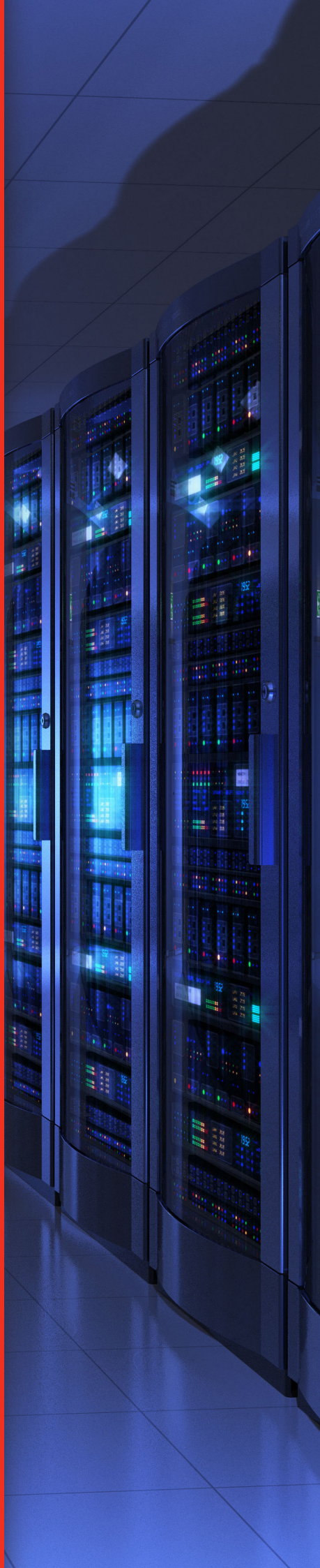
GLOBSEC
POLICY INSTITUTE

Counter-terrorism Intelligence Exchange Reform Strategy



GLOBSEC INTELLIGENCE REFORM INITIATIVE
Supporting Paper

GLOBSEC
POLICY INSTITUTE

Counter-terrorism Intelligence Exchange Reform Strategy

GLOBSEC INTELLIGENCE REFORM INITIATIVE
Supporting Paper

STRATEGIC PARTNER OF GLOBSEC

Microsoft

Introduction

Ibrahim El Bakraoui, a Belgian national, was in Gaziantep, near the Syrian border, when he was arrested by Turkish police. As a "suspected terrorist", authorities quickly moved to expel him from Turkey. Turkish police notified the Belgian consulate of his deportation but Belgian authorities did not pursue El Bakraoui for his alleged links to terrorism. Nearly a year later, El Bakraoui and his associates carried out the 2016 Brussels bombing, killing thirty-two civilians and injuring 316 more, the deadliest act of terrorism in Belgium's history. Eight days before the attack, a day after a failed raid by Belgian authorities to arrest El Bakraoui, the FBI shared with Dutch intelligence services that they had been tracking El Bakraoui for his alleged terrorist connections since September 2015.

Failures of intelligence sharing have marked counter-terrorism efforts since 9/11. Before 9/11, U.S. intelligence and law enforcement agencies had failed to share information about Nawaz Alhamzi and Khalid Al-Midhar, two individuals who eventually carried out the attacks. Since then, insufficient intelligence among counter-terrorism authorities has been a hallmark of most major terrorist incidents. European states have also struggled to improve coordination and intelligence-sharing among their domestic intelligence agencies and law enforcement. Unlike the U.S., European counter-terrorism efforts are complicated by the interconnectedness of domestic and regional security. Unfortunately, regional cooperation is also significantly hampered by legal restraints on cross-border information-sharing and, more troubling, general distrust.

This paper will examine the current state of intelligence exchange among transatlantic intelligence services. It will explore both the cultural and operational obstacles to greater and more efficient intelligence exchange as well as the best practices and failures of current information exchange platforms. Considering these obstacles and current practices, we set out several fundamental design principles necessary to create an effective intelligence exchange. We suggest that a decentralized, federated search interface, designed to overcome interoperability, trust, and security issues, could greatly improve intelligence-sharing and encourage greater collaboration among partners.

