearly 3,000 personnel and having budgets which amount in total to USD 330 million

a year, have been established as main analytical elements within the federal, state and local security environments.[1]

In response to the terrorist menace, fusion centers have also been established at the national level in numerous states of the European Union.[2] The first such center was set up by the French government in 1984. The Co-ordination Unit of the Fight Against Terrorism (Unité de Coordination de la Lutte Anti-Terrorism, UCLAT) was created to coordinate and integrate efforts of all units and authorities fighting terrorism. It operated at the strategic level, coordinated intelligence collection and data fusion processes and supported operational elements of counterterrorism forces.[3] A similar fusion center, focused on counterterrorism, was established at the same time in Belgium.[4] The post-9/11 escalation of terrorist threats world-wide, and the spectacular deadly attacks carried out by jihadist terrorists in Spain, UK and the Netherlands in the mid-2000s, reinforced the commitment of the EU governments to create new fusion centers or reorganize those already at the full operational capability.[5] A number of them were set up in several European countries.[6] With the rapid advancement of sophisticated information and computer technologies, the increasing interest in facilitating and improving a cross-sectional and multi-source data processing and analysis, brought the concept of data fusion to close attention of state security institutions, including intelligence agencies.

The complex architecture of crime networks, their sophisticated communication systems and deep clandestinity forced the governments to exploit more effectively scattered, singled, often isolated data, acquired – sometimes accidentally – by law-enforcement agencies, border guards, financial intelligence units and intelligence services. The necessity to 'connect the dots', i.e. the ability and capacity to draw knowledge-loaded materials from segmented institutions and out of dispersed sources, has been a significant challenge and a difficult task with increasing threats from terrorism and organised crime. Data/information fusion methods, techniques and tools were perceived and introduced to everyday analytical practice as a remedy for shortcomings of data/

1 C. Farivar, "20 Years after 9/11, 'Fusion Centers' Have Done Little to Combat Terrorism", *NBC News*, 11 September 2021, at https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949, 14 September 2021.

2 Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Antwerp 2010; G. Persson, *Fusion Centres – Lessons Learned: A Study of Coordination Functions for Intelligence and Security Services*, Stockholm 2013.

3 O. Brun, "UCLAT", in H. Moutouh, J. Poirot (eds), *Dictionnaire du renseignement*, Paris 2018, pp. 799-800.

4 R. van der Veer, W. Bos, L. van der Heide, *Fusion Centres in Six European Countries: Emergence, Roles and Challenges*, The Hague 2019, pp. 3, 5.

5 A survey on fusion centers across Europe prepared by the Belgian Standing Intelligence Agencies Review Committee in 2009 includes twenty such national entities, surprisingly missing France and the UK. See Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe...*

6 France, Germany, the United Kingdom, the Netherlands, Belgium, Spain, Italy, Denmark.

information sharing and intelligence production. It has met the main operational requirement of an integrated approach to intelligence based on all-source information collection and analysis.[7]

Data/information fusion should be considered as an adaptive and multi-level process in which data acquired from multiple sources are aggregated, processed and integrated to fused information, which is of a greater added value than any of its parts.[8] According to Dennis Buede and Edward Waltz, data fusion means *an adaptive knowledge creation process in which diverse elements of similar or dissimilar observations (data) are aligned, correlated, and combined into organized and indexed sets (information), which are further assessed to model, understand, and explain (knowledge) the make-up and behaviour of a domain under observation*.[9]

Data fusion methods, techniques and tools bring together data and information obtained from various sources. It is done in the fusion center: a single physical location where correlation, combination, assessment and fusion can take place in a secure, stable and professional environment.[10] A fusion center is a large data clearing house where information is collected, collated, securely stored, scrutinized, interpreted and analyzed, and finally converted into intelligence (so-called intelligence product).[11]

From an organisational perspective, fusion center is a territorially located collaborative effort of various stakeholders: both traditional (such as law-enforcement services, intelligence agencies, diplomatic services) and non-traditional (such as public safety entities, social services, non-governmental organizations (NGO) and the private sector, all collectors of data and information.[12] Resources, expertise and technical means are pooled in a fusion center with the goal of maximizing organization capabilities to detect, identify, prevent, investigate, and respond to security threats. Thus, a fusion center is focused on both the strategic requirements of early warning and situational/risk awareness, as well as on operational tasks, especially with regard to the quick and efficient prevention of and response to threats and hazards suddenly emerging in the area of individual and public safety as well as national and international security.

Fusion centers have spurred mixed reactions. However, the need to consolidate data and information sources with a network-centric analytical facility has raised no doubts. Many efforts have been taken at the regional, national and international levels

[7] See B. Connable, *Military Intelligence Fusion for Complex Operations: A New Paradigm*, Santa Monica, CA 2012, p. 1.

[8] E. Blasch, "Information Fusion for Decision Making – Designing Realizable Information Fusion Systems", in E. Shahbazian, G. Rogova, P. Valin (eds), *Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, Amsterdam 2005, p. 5.

[9] D. Buede, E. Waltz, "Data Fusion", in *McGraw Hill Encyclopedia of Science and Technology*, New York 1998.

[10] R. Graphia Joyal, *State Fusion Centers: Their Effectiveness in Information Sharing and Intelligence Analysis*, El Paso 2012, pp. 60-62.

[11] A. Gruszczak, "Establishing an EU Law Enforcement Fusion Centre", *European Journal of Policing Studies*, vol. 4, no. 1 (2016), p. 110.

[12] G. Persson, *Fusion Centres – Lessons Learned...*, p. 15.

to integrate many different stakeholders to a common framework for data/information/knowledge delivery, assessment, analysis and production. The United States, especially in the aftermath of 9/11, has expanded and strengthened data fusion centers, predominantly at the state level. They were tasked, in addition to criminal intelligence and intelligence-led law enforcement, with counterterrorism, mainly to support relevant federal authorities.

