Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Regular Article

Information exchange of law enforcement agencies within the EU in context of COVID-19 outbreak

Gábor Kemény a, Michal Vít b, *

a Fellow at Police Law Enforcement School, Budapest, Hungary
b Metropolitan University Prague, Czech Republic

1. Introduction

The current outbreak of the coronavirus disease (COVID-19) has had a serious impact on public health, security, and economy (EEAS, 2020) across the globe. Moreover, the pandemic poses an enormous threat to the internal security of the EU and its member states, as crime, such as terrorism, cross-border criminality, the trafficking of human beings, the smuggling of people and goods (medicines, weapons) etc. is a 'seriously disrupting factor and a diversion from national and EU efforts to ensure the health and safety of citizens' (Europol, 2020a, p. 2). Cross-border law-enforcement cooperation is an important tool in the fight against these threats as it contributes to the detection of criminal activities (Frontex, 2018a, 2018b, p. 6), supports police in sharing information about the movement of persons from highly infected regions and helps national and international authorities to monitor the spread of the disease. For this reason, it is understandable why the EU and its agencies, such as Europol (Europol, 2020b, p. 13) and Frontex (Europol, 2020b, p. 13) urges national authorities to share real time information with each other and with the EU. At the same time, national law enforcement authorities have to deal with new nature security related to public security. Said that, the authorities tackle situations that are in very similar nature when it comes to individual EU and non-EU countries such as demonstrations against COVID-19 measures, reinforcement of border controls within Schengen area. However, as terrorists’ attacks from Vienna in November 2020 showed, the need of real-time information exchange of law enforcement agencies has not decreased by any mean. Contrary the opposite, the networks of organized crime accommodate in new realities (UNODC and Coronavirus (COVID-19), 2021).

In this context, the current outbreak of COVID-19 creates new opportunities for organized criminal groups to utilize this window of opportunity for smuggling various goods using new means of communication and transportation. In this, it has to be noted that law enforcement agencies are extensively involved in crisis management aiming to decrease further spreading of virus infection. This logically decreases the institutional capacity to tackle the complexity of organized crime of a transnational nature, such as the smuggling of human beings, narcotics etc. As a result, the coronavirus outbreak has significantly strengthened understanding sovereignty of the state as a provider of security to its citizens. However, nationally framed responses implemented across the world have difficulty confronting globalized security threats related to organized crime (European Commission, 2020a, 2020b). At the same time, according information provided by experts dealing with organized crime, the networks have significantly professionalized their activities, such as using cutting edge technologies and special mobile applications hand in hand with even better shady cooperation with law enforcement agencies as speaking about Western Balkan countries. This combines usage of rather traditional means of organize crime when it comes of processing activities via tribes in rural areas.
areas and modern IT technologies when smuggling all kind of goods (Riehle, 2020).

Despite the preoccupation of national law enforcement agencies with COVID-19 related measures, incidents related to smuggling and trafficking occurring, for example, on EU external borders, demonstrate an imminent need to strengthen cross-border cooperation and effective information exchange. This creates even higher pressure on smooth collaboration of law enforcement agencies. As the case of terrorist’s attack in Vienna shows, the trust based and effective collaboration is the most important tool to tackle complex nature of transnational security threats. However, the cooperation under umbrella of the EU, shows limits of developing institutionalized trust and smooth cooperation. The incidents in February/March 2020 involving migrants aiming to enter EU territory at the Greek-Turkish border have illustrated the complexity of border protection in a politically sensitive part of Europe. It has showed that Frontex, and in wider terms the EU, is not able to harmonize institutional trust-based culture when it comes for less formal cooperation of national law enforcement agencies. In this case, Danish border police refused to participate on push backs of migrants’ vessels as ordered by Greek border police (Politico and Danish boat in Aegean 2020). At the same time, in light of progressed COVID-19 pandemic, the capacity of Frontex being the right tool for effective information exchange as the internal capacity of Frontex has been publicly questioned in early 2021 (Nielsen, 2021). Such a development demonstrates rather the politicization of border protection – and cooperation of law enforcement agencies – rather than the development of institutionalized cross-border cooperation. The COVID-19 crisis puts the cooperation of law enforcement agencies into a new perspective.

The authors of this paper firstly argue that the national law-enforcement agencies are prepared to provide an adequate response to the institutionalized demands of law enforcement cooperation. Secondly, states are seriously hindering the required timely cross-border information exchange even in context of current organisational, legal and technological proximity, which has developed over the long term.