Crisis of Intelligence-Sharing

Intelligence-sharing among transatlantic intelligence agencies currently operates through a stilted, bureaucratic and slow process. Agency information exchange developed from a rudimentary starting point, the sharing of diplomatic reports. The exchange later expanded to include selected intelligence assessments and, most recently, the creation of joint analyses. Unfortunately, in the absence of formal intelligence exchange, most information sharing occurs through informal media—like the Club de Berne (CdB).[1] While a voluntary and non-decisive organization, the CdB has offered senior intelligence officials a forum to exchange and discuss high-level intelligence strategy. In the aftermath of 9/11, CdB established the Counter-Terrorism Group—which is believed to generate threat assessments, collaborate with U.S. envoys and established their own threat database. Most importantly, representatives of CTG meet on a weekly basis—both demonstrating, and attempting to support, the demand for a more consistent and regular exchange of intelligence at the tactical level.

Among European law enforcement agencies, Europol operates as the most significant collaboration point for Member States. Without any collection capabilities of its own, Europol relies on voluntary information and intelligence provision from member states and notifies MS when they uncover any criminal connections or situations through their intelligence analysis. This information is transmitted among MS and third parties, like the U.S., through the Secure Information Exchange Network Application (SIENA), which provides fully-secure information transfer. Europol also maintains the most strict information-handling codes, reflecting MS concerns about shared intelligence usage.

In support of European efforts to grapple with the increasing threat of terrorism, the European Counter Terrorism Centre (ECTC) was established within Europol, which leverages integrated databases and

1 The Club de Berne is an intelligence sharing forum which, while not an EU organization, convenes the heads of intelligence services for all MS of the EU, Norway, and Switzerland.

computer networks to store and exchange counter-terrorism (CT) data. The ECTC databases track foreign fighters, illegal arms trafficking, terrorist financing, and jihadi internet activities. Users access data through the Europol Information System. Access rights can be tailored for individual user access and data owners can restrict, and receive notification about, data usage. This current system has gone a long way to accelerate law enforcement response to terrorist activities and increase MS police trust in Europol. However, many intelligence services are still reluctant to share information with Europol, limiting Europol's value to attack reaction rather than attack prevention.

Interpol has also made significant progress on CT law enforcement. Interpol's Counter-Terrorism Fusion Centre investigates organizational hierarchies, training, financing, and terrorist motives. The centre focuses on law enforcement information exchange, integrating and analyzing criminal data, foreign fighter tracking, and border security records. Interpol still, however, suffers from the same trust issues with MS intelligence services as Europol.

However, CT leaders recognize that, to advance preventive efforts throughout the transatlantic, MS will need to build mutual capacity and increase integration among information sources. European concerns and emphasis on privacy have heretofore prevented the use of digital intelligence and data mining tools but the recently passed Passenger Name Record (PNR) legislation opens new opportunities to investigate and track suspects for CT purposes. In the United States, PNR tracking and analysis was a critical investigation method for the CT effort after 9/11.

Speed also continues to frustrate advocates for information exchange, as intelligence services move through a slow, bureaucratic process for sharing intelligence. Interoperability of data is not a default characteristic for cleared intelligence, creating further delays to intelligence analysis. Investigations are also delayed by the intelligence service tendency to share pieces of intelligence multiple times, bilaterally instead of a single time multilaterally. Even in cases where trust occurs and intelligence is exchanged, these operational inefficiencies can impede successful CT efforts.

In the 2016 GLOBSEC Intelligence Reform Initiative Report, many interviewees reiterated that distrust still permeates and obstructs coordination on intelligence-sharing in support of counter-terrorism efforts. A leading cause of this distrust, often mentioned as an exchange impediment for Europol and Interpol, is the capacity gap and control issues between European states' intelligence and law enforcement agencies. Inadequate evidence gathering, case management, and prosecution by less capable agencies can lead to law enforcement failure and waste of the contributing agency's investigation efforts. Agencies fear that sharing information with less capable agencies could result in leaks of covert operations and procedures, 'burning' of intelligences sources and loss of information control. Agencies also do not trust that if intelligence is passed along, they will be able to retain control of when it is actioned and that the recipient will respect the originator legal framework.

For some intelligence liaison, information-sharing is complicated by lingering Cold War distrust between recently democratized European states and those with longer democratic traditions.[2] Former Western bloc states cite fears about divided loyalties for certain intelligence leaders, unclear control mechanisms for intelligence, and possible leaks as impediments to greater information-sharing with former Eastern bloc states.