It is important to mention that a fusion center was set up on the initiative of the United States in the North Atlantic alliance, mostly aiming to support NATO's out-of-area operations. NATO's Intelligence Fusion Center, located in the Royal Air Force Molesworth station near Huntingdon, UK, integrates DIOs from NATO nations for the production of full-spectrum, multi-domain operational and strategic intelligence. Its products are delivered to NATO's Allied Command Operations, NATO Special Operations Headquarters, NATO members and partners participating in specific NATO-led missions.[13]

The European Union followed the holistic concept of data/information fusion. It was determined by the need for an effective integration of varied and heterogenous streams of information and intelligence acquired from Member States' security and intelligence services, complemented with deliverables produced by different EU networks.

FUSING INTELLIGENCE IN THE EU

European intelligence cooperation, in both the military and security dimensions, has suffered from a deficit of reliable mechanisms for effective intelligence and information. This refers both to national authorities, as well as trans-governmental agencies and bodies. As a result, multiple local, national, regional and supranational counterparts, having access to varied sources of data and information, have often been hesitant to share their assets and provide their own intelligence products to relevant EU institutions and bodies. Due to such shortcomings and deficiencies, fusion centers were considered as a workable solution to the problem of barriers and obstacles in the cooperation between agencies working in a diversified, often decentralized, complex legal and institutional environment. However, domestic deficits in intelligence sharing were often deepened by bottlenecks and stove-piping in the realm of international security cooperation and intelligence exchange.

Such a view seemed to be particularly adequate to intelligence activities before and after the 2004 terrorist bombings in Madrid. Weaknesses and shortcomings of intelligence collaboration between national agencies were evident. There was a strong push in the post-Madrid period to launch new initiatives in the area of intelligence cooperation, involving national intelligence and security services, as well as EU institutions and bodies. Moreover, it was assumed that the latter should be particularly useful to build

[13] J.S. Gordon, "Intelligence Sharing in NATO", *Atlantisch Perspectief*, vol. 41, no. 6 (2017), pp. 16-17.

horizontal arrangements, which could prove to be effective in the fight against terrorism. In the wake of another spectacular terrorist act in Europe, that time in London in 2005, the search for an EU fusion center became the matter of handling and processing data and information acquired from open sources and pre-assessed data delivered by national intelligence services with the maximum efficiency.

Initially, the Joint Situation Center (SITCEN), established under the aegis of the High Representative for the Common Foreign and Security Policy in 2000, was taken into consideration as a prospective intelligence fusion center in the EU.[14] Gilles de Kerchove, the former EU Counter-Terrorism Coordinator, argued that *The SITCEN 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 summarised*.[15] He added, to strengthen the force of his argument, that fusion mechanisms triggered within SITCEN were sufficiently effective to warn policy makers about threats posed by incoming jihadists from the Middle East, the Arabian Peninsula or the Horn of Africa, or strengthen their awareness of the precursors used to construct explosives or make them aware of the use of the Internet for radicalization and recruitment to extremist jihadi groups.

However, the slow pace of intelligence cooperation development within the EU and significant limitations concerning SITCEN provided several EU Member States with a spur for an informal initiative on intelligence fusion. In November 2009, the Spanish Presidency of the Council of the European Union created the Committee of Counter-Terrorism Coordination Centers (CCCAT), known as the Madrid Group. This initiative was supported by fusion centers from a number of EU member states. Its aim was to cooperate with the EU Counter-Terrorism Coordinator and SITCEN (transformed in 2012 into INTCEN – EU Intelligence Analysis Center, now EU Intelligence and Situation Center).[16] The Madrid Group as a forum for the exchange and sharing of insights and experiences on threat assessments and counter-terrorism holds informal bi-annual meetings.[17] The meetings are financially supported by the European Commission.[18]

The Madrid Group has been one of several undertakings in the EU which aimed at reducing the deficit of EU actionable intelligence. Some limited forms of intelligence fusion were already present in information hubs established in EU agencies and in units

[14] Council of the EU, *Note from Presidency and the Delegations from the Netherlands and United Kingdom to Article 36. Subject: EU SitCen Work Programme*, doc. no. 5244/05 EXT 1, Brussels, 11 January 2005.

[15] G. de Kerchove, "Future Challenges in the Fight Against Terrorism", in Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe...*, p. XXI.

[16] Ch. Jones, "»Call It Intercontinental Collaboration«: Radicalisation, Violent Extremism and Fusion Centres", *Statewatch Analysis*, no. 255 (2014), p. 10.

[17] R. van der Veer, W. Bos, L. van der Heide, *Fusion Centres in Six European Countries...*, pp. 2-3.

[18] G. De Kerchove, C. Höhn, "The Role of European Intelligence in Countering Terrorism", in J.-H. Dietrich, S. Sule (eds), *Intelligence Law and Policies in Europe: A Handbook*, München–Baden-Baden–Oxford 2019, p. 113.

responsible for cooperation within the security dimension. INTCEN was responsible for threat assessment and the building of situational awareness for the EU's external missions and operations; the Intelligence Division of the EU Military Staff (EUMS) – for military intelligence required for CSDP operations; the Crisis Room – for crisis management and early warning; Europol and Eurojust – for criminal intelligence; and Frontex – for situation assessment and risk analysis on the EU's external borders. However, the effectiveness of information and intelligence processes and procedures was often not timely, sometimes disappointing with regard to quality. Even in some strategically important cases an accurate, timely and effective all-source analysis and intelligence products were barely sufficient and useful for decision makers.