This paper stems from context of institutionalized cooperation of law enforcement in the EU. Given the clashing nature of EU and EU member states cooperation in the field of law enforcement, this paper emphasizes established channels of cooperation diminishing a strictly nationally bounded approach to law enforcement. However, given how differentiated both horizontal and vertical cooperation is in the field of security cooperation, the response to the EU, EU member states, but also EU candidate countries creates a blurry cooperation framework.

2. The relevance of police cooperation and information exchange

An increasing terrorist threat and the need to combat terrorism led to the establishment of the first intergovernmental forum, the so called TREV group in 1975. Although this intergovernmental initiative could still be considered a political forum, police experts, high ranking officers and officials of security services could also participate in the meetings beside national ministers and could influence the results of the forums.

International police cooperation in Europe became vital in 1984, when France and Germany agreed to gradually eliminate border controls on their common border and transfer it to the external borders. One year later the Benelux countries expressed their willingness to join this initiative. The strengthening of police and customs cooperation was one of several proposed measures. The so-called Schengen Convention was signed five years later in 1990. The convention provides for an action plan for the establishment and implementation of a free movement regime by abolishing internal border checks at the common border. In order to safeguard internal security and to ensure the elimination of the security deficit caused by the abolition of checks at internal borders, police cooperation became a complementary measure (Sardjoe, 2017, p. 26). The convention lists the modes of cooperation, with Article 39 encouraging the police authorities of the Member States (MS) to assist each other in preventing and detecting criminal offences. Cross-border police cooperation has become increasingly important in the last two decades with the enlargement of the EU and the Schengen area, and also because of the different security threats that arise and which show a cross-border character. One of the crucial and indispensable elements of this international police cooperation is cross-border information exchange. Without this, proper decision making cannot be ensured (Sardjoe, 2017, p. 26), therefore security cannot be achieved and maintained.

The utmost importance of information exchange and increased operational cooperation to ensure that ‘the internal and external dimensions of security work in tandem’ (European Commission and COM, 2004, p. 9) has pervaded the whole text of The European Agenda on Security. International cooperation also helps to address the root causes of migration, to ensure coordinated actions, to increase the effectiveness of saving lives and securing maritime borders and to crack down on criminal groups as described in the European Agenda on Migration. The role of police cooperation and information exchange to increase stability and to decrease security risks, such as hybrid threats, cyber security and terrorism was also highlighted in the roadmap of the Netherlands Presidency of the Council of the European Union in 2016 (Sardjoe, 2017, p. 26).

Various systems, bodies and agencies have been established and tasked within the EU to achieve the above written goals and aims. The Schengen Information System (SIS) (European Commission and COM, 2015) is intended to support border control, police cooperation and law enforcement information exchange with its unique alert system. Cooperation in police training and the exchange of best practises are the main tasks of the European Police Colleague (CEPOL) (Council of the European Union, 1070). The European Police Office (Europol) is responsible for facilitating information exchange among the law enforcement agencies of the MSs (Council of the EU, 2007). The European Union’s Judicial Cooperation Unit (Eurojust) was established to support judicial cooperation between national authorities in the fight against terrorism and serious organised crime. Furthermore, one of the main tasks of the European Border and Coast Guard Agency (Frontex) is to develop and implement the EU Integrated Border Management (IBM) concept, where one of the components is the inter-agency cooperation and information exchange.

3. Channels of information exchange

In reality, different units and services are dealing with different parts of law enforcement cooperation and information exchange in the countries and there are significant differences between the MSs regarding the responsibilities of the services. This complex legal and operational landscape formulates the need to establish a network of databases and creating a ‘one window’ system by putting one police unit in charge of international police cooperation in each country. This has resulted in the creation of the Single Point of Contact (SPOC). SPOCs are ‘responsible for managing the information flow exchange between the different units and designated contact points both at national and international level’ (European Council, 2018). SPOCs can be found on the central national level, mostly under the umbrella of the International

---

1 In this context, the EU Commissioner Kyriakides expressed himself as follows: “Firstly, and I cannot stress this enough: ensuring real time exchange of information and coordination of measures between us and ensuring that everyone is prepared to contain the spread of the virus are crucial elements for an effective and coherent response. This is precisely why we have our well-established channels of information exchange in place at EU level and why we provide scientific and evidence-based guidance to help Member States prepare their health systems and health care workers. Our scientific experts who are here with us today will elaborate further on this” (European Commission, 2020a, 2020b).