Technical gaps also stand in the way of successful operationalization of CT intelligence. Interoperability is not standard during information exchange, requiring recipient formatting before analysis can take place. Shared intelligence is also often altered and controlled based on the data privacy laws of the originator MS. The lack of harmonization and differing privacy standards can lead to varying levels of detail and value for shared intelligence.

2 GLOBSEC Intelligence Reform Initiative, Reforming Transatlantic Counter-Terrorism, 19 (See Bibliography)

Intelligence Exchange Examples and Best Practices

While intelligence exchange may not be operating at the desired level, there are a number of existing information exchange systems throughout Europe which can provide some understanding of how classified information exchange can operate—and how effective it is.

Schengen Information System (SIS): SIS is a European Commision database used by EU MS to distribute information for national security, border control, and law enforcement. Arguably the most successful of all European information exchanges, MS are individually responsible for entering and updating information within the database. They can also engage each other in supplementary information exchange, using a dedicated supplementary data request through the National Entry Bureau. In meetings to propose revisions to current European information exchange, the Commission agreed that SIS should be expanded to provide a greater range of alerts, greater use of biometrics, and, most significantly, enlarged access for law enforcement agencies.[3] Such revisions would make it "mandatory for Member States to issue alerts on persons related to terrorist offenses". This type of automated warning or alert to law enforcement, from any EU MS, about credible threats seems to reflect the European Commission's efforts to prevent future intelligence failures, like the case of El Bakraoui. SIS is the most actively used information, both for entry and consultation, which could be credited to the requirements on EU MS as signatories to the Schengen agreement.

European Information System (EIS): EIS provides a centralized repository for data on crimes, suspected/convicted criminals, criminal offenses, and criminal resources. Differing from SIS, issuing authorities have full control over data inserted in EIS and submission is on a voluntary basis. A downside of the voluntary arrangement, however, is that contribution and utilization of EIS is quite deficient, with more than 90% of contributions about Foreign Terrorist Fighters (FTF) coming from just five member states.[4] The ECTC has also noted that there is a significant discrepancy between the high numbers of alerts in the SIS and the limited number of foreign terrorist fighters cases in the EIS, indicating, among other things, that participating states are not even entering information, previously shared with SIS, into EIS.

Prum Framework: Adopted by the Council in 2008, the Prum decision sets out a set of rules for operational police cooperation. Unlike SIS and EIS, the Prum framework is focused on automated sharing of internal data. Rather than searching a database or making a formal information request, Prum allows EU MS to access each others automated DNA analysis files, automated fingerprint identification systems, and vehicle registration data. When such evidence is found at a crime scene, it is automatically compared with samples from all other EU MS databases. While an effective tool, not all MS currently bound by Prum have taken the necessary steps to stand up the system.

European Criminal Records Information System (ECRIS): ECRIS is a *decentralized* information system for the exchange of criminal records among most members of the EU. Rather than establishing one central repository, records are maintained in national databases and exchanged electronically by request. Despite the obvious utility for both criminal investigation case-building and prosecutorial case-building, less than 5% of convictions of third country nationals referenced any corresponding criminal records in other MS. Even though the data might be available, law enforcement does not have any situational awareness of who holds the data. In January 2016, the commission proposed to upgrade the system by establishing an index system to enable national authorities to identify which countries hold criminal records for a person of interest.

Eurojust Case Management System (ECMS): Rolled out in 2004, the ECMS was developed to manage and coordinate prosecutions in which Eurojust is providing support, facilitate access to information on ongoing investigations and prosecutions, and enforce Eurojust data protection rules through a system of permissions, alerts and logging.[5] To the benefit of law enforcement, ECMS provide case registration, meeting organization, message exchanges, statistical analysis, object-oriented network analysis, and automated detection of links between cases. While the system provides a number of valuable tools

3 Dumbrava, European information systems in the area of justice and home affairs

4 Ibid.

5 Eurojust Council Document No. 11260/15

for case management and direct collaboration among investigators, limited useful information has been entered into ECMS, in large part due to many national desk reliance on manual files and case data does not follow a common standard on details and terminology.