Meanwhile, the migration crisis, terrorist attacks, expansion of certain categories of organized crime (especially the smuggling of people) as well as the emergence and rapid proliferation of new technology-driven threats and concerns (Dark Net, cryptocurrencies, sophisticated malware) built up a mounting pressure on the national authorities in Member States, as well as relevant EU agencies and bodies. Data fusion for the purposes of intelligence-driven knowledge production and situational awareness had been practised before the migration crisis and the surge in terrorist attacks in the years 2014-2015. Europol, as the core of the criminal intelligence hub in the EU, gradually developed the concept and methodology for identifying focal areas of criminal activity which were also a starting point for data collection. In addition, it worked out tailored methods and tools, such as indicators, relevant factors, horizon scanning, analysis and notification.

The growing relevance of the situation at the external borders for security of the EU made Frontex tasked with delivering tailor-made, non-standard, multi-function analyses and risk assessments focused on situational and pre-frontier intelligence estimates. For this purpose, in 2013 Frontex implemented the fusion services concept as a reaction to the growing diversity of sources, methods and tools of data/information gathering. In 2014, EUROSUR Fusion Services (EFS) were launched in order to provide situational awareness for Member States and other Frontex's stakeholders by granting access to multi-source information and analysis acquired from different sources.

EFS serve the European Border Surveillance System (EUROSUR) to fulfil its main tasks of ensuring situational awareness and reaction capability at the external borders of EU Member States by delivering surveillance and tracking data, with the aim of producing European situational picture and common pre-frontier intelligence pictures.[19] EFS included also a set of multi-domain functional services offered to EU by Member States and non-EU Schengen countries. Products are provided to recipients by fusing data and information provided by Frontex and relevant EU agencies, such as the EU Satellite Center, the European Maritime Safety Agency, European Fisheries Control Agency (EFCA), Europol, as well as commercial partners.[20]

[19] Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Draft Programming Document 2019-2021*, doc. no. 5247/18, Brussels, 30 January 2018.

[20] Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Report on the Functioning of Eurosur – Part I*, doc. no. 6215/18, Brussels, 15 February 2018, p. 10.

In the next, more advanced phase of their development, EFS encompassed new surveillance elements in order to facilitate management of diversified categories of data and provide real-time surveillance solutions to Frontex, other EU agencies and EU Member States.[21] Dedicated services are provided to Europol and some EEAS missions and operations, such as EUNAVFOR MED or EUBAM Libya.[22] The latter example could be used to illustrate the increasing importance of the accurate situational assessment in the Mediterranean Sea Basin, especially since the outbreak of the migration crisis in the mid-2010s, for the EU's operational activities.

The EUNAVFOR MED military operation (code-named Sophia), launched in 2015 in the central part of the Mediterranean Sea, was aimed at disrupting the business model of human smuggling and trafficking networks.[23] During the rollout of operational activities, a lot of data and information have been collected, stored and sent to relevant EU agencies and bodies for processing and analysis. In 2018, the Council took a decision to establish a crime information cell, located within the EUNAVFOR MED organizational structure, to ensure that any data and information gathered within the framework of *Operation Sophia*, relevant for crime prevention, investigation and prosecution as well as for security of the EU's external borders, is stored, processed and made available to authorities of Member States and Justice and Home Affairs (JHA) Agencies' Network. In addition, EEAS bodies, such as INTCEN and European Union Military Intelligence Directorate (EUMS INT) were involved in exchanging strategic analyses.[24] Crime Information Cell(s) (CIC) could be also used by EU civilian missions to help collect and share information acquired and gathered 'in the field'.[25] Subsequently, CIC was formed for the successor of EUNAVFOR MED Sophia – a maritime operation IRINI. The cell comprising staff from relevant law enforcement authorities of Member States and EU agencies facilitated the acquiring, collection and transmission of information on the arms embargo on Libya, the illegal exports of petroleum from Libya and on human smuggling and trafficking.[26]

The examples presented above illustrate efforts undertaken by EU institutions and bodies with the aim of maximizing exploitation of available data and information

[21] Ibid., pp. 10, 14.

[22] Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Report on the Functioning of Eurosur – Part II*, doc. no. 6215/18 ADD 1, Brussels, 15 February 2018, p. 5.

[23] "About EUNAVFOR MED Operation SOPHIA", at https://www.operationsophia.eu/about-us/#mission, 18 November 2022.

[24] Council of the EU, *Note from Presidency / EEAS Services / COMMISSION Services / GSC to Standing Committee on Operational Cooperation on Internal Security (COSI), Political and Security Committee (PSC). Subject: Cooperation between CSDP Missions/Operations and JHA Agencies*, doc. no. 14265/17, Brussels, 20 November 2017, p. 5.

[25] Council of the EU, *Cover Note from European External Action Service (EEAS) to Political and Security Committee (PSC). Subject: Priorities for Civilian Crisis Management*, doc. no. 13258/17, Brussels, 16 October 2017, p. 7.

[26] "EU Common Security And Defence Policy. Operation EUNAVFOR MED IRINI", May 2020, at https://www.operationirini.eu/wp-content/uploads/2020/05/factsheet_eunavfor_med_irini_070520.pdf, 12 February 2021.

acquired during operational activities for the strengthening of security of the EU and reduce vulnerability to risks and threats emerging in close proximity to the EU's external borders. They also illustrate the potential of a multi-source intelligence analysis and an urgent need for an institutional setup in the EU enabling an effective fusion of the data and information gathered. In the following section two EU institutional arrangements are presented and discussed in the context of fusion capabilities.

THE SINGLE INTELLIGENCE ANALYSIS CAPACITY

The EU Intelligence and Situation Center (INTCEN) was established within the EEAS for preparation and delivery of situation and risk assessments as well as special reports and briefings concerning the EU's Common Foreign and Security Policy (CFSP). Its activities have been focused on matters related to the CSDP, crisis-management missions, military and civilian operations, and immediate reactions to new threats, which needed to be tackled by both military and civilian instruments. From the early days of its activities, it has demonstrated a tendency to strengthen ties between military and civilian intelligence and, by adding open-source analysis, to work out a multi-source approach to the most critical aspects of EU security policies.