---
Law Enforcement Coordination Unit (ILECU). SPOCs are usually divided into several functional sub-units, which are responsible for conducting different types of cross-border activities, such as information exchange with other countries, and with Interpol (using the Interpol National Central Bureau-INCB), Europol (European Union Agency for Law Enforcement Cooperation, 2020) (through the Europol National Unit-ENU) and Sirene (European Commission and COM, 2004, p. 9) (by National Sirene Bureau) as we learned from the so called EXIM communication of the European Council (European Commission and COM, 2004, p. 9). This simple and uniform approach at the national level aims to ensure that all information exchange requests are dealt with efficiently (European Union Agency for Law Enforcement Cooperation, 2020). SPOCs mostly operate 24/7, although this still does not mean a SPOC can immediately answer requests, especially if a SPOC depends on other units which are not working round the clock. Research shows that the SPOC seems to be one of the most efficient tools for cross-border information exchange (Tsai, 2002), and that communication is easier and more efficient between the MSs which have a SPOC (Doherty et al., 2015). However, the Deloitte study from 2015 states that the application of the SPOC concept varies across the MSs and the created structures only partly comply with the ‘one window’ criteria detailed in the EXIM communication, therefore the process remains voluntary and limited in scope (Doherty et al., 2015).

This and new challenges, such as the abolition of border controls at the internal borders between MSs within the Schengen area needed a less-centralised information exchange channel at the internal frontiers, which has led to the creation of the Police and Customs Cooperation Centres (PCCC). PCCCs are located regionally, presenting an innovative approach to cross-border information exchange (statwatch.org and Future Group, 2018). They facilitate instant, direct and smooth information exchange with neighbouring countries, support the operational units in the border areas and help to make quick decision (Salonen, 2010; statwatch.org and Future Group, 2018). The generally high number of cross-border information exchanges is usually not related to the most serious and organised crime (Doherty et al., 2015), petty and medium crime, illegal migration and public order related information exchange is conducted mostly by the PCCCs (statwatch.org and Future Group, 2018). The role of the PCCCs is crucial as the majority of cross-border information exchange is conducted between neighbouring countries (Doherty et al., 2015) and the volume of information exchange is larger in the border areas. Research shows that the information exchange conducted by the PCCC is faster and more efficient than the SPOC conducted one (Kemeny, 2019).

A Frontex initiated pilot project aimed to utilize the Frontex Focal Points which are deployed at the external borders and the PCCC system in order to facilitate swift border management related information exchange. The project, which dates back to 2016, started information exchange among 11 MSs and 17 PCCC. The goal was to institutionalize a real time information exchange between the border crossing points and the staff of PCCC to check and receive relevant information on persons and on vehicles (Council of the European Union, 2016; Frontex, 2018a, 2018b).

The Europol information exchange channel is one of the most widely used channels among the MSs for data sharing (Salonen, 2010). Although this channel is mostly used to exchange and share information related to serious and organised crime between a MS and Europol, the agency has developed and maintained the SIENA system, which provides the opportunity for various data to be exchanged bilaterally between MSs.

Interpol, similarly, to Europol, provides its own data sharing channel around the clock. The so called I-24/7 system facilitates cross-border information exchange among 188 countries to support criminal investigations. All types of police-related data is exchanged through this channel, most commonly checks on persons and vehicle-related information exchange (Salonen, 2010).

Finally, we have to mention the work of liaison officers, who are usually deployed at embassies in a host country. This channel is widely used when sensitive data is requested or when quick information exchange is needed (Salonen, 2010). However, as the primary role of the officer is not information exchange, this channel cannot be used when a huge amount of information is requested.

### 4. Information exchange in practice

Not only differences in national structures, but also the variety of the nature (purpose, type) of exchanged information and the different legal backgrounds has contributed to the creation of a wide range of information exchange channels. Different channels make it ‘more difficult to know which channel, and what means of communication, should be used for the cross-border information exchange’ (Salonen, 2010) and this sometimes ‘leads to confusion by making available several appropriate communication channels’ (Salonen, 2010).