Examining these various information exchanges, we can see that, quite often, their effectiveness is rooted in their structure and operational goals. Required contribution provides for more useful data than voluntary, automated alerts are preferable to data requests, non-standard format is a major obstacle to effective use. It is important to recognize, however, the interrelations between these issues. If non-standard formats frustrate contributors to an information exchange, they will value it less—and contribute less. If information contribution is driven solely on the contributor's prerogative, their apathy may have them contribute information in a non-standard format, if at all. The drawbacks of these systems all feed into each other, in a race to bottom started by their originating design. An effective system must overcome the apathy, overcome the trust issues, overcome the capacity issues. Drawing from the 2016 GIRI report, and the lessons of the aforementioned information exchanges, we believe there are six critical requirements, or principles, to establish an effective information exchange.

Principles to Trust

Technology is not, by itself, a solution for trust and capacity issues. Transatlantic intelligence agencies could have the most dynamic intelligence database but, without data, it would prove useless. Agencies could be ready and willing to share information, but without a system to communicate and share intelligence safely and securely, any efforts would also fail. The principles and recommendations underlying the creating of a technology solution for intelligence exchange must seek to bridge both the operational and technological gaps within the community. Recognizing this, there are several principles which motivate the structure and capabilities of our proposed system:

- **Data Standardization**: A continuing frustration, and major impediment to effective intelligence exchange, within the intelligence community are the continuing usage of legacy technologies and proprietary solutions which are based on unique data formats. Non-standard data practices can produce intelligence in multiple unique formats with data gaps or excess, requiring additional levels of processing and even follow-ups to clarify integrity issues. The inherent uncertainties can frustrate analysts and, in turn, decrease the desire of intelligence representatives to engage in intelligence exchange. Systems using non-standard formats are typically not interoperable, meaning that authorities must manually request and pursue partner intelligence. Within the U.S., law enforcement and intelligence agencies information exchange has benefited from the issuance of information exchange standards. The National Information Exchange Model (NIEM) Standards "defines agreed-upon terms, definitions, relationships, and formats—independent of how information is stored in individual systems—for data being exchanged.[6] For participating agencies, when intelligence is prepared for exchange, it is converted to match NIEM Standards—allowing for easy processing by the receiving agency. Producing analysts know what and how data should be included, without significant consultation, and receiving analysts have a known format and pre-established method for integrating the data into their existing analysis. Such standards allow for less laborious, faster exchange and provide for easy consumption by the receiving service. Internal intelligence reports can even be automated for conversion to the standardized format, only requiring a check by an intelligence officer and reducing the majority of the workload. In a more sophisticated environment, cognitive algorithms could also be used to automatically pull the standard data fields from any inputted data, not just pre-formatted intelligence reports. These algorithms can extract PNR from a criminal report, identify suspect images from photographs, or provide contextually-aware translations of foreign intelligence.

6 National Information Exchange Model, Developer Resources.

- **Data Classification:** A continuing deterrent to intelligence exchange is fear of data misuse on the part of the receiving entity. Once the developing agency hands over data to the receiving organization, they lose control over how that data is used, who has access to it, how it is processed and presented. Improper handling on the part of the receiving entity could lead to damage to the developing agency's intelligence gathering apparatus or reveal secret information to unapproved entities. Contributors are also concerned that data recipients will not appropriately respect the complicated national and multi-national legal arrangement which govern data transfer and usage. A control-focused data exchange would label and map intelligence with specific distribution rules, much like the Traffic Lights Protocol, governing how exchanged data can be used.[7] Similar to the Traffic Lights Protocol, entered intelligence would have a forced classification labeling, with both visual and metadata identifiers to clearly identify how the intelligence can be transferred or manipulated. Distribution could be limited to a specific task force, to those with a certain level of demonstrated security, to certain types of usage. This classification system could even be automated through an access management system to ensure that data movement and usage complies with the authorized data governance rules and convince data holders that intelligence usage will comply with their desired classification. In a more sophisticated environment, intelligence could even be scrubbed according to the geography of the requesting agency (ex. Data travelling from Germany to France would be altered differently than data travelling from Germany to the US).