EU INTCEN has worked on open-source material and contributions from Member States' civilian security and intelligence organizations, as well as diplomatic reports delivered by EU delegations and missions around the world. It has received, on a regular basis, inputs from EU agencies (such as EU Satellite Center, European Maritime Security Agency, Europol) as well as – upon request – from Member States' civilian security and intelligence services. As a result, the quality and quantity of INTCEN outputs, especially intelligence-driven products, increased substantially although its hierarchy still fell short of needs and expectations of EU institutions and services.

The reason behind intelligence deficits has been known for a long time: it was the unwillingness of Member States to step up information exchange by including highly classified materials. Also, its access to military intelligence was unsatisfactory. This was the main cause of the launching in 2007 of the Single Intelligence Analysis Capacity (SIAC) format, aiming to pool civilian intelligence obtained by EU INTCEN and inputs provided by the Intelligence Division of the European Union Military Staff (EUMS), mainly on early warning and situation assessment. It opened new possibilities for cooperation of both entities and producing joint intelligence assessments, based on integration of data, information and exploiting properly human resources available within the EU. The main objective was reinforcement of policy development, early warning, situational awareness and crisis response with a view to plan and conduct CSDP missions, operations and exercises.[27] According to top representatives of EU INTCEN and EUMS INT, *SIAC delivers a unique joint service, combining intelligence*

[27] J. Kozłowski, J.M. Palacios-Coronel, "Single Intelligence Analysis Capacity (SIAC) – A Part of the EU Comprehensive Approach", *Impetus. Magazine of the EU Military Staff*, no. 17 (2014), pp. 10-11.

from all participating Member States' military and civilian intelligence and security services within the SIAC framework.[28]

Although under SIAC arrangement a fully-fledged information fusion capability has not been developed, its input to strategic and operational situational awareness and decision-making processes was considerable and promising. In the quest for an increased level of situational awareness, the Council in late 2016 recommended the use of SIAC as a requirement for an *enhanced civil/military intelligence and strategic foresight*, which should be made possible through the use of SIAC as *the main European hub for strategic information, early warning and comprehensive analysis*.[29] The Council, in its conclusions on security and defence, adopted in May 2017, supported *the gradual approach chosen to enhance the capabilities of the Single Intelligence Analysis Capacity (SIAC) of the EU and the short term needs already defined for additional staffing. It will revert to the issue again in view of further progress achieved and plans elaborated for the longer term development on SIAC*.[30]

Due to problems, barriers and challenges of data fusion practices within the EEAS, SIAC offered a remedy to deficits and limitations of intelligence cooperation under CSDP. It sought to enhance efficiency of information gathering and intelligence sharing within the EU by increasing value and utility of intelligence outputs built on civil and military deliverables from Member States intelligence organizations. In emergencies or obvious signs of a crisis or a conflict posing a real challenge to the EU, SIAC was able to deliver dedicated and joint intelligence products based on the all-source analysis of available data and information obtained from relevant EU bodies and external counterparts. However, SIAC does not ensure a fully integrated intelligence analysis process due to the problems with receiving necessary data, information and intelligence from Member States.

The SIAC model was recognized by the Council as an effective tool for the production of comprehensive analytical assessments and a significant contribution to strategic awareness. The inclusion of SIAC into the preparing of Strategic Compass, an action plan for strengthening the EU's defence and security policy by 2030, was a valuable experience in testing intelligence analysis capabilities and activating national intelligence military and civilian organizations to deliver their inputs in spite of the existing reservations. The first-ever comprehensive 360-degree EU threat analysis conducted by the SIAC was presented to Member States in November 2020. The Council recognized that *this first, valuable experience and its lessons learned should lead to a more regular and comprehensive process of intelligence analyses of threats and challenges to the EU, based on Member States' voluntary inputs*.[31]

---

[28] J. Morgado, R. Jeżewski, "The Single Intelligence Analysis Capacity (SIAC)", in J. Rehrl (ed.), *Handbook on CSDP: The Common Security and Defence Policy of the European Union*, Vienna 2021, p. 76.

[29] Council of the EU, *Implementation Plan on Security and Defence*, doc. no. 14392/16, Brussels, 14 November 2016, pp. 11, 26.

[30] Council of the EU, *Council Conclusions on Security and Defence in the Context of the EU Global Strategy*, doc. no. 9178/17, Brussels, 18 May 2017.

[31] Council of the EU, *Council Conclusions on Security and Defence*, doc. no. 8396/21, Brussels, 10 May 2021, p. 3.

EU HYBRID FUSION CELL: AN ATTEMPT AT ALL-SOURCE SITUATIONAL ASSESSMENT

Following turbulent developments in the Middle East (especially war in Syria) and Ukraine (annexation of Crimea, Russia-sponsored rebellion in eastern provinces), the European Union as well as NATO were afraid of potential threats resulting from a new form of conflict, denominated hybrid war, proliferating in eastern and southern neighbourhood of the Euro-Atlantic area. EU Member States decided to counter hybrid threats and foster the resilience of the EU and its Members by mobilizing appropriate instruments, resources and methods, including information exchange and relevant intelligence-sharing. In a Joint Communication on countering hybrid threats in the European Union, in April 2016, the High Representative of the Union for Foreign Affairs and Security Policy put forward a proposal of establishing an EU Hybrid Fusion Cell within the existing EU INTCEN structure, *capable of receiving and analysing classified and open source information on hybrid threats*.[32]

A Fusion Cell was expected to acquire, analyse and share classified and open-source information on hybrid threats. The institutional sources will include the EEAS, the Commission, EU agencies and relevant services of Member States. It was assumed that EU staff (including officials deployed to EU delegations, operations and missions) and liaison representatives in Member States, operating as national Points of Contact (PoC), should undergo specialist training to identify hybrid threats and assess its potential negative impact, as well as ensure cooperation and secure communication.[33]