The choice of channel is partly regulated by EU law, as we learned from the above introduced EXIM communication. The use of the Sirene Bureaux and the ENU (which are not the subjects of this research) is exclusive in EU legislation in predefined cases, but the choice of channel for information exchange in other cases is up to the MSs. This seems to be supported by the Swedish Initiative (Council of the EU, 2006), as it states: MSs can choose any channels which are used for international LEA cooperation. Contrary to this, the Schengen Codex states that, the request must be sent to the central national agencies which are responsible for international police cooperation. If the requested authorities do not have the authority to complete the request, it should be forwarded to the competent authority. If the request cannot be made in good time using the central authority, it can be sent directly to the competent police authority. The central authority should be informed by the requester about the request as soon as possible.

The decision of the MS about which channel is to be used in a specific case usually depends on the subject matter, the requested country, the level of confidentiality and urgency. However, the Manual on Law Enforcement Information Exchange (Council of the EU, 2006) suggests observing four criteria in order to select the most appropriate communication channel and to avoid thematic overlaps. These criteria are geographical (origin, residence of person, object), thematic (confidence, channel was used for previous related request), technical (ICT, compatibility) and time approach (urgency, priority) (European Council, 2016). The Manual also states that the requester (end-user) has a significant autonomy in choosing the channel which is considered to be most appropriate and efficient (Council of the European Union, 2010). In order to internally unify the use and the selection of channels, some MSs have produced a manual, mostly non-binding in legal terms, which ensures an overview for the LEA officers. However, stricter and legally binding internal manuals are usually missing ‘as there is a strong tradition of leaving the choice up to the law enforcement officer’ (Doherty et al., 2015).

Despite all these factors, the choice of channel depends on many factors, such as personal considerations, preferences for a certain channel etcetera (Kemeny, 2019), ‘which are not consistent across or

---

2 Europol National Units exchange information related to serious internationally organized crime, such as preventing and combating terrorism, drug trafficking, trafficking in human beings, smuggling of human beings, trafficking in nuclear and radioactive substances, motor vehicle crime, counterfeiting and forgery of means of payment, money laundering. National Sirene Bureaux exchange information on persons wanted for arrest for extradition purposes, third country citizens to whom entry to the territory shall be refused, missing persons, persons summoned to appear before the judicial authorities, persons due to be subject to discreet surveillance or a specific check, vehicles, persons, boats, aircraft and containers being subject to discreet surveillance or a specific check, vehicles, firearms, official documents and banknotes to be seized or used as evidence in criminal proceedings.
even within the Member States’, as we learned from another study (Doherty et al., 2015).

The previously discussed unstructured choice of channel poses problems for the players and officers who are engaged in information exchange and poses a risk to the quality of information exchange (Doherty et al., 2015). The unstructured choice also serves as a ground for sending requests via more communication channels, which causes duplications (Doherty et al., 2015).

In addition to the above-mentioned formal channels, informal communication, typically via personal contacts, also plays an important role. The extent of the use of this channel is impossible to estimate, but there are cases where informal communication channels are used to receive the answer rapidly or to speed up the already ongoing information exchange (Saloven, 2010). As the received information cannot be used in the judiciary procedure, an informal request is usually followed by a formal request at a later stage (Doherty et al., 2015).

5. Factors effecting inter-organisational information exchange

Efficient information-sharing requires adequate organisational-managerial, legal and technological environments, which are determined by various factors such as the Information and Communication Technology (ICT), organisational structure, culture and values, human resources, trust, leadership, rewards, self-interest, legal instruments and regulations. (Council of the EU, 2005; J; Zhang & Dawes, 2006).

5.1. Organisational environment and management

In the literature two main types of organisational structure are distinguished: the bureaucracy and the adhocracy (Duncan et al., 2003; GruszczakBossong and Carrapico, 2016; Lunenburg, 2012; Mintzberg et al., 1989). Bureaucracy can be characterized by formalized and hierarchized structure, functional departmentalisation and by standardized regulations and procedures (Argote et al., 2000). Formalisation is often correlated with ‘red tape’, the presence of excessive, rigid and redundant formal rules or procedures that serve no noticeable organisational functions ‘and result in inefficiency, unnecessary delays, frustration, and annoyance’ (Bozeman & Scott, 1996). This formalisation can hinder and prevent action or decision-making and have a negative impact on innovation, openness to new ideas, motivation (Arches, 1991; Bozeman & Scott, 1996; Chung-An, 2010; Rousseau, 1978). In the field of cooperation, centralisation and hierarchical structure hinder initiatives and actions for the exchange of information, as individuals lack autonomy and managerial approval is required in most decision making processes (Kim & Lee, 2006), which strictly controls the information flow and exchange (Argote et al., 2000; Kim & Lee, 2006; Wheatley, 2006).