- **Data Protection**: Intelligence exchange throughout the transatlantic is often varied due to data security and integrity concerns. While members of Five Eyes can be sure that their alliance members have reasonably high levels of security to protect their data, certain members of the transatlantic community have been, and continue to be, the victims of data breaches and data manipulation. Any instrument which seeks to trade or store classified information is going to be an even greater target for sophisticated cyberattacks. The data is also threatened by the possibility of data manipulation, to either obfuscate intelligence data or purposefully mislead intelligence consumers. Such a scenario could have dire consequences for the intelligence operations and cause significant intelligence failures. The individual exchange partner agencies would also require a high level of security in order to be provided with access to sensitive intelligence. The mechanism could also leverage out-of-band processes for validating the integrity of exchanged data.

- **Data Tracking**: As previously discussed, traditional exchange of intelligence comes with the fear that data can be transferred endlessly, to authorized and unauthorized personnel—and even outside entities. A trusted intelligence exchange would then require a transparent tracking system, to register who, how, why, and where someone has generated a request for intelligence exchange. An auditable data trail such as this would allow for advanced compliance management. Data tracking is also a significant asset for maintaining a clear chain of evidence and provides a clear usage history for digital forensics, in the case of date breaches or procedure violations. Such a system could be implemented through a compliance tool or even a tamper-proof blockchain ledger, such that continuity could be maintained among FIU servers in the case of a disruption or compromise.

- **Data Contribution**: The most significant barrier to intelligence exchange is always mutual contribution. Participants are eager to receive intelligence from partners but more reticent to share anything of their own. There is no way to compel the dissemination of intelligence to transatlantic partners, so contribution of intelligence must occur on a voluntary basis. Unfortunately, without burden-sharing among partners, exchange, like any foreign relation, can become anemic and sharing can break down. However, exchange can be supported and contributors encouraged by structuring the exchange in a configuration that favors contribution. By establishing different layers of access within an intelligence exchange, based on contribution level, partners can no

7 US-CERT, Traffic Light Protocol (TLP) Definitions and Usage

longer free ride within the system. If an intelligence partner contributes only a small amount of intelligence, they will only receive a small amount of intelligence in return. If they increase their contribution, they will receive more. This can alleviate the frustration of free-riding for contributors and puts pressure on free-riders to contribute more—both to access valuable intelligence and receive access to the inner circle of exchange.

- **Data Insight**: While not an obvious barrier, data insight is a necessary component to an intelligence exchange. Exchange platforms, like any other enterprise, are evaluated on their performance and success. While contribution levels are an important indicator. active utilization is also a significant metric for a system's success. If analysts are frequently using an exchange platform for analysis, beyond even the core process of exchanging information, then the system should be considered a valuable resource and be supported. Considering the technologies available, intelligence exchanges should be equipped with cognitive technologies, like computer vision, face recognition, emotion recognition, language understanding, speech and text recognition, and multilingual analysis. Analyst should be able to, without programming skills, correlate objects and visualize data within the system. Machine learning algorithms and open-source programming could enable analysts to develop trend and pattern analysis using statistical computing and graphics. Systems should be leveraging emerging predictive analytics to correlate all-sources of data and uncover hidden connection. Offering cutting-edge analysis tools significantly increases the 'stickiness' of an intelligence exchange platform, heightening its value proposition and encouraging greater participation and support from its members' leadership.

A New System of Exchange

This paper suggests that the creation of a decentralized federated search interface could effectively bridge the trust and capacity gaps which currently frustrate effective classified intelligence exchange. In 2006, the European Commission established an informal group of the EU member state Financial Intelligence Units (FIUs) to encourage exchange of information and collaboration on the investigation of money laundering and terrorist financing. Soon afterwards, the EU FIUs proposed and developed their own intelligence exchange system, called FIU.net.[8] Now a fully funded part of Europol, FIU.net is a decentralized computer network which provides request-driven and automated data analysis of network-wide information.[9] Each EU MS FIU has its own FIU.net server, where they upload all information which they wish to contribute to the exchange. When a participating FIU wants to search for any relevant information from fellow FIUs, they upload the subject data to the system and initiate a request to search for connections between their data and the data on other FIU servers. If there is relevant data, the user is notified and they can then initiate communication with the data holder about accessing the information. The service also offers an automated analysis tool, called Ma^{3}tch, which offers continuous, anonymous matching of information within the FIU.net servers. An FIU.net server will generate a hash of all the data fields in a piece of intelligence, like the name "John Smith".[10] The server will then transmit this hash to all other FIU.net servers, where it will be compared against the hashes of data fields for their own intelligence. When matches occur, both FIUs are notified about the possible link between their intelligence. The information-sharing platform is structured in such a way that providing intelligence is the path of least resistance and just opting-in can yield enormous intelligence benefits.