The EU Hybrid Fusion Cell (HFC) was established in early 2017 within EU INTCEN, reaching full operating capacity in May 2017. INTCEN's communication system enabled transmission of classified and open-source information. Analysis carried out within HFC resulted in assessments and briefings as well as a periodical *Hybrid Bulletin*, first released in January 2017. It offered intelligence-driven insights about hybrid threats and related issues, except terrorism, which was the responsibility of the Directorate for Conflict Prevention and Security Policy of EEAS.[34]

Gerhard Conrad, the then director of the EU Intelligence and Situation Center, said that HFC is established to *analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, in order to rapidly contextualize incidents and trends and to inform the EU's strategic decision-making processes, including by providing inputs to the*

[32] European Commission, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union Response*, doc. no. JOIN(2016) 18 final, Brussels, 6 April 2016, p. 4.

[33] Ibid., p. 5.

[34] European Commission, *Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats – a European Union Response*, doc. no. JOIN(2017) 30 final, Brussels, 19 July 2017; E. Hoorickx, "Countering 'Hybrid Threats': Belgium and the Euro-Atlantic Strategy", *Security & Strategy*, no. 131 (2017), p. 29.

security risk assessments carried out at EU level.[35] Hence, support for strategic and, to some extent, political decision making in relation to long-term and rapidly emerging hybrid threats and non-conventional activities has become the main task of the Cell.

In this regard, it is worth underlining the position of HFC in a wider, Euro--Atlantic context of security and defence. NATO as an institutional actor in the European security arena was actively developing its analytical capabilities regarding hybrid risks and threats. At the summit in Warsaw in 2016, NATO and the EU adopted the Joint Declaration which contained the commitment to boost ability to counter hybrid threats by *working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between states; and cooperating on strategic communication and response*.[36] At that time NATO did not have a unit specialized in analysis and exchange of data and information on hybrid threats. It relied mostly on centers of excellence dealing with some matters linked to hybrid warfare, such as CBRN defence, energy security, cyber defence and strategic communication.

A European Center of Excellence for countering hybrid threats (Hybrid CoE) was established in Helsinki as a follow-up to NATO's Warsaw summit, and a direct reference to a recommendation specified in the European Commission's Joint Communication on countering hybrid threats of April 2016.[37] The Hybrid CoE was inaugurated in April 2017 as an autonomous network-based international organization open to all EU and NATO countries. Its mission was to promote a comprehensive approach to preventing and countering hybrid threats. Parallelly, the Hybrid Analysis Branch was set up within NATO's Joint Intelligence and Security Division (JISD), with the aim of analyzing the full spectrum of hybrid activities on the basis of information and intelligence drawn from military and civilian sources.[38] It was also intended to facilitate the exchange of information on hybrid threats between the Alliance and the EU through the improvement of mutual situational awareness, alignment of their responses to hybrid threats, as well as mutual briefings on the hybrid threat picture.[39] The staff-to-staff sharing of information between the EU Hybrid Fusion Cell and the NATO Hybrid

[35] European Union Military Committee, "Common Security and Defence Policy: Intelligence and Situation Center (INTCEN)", *Chairman's Newsletter*, no. 29 (2016), p. 3.

[36] NATO, "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization", *Press Release*, no. 119 (2016), 8 July 2016.

[37] A. Jacuch, "Countering Hybrid Threats: Resilience in the EU and NATO's Strategies", *The Copernicus Journal of Political Studies*, no. 1 (2020), p. 19.

[38] A. Freytag von Loringhoven, "Adapting NATO Intelligence in Support of »One NATO«", 8 September 2017, at https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html, 22 September 2017.

[39] E. Hoorickx, "Countering 'Hybrid Threats'...", p. 30; M. Rühle, C. Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats", *NATO Review*, 19 March 2021, at https://www.nato.int/docu/review/articles/2021/ 03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html, 21 May 2021.

Analysis Branch was activated, and the Hybrid CoE engaged in the exchange of available open-source information.[40]

The effects of the first years of HFC's activities were limited by the lack of sufficient budgetary means and scarce personnel resources. It did not cover the full range of hybrid threats. Therefore, the efforts were focused on selected topics, such as Russian hybrid tools: cyber technology, disinformation and propaganda. It made use of a network of PoCs in Member States and EU institutions (mostly the European Commission) and was receiving intelligence related to hybrid threats on a voluntary basis.[41] Over time, the Hybrid Fusion Cell earned recognition as a focal point for hybrid threat assessments. It extended cooperative links to relevant EU agencies and bodies and was involved in the production of analytical reports on civil and military aspects of hybrid threats – within the framework of SIAC.[42]

In December 2019, the EU Council adopted conclusions on complementary efforts to counter hybrid threats. Ministers stressed the need to strengthen the role of the Hybrid Fusion Cell in the further development of the existing situational awareness abilities possessed by the EU and its Member States. They emphasized that the work of HFC should be further enhanced, taking into account an appropriate level of resources and a better use of the intelligence analysis of hybrid threats.[43]

As part of the EU's efforts towards an enhanced situational awareness and resilience building, the Hybrid Fusion Cell was consolidated as the EU focal point for hybrid threat assessments.[44] It regularly produces written reports on hybrid threats and delivers hybrid trends analyses and present oral briefings to EU decision-makers and Member States' representatives. In 2021, it conducted a first identification round of sectoral baselines, an important step to monitor progress in protecting Member States and EU institutions against hybrid threats.[45] The Strategic Compass, adopted in March 2022, calls for the creation of an EU Hybrid Toolbox to respond to a broad range of hybrid threats. The Hybrid Fusion Cell also provides foresights and situational awareness contributing to a broader Hybrid Toolbox by addressing foreign information manipulation and interference.[46]

---

40 D. Zandee, S. van der Meer, A. Stoetman, *Countering Hybrid Threats Steps for Improving EU–NATO Cooperation*, The Hague 2021, p. 9.