On the contrary adhocracy is “consisting of organic structure with little formalisation of behaviour [...] it gives quasi-formal authority to staff personnel”3 which foster adaptability, ensure flexibility and swift response to the current need or to changing environmental requirements4. These organizations can freely exchange information among professionals and communicate beyond boundaries.5 Communication within and among the decentralized organizations is intensive and the informal communication plays an essential role to information sharing. Research found positive correlation between the extent of information sharing and the degree of reciprocal interdependence means each participating organisation possesses information that others need and needs information which others possess.

Organisational culture also influences the attitudes of individuals and the collective actions regarding information sharing. (Creed et al., 1996) Organisational differences, such as the diverse national systems, different cultures, the different geographical locations of national services, the different divisions of police tasks among various organizations and the different task distribution within one organisation result in a different structure of cross-border information exchange. This significantly influences the efficiency of such exchanges (Creed et al., 1996; Tsai, 2002). This structural and cultural diversity and its effect on cross-border information exchange was recognised by the European Commission (European Commission and COM, 2004, p. 9) in 2004, emphasising the importance of creating a common culture and common instruments in order to increase cross-border information exchange and cooperation. The general framework of international police cooperation is characterized by the diversity of the above written national structures and by the regional police organizations and EU instruments.

Researchers found that ‘the style of the leadership can enforce the negative and positive attitude towards information exchange’ (Jian & Jeffres, 2006). An authoritarian leadership style, for example, can dissuade staff from developing a positive approach towards information sharing. Contrary to this, transformational leadership encourages staff to exchange information (Saloven, 2010). Moreover, strong leadership supports the sharing of information, the organisational culture, the reward system and provides vision and guidance which can support initiating and exchanging information in an organisation (European Commission and COM, 2004, p. 9).

The researcher argues that the conditions of the human resources also influence the exchange of cross-border information. One of the main reasons for delays in response is the lack of staff, as the agency ‘may focus on urgent issues within its own organisation when the immediate benefits of sharing information cannot be foreseen’. (Saloven, 2010).

5.2. Policy, legal environment

In the field of cross-border information exchange, studies have pointed out that the requirements of different national legal systems, different data protection and privacy regulations, secrecy and confidentiality issues are among the main hindering factors of cross-border information exchange (Saloven, 2016; Styczynska & Beaumont, 2017). A difference in national data protection and privacy rules regulate the access to the same type of information differently in each Member State (MS). Different national legal requirements and restrictive or varying interpretations of existing rules, as well as uncertainty about what information another MS can provide also hinder efficient cross-border information exchange and violate inter alia the principle of availability. Different national laws lay down different law enforcement procedures for cross-border information exchange which also blocks the process. Judicial approval or the need for special permission for information exchange is a good example, as some countries require court approval to disseminate certain information, while others do not. The different national classification systems, interpretations and a lack of harmonisation of national legislation and the different understanding of EU and international legal bases also pose problems for the exchange of confidential information, and could cause implementation problems (Saloven, 2010).

---

3 Mintzberg, Henry. (1980). Structure in S’S: A Synthesis of the Research on Organisation Design. Management Science. 26.322-341. p.337.
4 Maximini, Dominik, The Scrum culture: introducing agile methods in organizations, Springer 2015, p.18.
5 Edgar H. Schein, Organisational Culture and Leadership, Fourth edition, John Wiley & Sons, 2010. p.168.
6 Bob Travica, New Organisational Designs: Information Aspects, Stamford, Conn. Abtlex Pub. Corp., 1999. p.138.
7 Bob Travica, Information aspects of new organisational designs: exploring the non-traditional organisation, Journal of the American Society for Information Science, Volume 49 Issue 13, Nov 1998. Pages 1224-1244. p.1228.
Finally, in the ICMPD study a lack of strategic approach, the proliferation of non-binding (intergovernmental) instruments, a slow decision-making procedure on the EU level, slow implementation of legal instruments adopted by the European Council (European Commission and COM, 2004, p. 9) and the existence of signed but not ratified agreements (European Commission and COM, 2004, p. 9) were identified as the main policy impediments.