8 When the EU MS created their Financial Intelligence Units, they were tasked with fighting these crimes within their own countries. However, recognizing that these activities operated across EU MS, and across the world, the Dutch FIU proposed that the FIUs of France, Italy, Luxembourg, UK and the Netherlands work together and exchange intelligence. Eventually, the FIU of all EU Member states united to create FIU.net, which allows an individual FIU to search if any FIU partners have relevant intelligence to any of their ongoing investigations. Europol, Financial Intelligence Units – FIU.net.

9 Europol, FIU.NET and MA3TCH

10 A hash is a computational operation which take an inputted object or data field and outputs a small number or string. In most cases, and the case mentioned here, hash operations are also cryptographic, meaning that they are resistant to identifying the original inputted object based off of examination of the output string.

The decentralized, federated interface searches for connections between the data in the user's server and the servers of network members. When a shared data object is discovered, both users are notified.

The creation of a "TIU.net" (Transatlantic Intelligence Unit), a federated search interface, could leverage the cross-domain protections of FIU.net which facilitate classified intelligence exchange and, incorporating our trust principles, provide a system with valuable, actionable intelligence for security authorities. Intelligence services would have their own, on-site server where they would contribute intelligence. Other intelligence services would not be able to access this server nor transfer data from it. When an intelligence analyst needs to determine if there is other available intelligence, they would generate a request from their server, submitting the NIEM-standardized data in the pre-set data template. In a sophisticated environment, both structured and unstructured data, from internal classified intelligence, open-source intelligence, and even Internet of Things sources, could all be automatically processed into a NIEM standard format and forwarded onto the platform. "TIU.net" would then search other servers for data matching the requested fields. If there is a match, the analyst can then open up an automated data request to the hosting entity, to begin the process for gaining approval for data access. The data owner would then be able to approve or deny the request for access and, in the case of approval, classify the data access according to how it can be used, manipulated, or disseminated. In cases where intelligence access is restricted, the system would automatically scrub the intelligence of higher classification data and the data tracking would ensure strict compliance to desired distribution and usage standards.

These kinds of rigorous and clear rules for data usage, respecting both security, regulatory, and privacy concerns, would go a long way to supporting legal and affective intelligence exchange and support a growing culture of pairing rigorous analysis with respect for civil liberties. However, it would still provide an unprecedented level of intelligence awareness and data availability for all participants in the federated architecture. Much as has been proposed for the European Criminal Record System, an increase in awareness of possible data available could yield massive benefits to individual intelligence efforts and cooperative arrangements. The speed and automation of making data requests would overcome the significant, manual processes in the bureaucratic process for getting data access. By pre-selecting data which is authorized for access under the system, the system is inclined to the sharing of the information, though the data holder may still set restrictions on how it can be used. An automated pattern recognition system, akin to the Prum Framework or Ma^{3}tch could actually generate intelligence insights and investigatory leads. As suggested for the Schengen Information System, the platform could even create alerts to law enforcement authorities in cases of credible threats. In the case of a foreign fight like El Bakraoui, a system like this could have automatically indicated a connection between FBI and Dutch investigations and generated an alert for Belgian authorities. Depending on the data classification governing usage and dissemination, member agencies could leverage more advanced predictive analytics to correlate shared data and uncover previously unknown people and entities of interest.

When intelligence agencies are in a position to collaborate, even among allies, there should not be bureaucratic or technical obstacles to that collaboration. Setting up joint operation centers should not be fraught with technological pain points, like modifying source code for interoperability, but rather

should leverage infrastructure which is readily configurable to support intelligence fusion efforts. In cases where intelligence agencies wish to work more closely, the proposed federated system would have the option of creating access-controlled, federated collaboration between intelligence services. Bilateral and multilateral agreements could provide for the development of certain "communities of trust" on the platform, providing access credentials for participating members to access data without a data request process. Collaboration through investigative workbenches allow for the sharing of information, real-time communication, and joint development of intelligence reports. By limiting access based on contribution level, intelligence partners would also need to contribute more to gain access to these attractive capabilities, increasing the incentive to more actively participate in the intelligence exchange.