41 E. Hoorickx, "Countering 'Hybrid Threats'...", p. 29.

42 G. Conrad, "Situational Awareness for EU Decision-Making: The Next Decade", *European Foreign Affairs Review*, vol. 26, no. 1 (2021), p. 61.

43 Council of the EU, *Complementary Efforts to Enhance Resilience and Counter Hybrid Threats – Council Conclusions (10 December 2019)*, doc. no. 14972/19, Brussels, 10 December 2019, p. 6.

44 European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy*, doc. no. COM(2020) 605 final, Brussels, 24 July 2020, p. 15.

45 European Commission, *Communication from the Commission to the European Parliament and the Council on the Third Progress Report on the Implementation of the EU Security Union Strategy*, doc. no. COM(2021) 799 final, Brussels, 8 December 2021, p. 8.

46 European External Action Service, *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*,

The Russian military invasion of Ukraine in 2022 showed a full spectrum of belligerent actions combining armed aggression in blatant violation of legal or humanitarian norms with hybrid operations encompassing cyberattacks, foreign interference, full-scale disinformation, energy coercion and even a militant nuclear rhetoric. The EU responded with a series of sanctions against Russia and the financing of military assistance to Ukraine. It also activated crisis response mechanisms and intensified work on intelligence-driven assessments and forecasts of the situation in Ukraine.

The Hybrid Fusion Cell was tasked to continue to provide comprehensive assessments of hybrid threats affecting the EU and its Member States. The General Affairs Council in its conclusions on a coordinated EU response to hybrid campaigns stressed that: *the SIAC, in particular the Hybrid Fusion Cell, will play a central role contributing to the decision-making process by providing strategic foresight and comprehensive situational awareness, notably to identify the origin and features of the hybrid campaign, provided they have the appropriate resources*.[47]

The latter denotes a critical aspect of HFC's fusion capabilities: dependence on inputs from Member States contributions, especially their intelligence services, as well as on the coordinated flow of information and analytical products within the EU. Diversity of attitudes toward hybrid activities revealed by the governments of EU Member States determines quantity and quality of information and intelligence provided to relevant EU bodies, especially to INTCEN and its Hybrid Fusion Cell. This makes all-source assessments incomplete and dependent on fragmentary knowledge.

CONCLUSIONS

The intelligence fusion concept, based on all-source data and information processed by a single institutional entity, has not raised major controversies thus far. However, the organization of fusion centers, costs they incur and quality of analyses provided by them have been subject to criticism, mostly in the United States.[48] From the perspective of international cooperation, including the advanced inter-governmental collaboration

Brussels 2022, p. 34 at https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf, 10 September 2022.

47 Council of the EU, "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns", 21 June 2022, at https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/, 24 June 2022.

48 K. Hibbs Pherson, R.A. Sullivan Jr., "Improving the Quality of Analysis in Fusion Centers: Making the Most of the Nation's Investment", *Journal of Strategic Security*, vol. 6, no. 3 Suppl. (2013); A. de Castro Garcia, F.C. Matei, T.C. Bruneau, "Combatting Terrorism Through Fusion Centers: Useful Lessons From Other Experiences?", *International Journal of Intelligence and CounterIntelligence*, vol. 30, no. 4 (2017); P.M. Regan, T. Monahan, "Fusion Center Accountability and Intergovernmental Information Sharing", *Publius. The Journal of Federalism*, vol. 44, no. 3 (2014); B. McQuade, *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*, Oakland, CA 2019.

and supranational coordination in the European Union, advantages of data fusion and all-source analysis are widely acknowledged.

Nevertheless, the method and organizational framework seem to be secondary to the substance of intelligence fusion concept, which is access to accurate, reliable, timely and valuable information. In the case of the European Union, this variable depends on numerous factors: legal bases, political will, information safeguards, threat assessments and perceptions, and – last but not least – on mutual trust.

Security and defense of the European Union relies on collaborative networks and national commitments of individual Member States, as well as binding collective arrangements extended to non-EU partners. The scope and pace of information exchange and intelligence sharing are determined by vital national security interests and can be performed only if no formal or practical obstacles exist. This should be complemented by promoting international cooperation without prejudice to the domestic norms and international obligations of each participating state. This means that formal rules and norms, as well as working arrangements, on the EU level with regard to data and information fusion and intelligence sharing are secondary to the principle of national security of each Member State.

This is formally enshrined in Article 4.2. of the Treaty on European Union (TEU)[49] and considered as a cornerstone of intelligence cooperation in the EU. The Council decisively argued that *the work of Member States' intelligence agencies for national security matters remains the sole responsibility of Member States*.[50] Irrespective of controversies surrounding the interpretation and implementation of relevant provisions of EU law,[51] national and supranational stakeholders of EU intelligence cooperation have recurrently invoked this national security clause to justify unwillingness or incapability to deliver relevant information or share intelligence products.

The EU's reaction to recent developments in Europe, especially the post-2015 strategy of managing the risks and threats generated by jihadi terrorism and the migration crisis, and the response to Russia's military invasion of Ukraine in 2022, have given evidences of the widening gap between political consensus and institutional framework at the EU level and information and intelligence delivery by individual Member States. Credibility of EU institutions, and effectiveness of their decisions and actions, depend to a considerable degree on a comprehensive and reliable strategic awareness and on an accurate real-time situational assessment, especially concerning security-related processes and developments.

The use of intelligence for tactical and operational purposes is also limited in the EU. It is national security and intelligence services, which are responsible for intelligence

[49] The Union *shall respect essential State functions* [of its Member States]*, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State*.