Several EU legal instruments emphasize the importance and create the legal background for cross-border information exchange. Thanks to the ‘principle of availability’ rule introduced in the Hague Programme (European Council, 2005), the information available for a national Law Enforcement Agency (LEA) should also be available to each MS LEA, which in practice means that the exchange of available information cannot be refused by a MS LEA. The programme also emphasizes the importance of border areas where closer cooperation and better coordination is indispensable to deal with crime and security threats. According to desk research the ‘principal of availability’ is a goal that cannot be fully achieved due to existing differences between the national laws and technical systems, operational capabilities and the lack of interoperability (Saloven, 2010).

5.3. Technological Environment

Although researchers argue that challenges deriving from the technological environment are less complex than the factors of the organisational and policy environment (Landsberg & Wolken, 2001), the importance of the technological background must not be underestimated.

The efficiency of inter-organisational collaboration and information exchange can be improved by advances in Information and Communication Technology (ICT) (European Commission, 2016). An appropriate ICT environment can ensure shorter response times and better data quality (European Commission, 2016). The ICT system supports information exchange if different systems are homogeneous, the system combines user friendly ICT applications and has a high number of users. However, the diversity of ICT systems makes the integration into one homogenous system complicated (Atabakhsh et al., 2004). The ICMPD study concludes that, the most common ICT related hindering factors come from the incompatibility of systems, such as different software versions being in place which can create obstacles to opening files, different size limitation of emails, security rules (firewalls, blocking attachment etc.) and a different level of available technology (fax, email, cloud, closed network etc.). The European Commission also recognised the heterogeneity of ICT systems. In one of its documents the Commission has shown that the large number of different and non-interoperable databases and communication systems create duplications and hinder cross-border information exchange (European Commission and COM, 2004, p. 9) as it results in delayed responses (European Commission and COM, 2004, p. 9). More databases and ICT systems make information exchange more difficult, therefore the homogeneity and interoperability of information systems should be improved according to the European Commission. The level of information security, the lack of secured communication channel and the old-style data transfer systems are other factors which can hinder inter-organisational information exchange (European Commission and COM, 2012). Ensuring access authorization, authentication, security and confidentiality are critical in the design of an ICT system (Chau, 2001).

A case management system which helps to evaluate, classify and disseminate information originating from all channels and national authorities and which has an interface to a secured communication platform, increases the efficiency of cross-border information exchange if it is accessible for information exchange channels.

The current ICT systems at the PCCCs are appropriate and help cross-border information exchange, but because of the lack of secured communication channels and in order to ensure privacy and security a large proportion of information exchange is still done by using ‘old school’ techniques, such as postal mail and fax (Saloven, 2010). To overcome these security concerns as a pilot initiative some PCCCs, e.g. PCCC Basel, PCCC CamFranc, PCCK Kerkade etc. started to use the Secure Information Exchange Network Application (SIENA) in 2015. Currently 13 out of the 59 PCCCs are using SIENA in the EU, furthermore a pilot project was launched in the Western Balkans with the same goal in 2021. SIENA is a state-of-the-art platform which provides a secured and fast ICT environment for EU law enforcement agencies and this can facilitate structured information exchange based on the Universal Message Format (UMF). It supports information exchange between MSs and Europol (within the Europol mandate) and it also facilitates bilateral data exchange between MSs (outside of the Europol mandate). The suggestion to use SIENA as a default tool was already emphasised in 2012 in the EXIM Communication (European Commission and COM, 2012).

Most MSs have a large number of different databases and several national LEAs have different policies, legislation and authorization regarding the use and management of their databases. Furthermore, not all necessary databases are available in a timely manner or to all of the staff who conducts information exchange (Saloven, 2010). Following the instructions of the SPOC guideline, several MSs also work with the case management system and its database which helps to evaluate, classify and disseminate the information originating from all channels and national authorities and which has an interface with SIENA and other platforms (Doherty et al., 2015).

6. How to determine intensified cooperation

In the context of the spread COVID-19 and the accompanying security threats related to the uncontrolled (cross-border) movement of persons, the changes in the modus operandis of the organized criminal groups driven by emerging or new demands (e.g. increased civilian demands for illicit firearms10), possible increase of opiate trafficking from Afghanistan11, the emerging new crimes or the proliferation of certain, previously infrequent crimes (e.g. counterfeit COVID-19 vaccines12) requires the intensified use of already existing information exchange channels. To answer this challenge, law enforcement information exchange shall be swift and efficient (Dressler & Duquet, 2021).