[50] European Parliament, *Reply (17 June 2013) to the question for written answer E-001671/13 to the Council Ins Cristina Zuber (GUE/NGL) and João Ferreira (GUE/NGL) (18 February 2013)*, Official Journal of the European Union 2013, no. C 371 E.

[51] Seen an excellent analytical paper by Satish Sule, "National Security and EU law restraints on Intelligence Activities", in J.-H. Dietrich, S. Sule (eds), *Intelligence Law and Policies in Europe*...

sharing and this has an impact on EU intelligence, on the EU's own resources (acquired by relevant agencies and bodies) and EU open-source intelligence.[52] The 'need-to--know' principle is a key for the EU's security-related intelligence initiatives. Data and information fusion and all-source analysis concepts are promising as reliable methods only when they are practised in joint fusion establishments, enjoying a continuous flow of data, information and finished intelligence to the extent made possible by stakeholders, i.e. intelligence institutions from Member States.

Peter Gill wrote a decade ago: *Fusion centres represent an important innovation in the effort to improve information sharing and coordination within increasingly diverse intelligence networks that operate at various 'levels' and across the public and private sector*.[53] This point is true with respect to national intelligence systems, while any transnational setting generates new challenges and additional issues that must be handled in a sensitive and efficient manner. The EU still has not presented effective solutions for this complex process of decision making to support its security and defense policies. The network architecture of CSDP is a solid basis for the cross-level intelligence cooperation but joint institutional undertakings, such as the Hybrid Fusion Cell or Single Intelligence Analysis Capacity, need a continued and consistent support of Member States as part of their commitment to the strengthening of the EU 'that really protects'.[54]

BIBLIOGRAPHY

"About EUNAVFOR MED Operation SOPHIA", at https://www.operationsophia.eu/about-us/#mission.

Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Antwerp 2010.

Blasch E., "Information Fusion for Decision Making – Designing Realizable Information Fusion Systems", in E. Shahbazian, G. Rogova, P. Valin (eds), *Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, Amsterdam 2005.

Brun O., "UCLAT", in H. ***Moutouh***, J. Poirot (eds), *Dictionnaire du renseignement*, Paris 2018, https://doi.org/10.3917/perri.mouto.2018.01.0799.

Buede D., Waltz E., "Data Fusion", in *McGraw Hill Encyclopedia of Science and Technology*, New York 1998.

Castro Garcia A. de, Matei F.C., Bruneau T.C., "Combatting Terrorism through Fusion Centers: Useful Lessons from Other Experiences?", *International Journal of Intelligence and CounterIntelligence*, vol. 30, no. 4 (2017), pp. 723-742, http://dx.doi.org/10.1080/08850607.2017.1297119.

[52] See A. Gruszczak, *Intelligence Security in the European Union: Building a Strategic Intelligence Community*, Basingstoke 2016.

[53] P. Gill, "Integrated Terrorist Threat Assessment in Europe: An Overview", in Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe...*, p. 219.

[54] 'A Europe that protects' is a slogan associated with the project of Security Union launched in 2016 by Jean-Claude Juncker, the then President of the European Commission.

Connable B., *Military Intelligence Fusion for Complex Operations: A New Paradigm*, Santa Monica, CA 2012.

Conrad G., "Situational Awareness for EU Decision-Making: The Next Decade", *European Foreign Affairs Review*, vol. 26, no. 1 (2021), pp. 55-70, https://doi.org/10.54648/eerr2021006.

Council of the EU, *Complementary Efforts to Enhance Resilience and Counter Hybrid Threats – Council Conclusions (10 December 2019)*, doc. no. 14972/19, Brussels, 10 December 2019.

Council of the EU, "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns", 21 June 2022, at https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/.

Council of the EU, *Council Conclusions on Security and Defence*, doc. no. 8396/21, Brussels, 10 May 2021.

Council of the EU, *Council Conclusions on Security and Defence in the Context of the EU Global Strategy*, doc. no. 9178/17, Brussels, 18 May 2017.

Council of the EU, *Cover Note from European External Action Service (EEAS) to Political and Security Committee (PSC). Subject: Priorities for Civilian Crisis Management*, doc. no. 13258/17, Brussels, 16 October 2017.

Council of the EU, *Implementation Plan on Security and Defence*, doc. no. 14392/16, Brussels, 14 November 2016.

Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Draft Programming Document 2019-2021*, doc. no. 5247/18, Brussels, 30 January 2018.

Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Report on the Functioning of Eurosur – Part I*, doc. no. 6215/18, Brussels, 15 February 2018.

Council of the EU, *Note from General Secretariat of the Council to Delegations. Subject: Frontex Report on the Functioning of Eurosur – Part II*, doc. no. 6215/18 ADD 1, Brussels, 15 February 2018.

Council of the EU, *Note from Presidency and the Delegations from the Netherlands and United Kingdom to Article 36. Subject: EU SitCen Work Programme*, doc. no. 5244/05 EXT 1, Brussels, 11 January 2005.

Council of the EU, *Note from Presidency / EEAS Services / COMMISSION Services / GSC to Standing Committee on Operational Cooperation on Internal Security (COSI), Political and Security Committee (PSC). Subject: Cooperation between CSDP Missions/Operations and JHA Agencies*, doc. no. 14265/17, Brussels, 20 November 2017.

European Commission, *Communication from the Commission to the European Parliament and the Council on the Third Progress Report on the Implementation of the EU Security Union Strategy*, doc. no. COM(2021) 799 final, Brussels, 8 December 2021.

European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy*, doc. no. COM(2020) 605 final, Brussels, 24 July 2020.

European Commission, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union Response*, doc. no. JOIN(2016) 18 final, Brussels, 6 April 2016.

European Commission, *Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats – a European Union Response*, doc. no. JOIN(2017) 30 final, Brussels, 19 July 2017.