In order to achieve the required efficiency during information exchange, decision makers should pay attention to the hindering and supportive environments. The centralised or decentralized nature and the culture of the organisation and the leadership climate are the most important hindering and supporting factors within the organisation-management environment. Policy makers should avoid the use of highly centralised, coercive bureaucratic organisational structures, 

---

8 Saloven, Matik et al. Study on the status of information exchange among law enforcement authorities in the context of existing EU instruments [online]. 2010, p. 83. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/do c_centre/police/docs/icmpd_study_lea_infoex.pdf.

9 Council of the European Union (2017), State of play of the roll-out of SIENA regarding PCCCs, available at: https://data.consilium.europa.eu/doc/document.ST-14629-2017-INIT/en/pdf (accessed 01.12.2020).

10 Dawes (1996), Illicit firearms trafficking in Europe during and after COVID-19, available at: https://vlaamsvredesinstituut.eu/en/newspost/illicit-fi rearms-trafficking-in-europe-during-and-after-covid-19/.

11 UNODC Drugs Monitoring Platform Brief: Possible impact of the COVID-19 pandemic on trafficking in opiates and methamphetamine originating in Afghanistan, available at: https://www.unodc.org/documents/data-and-analy sis/covid/DMF_Brief_short.pdf.

12 Europol (2020), How COVID-19-related crime infected Europe during 2020, available at: https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020.
where leadership favours strict obedience, a lack of openness, a lack of staff autonomy and in which most decisions require management approval, as this results in a less efficient information exchange process.

In order to increase efficiency, a supportive, stable and accountable legal environment, which ensures confidentiality and privacy should be created. The EU legislation plays an important role in creating and maintaining efficient cross-border information exchange. Legislators should strive to establish a clear, appropriately harmonized, similarly interpreted and supportive legal environment in order to increase efficiency. Additionally, legislators and decision makers should avoid rigid regulations, interpretations and procedures as these create serious obstacles during the information exchange.

Regarding the technological environment, we found that a state of the art, user friendly and homogenous ICT system can increase inter-organisational information exchange, but the system must also ensure adequate information security. When there is utmost need, real time information exchange should be carried out using the police information exchange channels, and police channels should be used to feed the decision makers.

Based on the identified hindering and supporting factors, one of our most important suggestions is to create a unified and harmonized legal background for cross-border information exchange and to equip all channels to be able to conduct fast cross-border information exchange. Legislation should also support the timeliness of information exchange, and deadlines need to fit everyday needs and thereby should be decreased. Furthermore, management must be aware of the importance of supporting, transformational leadership in the efficiency of information exchange, which can be ensured by organizing managerial training courses. Management could introduce a tailor-made incentive system and provide appropriate feedback. This could be supported by legislation which creates an institutionalized feedback system providing the opportunity to staff of exchange channels to be aware of the outcomes of their job. Staff and the ICT environment of the channels need to be adequate to carry out secured information exchange 24/7. The establishment of a direct and secure connection between the information provider and the requester would be one of the most feasible solutions. Next, interoperability should be ensured to increase the speed of the channels. User friendly and advanced ICT systems should be created which support rapid information exchange. Minimal requirements and ICT standards need to be elaborated and put in place in which can provide the opportunity to use UMF and secured channels during information exchange.

7. Conclusions

Capability and willingness of the countries to determine shared security challenges is one of the preconditions of an efficient law enforcement cooperation. Due to the existing broad variety of institutionalized cooperation within the EU and with non-EU countries cross-border cooperation still stems from readiness and willingness to use institutionalized cooperation. This is also true during the pandemic, when the response of law enforcement agencies on the changing criminal trends as a side effect of the COVID-19 solely relies on a willingness of sovereign countries to cooperate instead of being forced to acts so.

As we argue above, the institutional capacities for effective cooperation of law enforcement agencies depart from the identification of shared security challenges. This has led to the development of institutional, legal and technical capacity corresponding with the new realities of a globalized world. The authors of this paper have argued that an effective response to upcoming security challenges caused by COVID-19 requires a real-time law enforcement information exchange process and joint commitment in determining common security challenges.

**CRediT authorship contribution statement**

**Gábor Kemény:** Conceptualization, Methodology, Validation, Supervision. **Michal Vit:** Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing.

**Declaration of conflict of interests**

Authors of above-mentioned paper do not claim any conflict of interest in regard to submitted manuscript.

**References**

 [1] EEAES. (2020). *EU actions against coronavirus. European external action service*. https://eeas.europa.eu/headquarters/headquarters-homepage/75968/eu-action-against-coronavirus_en. (Accessed 20 April 2020), 2020.

[2] Europol. (2020a). *Pandemic profiling: How criminals exploit the COVID-19 crisis* (p. 2). European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-documents/pandemic-profiling-how-criminals-exploit-covid-19-crisis. (Accessed 20 April 2020), 2020.

[3] Frontex. (2018a). *Risk analysis for 2018* (p. 6). Warsaw: Frontex. European Border and Coast Guard Agency. https://frontex.europa.eu/assets/Publications/Risk_Analysis_Risk_Analysis_for_2018.pdf. (Accessed 2 February 2019), 2018.

[4] Europol. (2020b). *Pandemic profiling: How criminals exploit the COVID-19 crisis* (p. 13). European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-documents/pandemic-profiling-how-criminals-exploit-covid-19-crisis. (Accessed 20 April 2020), 2020.

[5] European Commission. (2020a). *Speech by Commissioner Kyriakides on COVID-19*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_20_337. (Accessed 20 April 2020).

[6] Riehle, C. (2020). *Europol: How COVID-19 shapes serious and organised crime landscape in the EU, turin.europa.eu* https://ecrin.eu/news/europol-how-covid-19-shapes-serious-and-organised-crime-landscape-eu/. (Accessed 20 March 2021).

[7] Politico, Danish boat in Aegean refused order to push back rescued migrants.(2020). https://www.politico.eu/article/danish-frontex-boat-refused-order-to-push-back-rescued-migrants-report/. (Accessed 20 April 2020).

[8] European Commission. (2020b). *Speech by commissioner Kyriakides on COVID-19*. https://ec.europa.eu/commission/presscorner/detail/en/speech_20_337. (Accessed 20 April 2020).

[9] Sarjoe, N. (2017). *Understanding inter-organisational information sharing*. Master thesis. Delft University of Technology.

[10] European Commission, COM. (2004). *Enhancing police and customs co-operation in the European Union, 0376 final. Brussels* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0037. (Accessed 11 October 2019) https://repository.tudelft.nl/islandora/object/uuid:b8f5d904-51bb-43c0-88bb-d2d7e979cf4d/datastream/OBJ/download (accessed 8 January 2020).

[11] European Commission, COM. (2015). *The European Agenda on security, 185 final*. Strasbourg 28 April 2015 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0018&from=EN. (Accessed 5 May 2019), 2015.

[12] 2017/800/435/110707/2016 Council of the European Union. Programme of The Netherlands Presidency of the Council of the European Union http://www.euonec.eu/sites/www.euonec.eu/files/attachment/files/national programma-engels.pdf. (Accessed 10 December 2019), 2016.

[13] Council of the EU. (2007). *Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1544587087919&uri=CELEX:32007D0533. (Accessed 10 October 2019).

[14] Council of the EU. (2005). *Decision 2005/681/JHA of 29 September 2005 establishing the European police college (CEPOL) and repealing decision 2000/820/JHA*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32005D0681. (Accessed 8 January 2020).

[15] European Parliament, 2016 European Parliament.. (2016). *Regulation (EU) 2016/794 of the European parliament and of the Council of 11 May 2016 on the European union agency for law enforcement cooperation (Europol) and replacing and repealing Council decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Article 4*.Dawes, 1996 Dawes, S S. (1996). Interagency information sharing: Expected benefits. *Manageable Risk*. doi:10.1002/SII(1520-6686(199622)15:3<377::AID-PAM3>3.0.CO;2-F

[16] Zhang, J., & Dawes, S. S. (2006). *Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks*. doi:10.1080/11539786.2006.11055189

[17] Gruszczak, A. (2016). *Police and customs cooperation Centres and their role in EU internal security*. In R. Bossong, & I. Carrapico (Eds.), *EU borders and shifting internal security* (p. 165). Heidelberg u.a.: Springer.

[18] Duncan, W. J., LaFrance, K. G., & Ginter, P. M. (2000). *Leadership and decision making: A retrospective application and assessment*. doi:10.1177/10717919030090401

[19] Mintzberg, H. (1989). *The structuring of organizations*. In D. Ash, & C. Bowman (Eds.), *Readings in strategic management* (pp. 322–352). London: Palgrave.

---

13 Unified Message Format (UMF) is a common framework for the structured cross-border information exchange, it defines a common vocabulary and logical structures for commonly exchanged information.