European External Action Service, *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*, Brussels 2022, at https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

European Parliament, *Reply (17 June 2013) to the Question for Written Answer E-001671/13 to the Council Ins Cristina Zuber (GUE/NGL) and João Ferreira (GUE/NGL) (18 February 2013)*, Official Journal of the European Union 2013, no. C 371 E.

European Union Military Committee, "Common Security and Defence Policy: Intelligence and Situation Center (INTCEN)", *Chairman's Newsletter*, no. 29 (2016).

"EU Common Security And Defence Policy. Operation EUNAVFOR MED IRINI", May 2020, at https://www.operationirini.eu/wp-content/uploads/2020/05/factsheet_eunavfor_med_irini_070520.pdf.

Farivar C., "20 Years after 9/11, 'Fusion Centers' Have Done Little to Combat Terrorism", *NBC News*, 11 September 2021, at https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949.

Freytag von Loringhoven A., "Adapting NATO Intelligence in Support of »One NATO«", 8 September 2017, https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html.

Gill P., "Integrated Terrorist Threat Assessment in Europe: An Overview", in Belgian Standing Intelligence Agencies Review Committee, *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Antwerp 2010.

Gordon J.S., "Intelligence Sharing in NATO", *Atlantisch Perspectief*, vol. 41, no. 6 (2017), pp. 15-19.

Graphia Joyal R., *State Fusion Centers: Their Effectiveness in Information Sharing and Intelligence Analysis*, El Paso 2012.

Gruszczak A., "Establishing an EU Law Enforcement Fusion Centre", *European Journal of Policing Studies*, vol. 4, no. 1 (2016), pp. 103-124, https://doi.org/10.5553/EJPS/2034760X2016004001007.

Gruszczak A., *Intelligence Security in the European Union: Building a Strategic Intelligence Community*, Basingstoke 2016, https://doi.org/10.1057/978-1-137-45512-3.

Hibbs Pherson K., Sullivan R.A. Jr., "Improving the Quality of Analysis in Fusion Centers: Making the Most of the Nation's Investment", *Journal of Strategic Security*, vol. 6, no. 3 Suppl. (2013), pp. 309-319, http://dx.doi.org/10.5038/1944-0472.6.3S.29.

Hoorickx E., "Countering 'Hybrid Threats': Belgium and the Euro-Atlantic Strategy", *Security & Strategy*, no. 131 (2017).

Jacuch A., "Countering Hybrid Threats: Resilience in the EU and NATO's Strategies", *The Copernicus Journal of Political Studies*, no. 1 (2020), pp. 5-26, https://doi.org/10.12775/CJPS.2020.001.

Jones Ch., "»Call It Intercontinental Collaboration«: Radicalisation, Violent Extremism and Fusion Centres", *Statewatch Analysis*, no. 255 (2014), pp. 1-15.

Kerchove G. de, "Future Challenges in the Fight Against Terrorism", in Belgian Standing Intelligence Agencies Review Committee (ed.), *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Antwerp 2010.

Kerchove G. de, Höhn Ch., "The Role of European Intelligence in Countering Terrorism", in J.-H. Dietrich, S. Sule (eds), *Intelligence Law and Policies in Europe: A Handbook*, München–Baden-Baden–Oxford 2019, https://doi.org/10.5040/9781509926169.ch-004.

Kozłowski J., Palacios-Coronel J.M., "Single Intelligence Analysis Capacity (SIAC) – A Part of the EU Comprehensive Approach", *Impetus. Magazine of the EU Military Staff*, no. 17 (2014), pp. 10-11.

McQuade B., *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*, Oakland, CA 2019, https://doi.org/10.1525/9780520971349.

Morgado J., Jeżewski R., "The Single Intelligence Analysis Capacity (SIAC)" in J. Rehrl (ed.), *Handbook on CSDP: The Common Security and Defence Policy of the European Union*, Vienna 2021.

NATO, "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization", *Press Release*, no. 119 (2016), 8 July 2016.

Persson G., *Fusion Centres – Lessons Learned: A Study of Coordination Functions for Intelligence and Security Services*, Stockholm 2013.

Regan P.M., Monahan T., "Fusion Center Accountability and Intergovernmental Information Sharing", *Publius. The Journal of Federalism*, vol. 44, no. 3 (2014), pp. 475-498, https://doi.org/10.1093/publius/pju016.

Rühle M., Roberts C., "Enlarging NATO's Toolbox to Counter Hybrid Threats", *NATO Review* 19 March 2021, at https://www.nato.int/docu/review/articles/2021/03/19/ enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

Sule S., "National Security and EU Law Restraints on Intelligence Activities", in J.-H. Dietrich, S. Sule (eds), *Intelligence Law and Policies in Europe. A Handbook*, München–Baden-Baden–Oxford 2019.

Veer R. van der, Bos W., Heide L. van der, *Fusion Centres in Six European Countries: Emergence, Roles and Challenges*, The Hague 2019.

Zandee D., Meer S. van der, Stoetman A., *Countering Hybrid Threats: Steps for Improving EU–NATO Cooperation*, The Hague 2021.

Artur GRUSZCZAK is a Professor of Social Sciences, Chair of National Security at the Faculty of International and Political Studies, Jagiellonian University in Kraków, Poland. He is an expert of the Centre International de Formation Européenne in Nice. He has provided expertise in security and intelligence matters for the Polish Ministry for Foreign Affairs, the Polish Parliament, the Polish Ombudsman, the European Parliament and independent analytical institutions such as Statewatch, Oxford Analytica and GLOBSEC. He is the author of *Intelligence Security in the European Union. Building a Strategic Intelligence Community* (Palgrave Macmillan, 2016). He is the co-editor of the *Routledge Handbook of the Future of Warfare* (Routledge, forthcoming 2023). His current research interests include European intelligence cooperation, democratic security and security protocolarization.