Such an exchange would require a high level of security, both for its infrastructure and within the internal systems of the partner agencies, to mitigate any possibilities of data leakage from internal or external attacks. The platform should be developed under the Secure Development Lifecycle Methodology, complying with NIST 800-4, and meet all partner security and privacy requirements. An intelligence exchange mechanism would require, among other protocols, the use of reliable identity management across services and dynamic rules of distribution. Rather than being provide blanked access, based on clearance level, users would instead be provided credentials according to a "need-to-know" protocol, accessing only the data and services required to perform their specific job duties and fulfill their responsibilities to any collaborations. Their usage would also be subject to situational restrictions, implementing time limits on access to certain services and restricting their usage to an approved geography of use (also known as "geo-fencing"). The system should require default encryption on all materials (using a mutually developed encryption algorithm), require multi-factor authentication (leveraging factors like biometrics or ID tokens), and provide advanced threat detection and monitoring capabilities (especially to protect against privilege escalation efforts). Concerns about insecure partner agencies can be accommodated by limiting the level of access to intelligence based on insecurity. If partners do not meet certain minimum standards, they will be significantly limited in the amount of data and scope of data they can request. In the case that their systems are breached, intruders will not be able to use the agency credentials to gain access to another agency's intelligence on the network. Once the partner has implemented the necessary security, they can then be granted greater access to request and use data on the exchange.

Technology to Trust

Trust is the most significant barrier to intelligence exchange. An intelligence services needs to be able to trust that the recipient of data will use it as asked, will not distribute beyond the approved representatives. They also need to be able to trust that, regardless of whether the recipient uses intelligence as desired, they have the appropriate protections to prevent others from gaining access and misusing the data. With such major concerns to contend with, it is no wonder that effective classified intelligence exchange has been limited, up till this point, to intimate circles of trust, like the Club de Berne or Five Eyes.

However, our enemies have no such issues collaborating. They are working together, sharing information, and planning operations. How can we, facing that, maintain our skepticism and effect half-hearted action to cooperate on counter-terror intelligence exchange. This paper proposes a new intelligence exchange, specifically designed to allay participant fears of misuse and data compromise. The configuration of the interface provides an engagement-inclined operating environment, which hopes to increase the connections and activities among members. By removing the barriers to exchange intelligence, the system should help to increase trust and offer significant support to intelligence operations and criminal investigations, demonstrating the value of data fusion.

Cooperation among allies should not stop with a decentralized search interface. The proposed system provides a much greater situational awareness of intelligence available but it does not, efficiently, put that intelligence to work. As the exchange develops, and collaboration through the platform

occurs, agencies will develop or improve their working relationships and increasing the trust between partners. Once participating agencies reach an acceptable level of trust, they should move forward with the development of a shared fusion center. A data fusion center would offer a level of insight and prediction beyond anything a federated search could offer. More than just simple correlation, a fusion center automates an array of analytical tasks and offer a whole dashboard of tools for establishing network and recognizing patterns in entered data. Any data, structure or unstructured, can be entered into a fusion center in real-time. A center would pull in intelligence from classified services, as well as any data streams connected with the system, ranging from social media feeds to Internet of Things (IoT) devices. Once this intelligence has been accumulated in data lakes, fusion centers can leverage a number of advanced processing techniques to draw connections between various intelligence sources. Cognitive algorithms can "understand" the messages of raw documents and extract pertinent information, recognizing names, objects, and places.

Just the processing of these massive data sets can provide a host of actionable intelligence that would not have been available previously—and far quicker too. However, fusion centers add even greater value through their advanced analytics tools. "Activity-based intelligence" can track flows and patterns of behavior by various entities and actors, across geographies. Sentiment analysis can even provide interpretations on the tone and intent behind a text's writers. Using a fusion center, and these advanced analytic capabilities, intelligence analysts from varying services can collaborate, analyze, visualize, and act on data from one centralized location. The platform would be the most effective method for analyzing the ever-increasing amount of intelligence data and provide unprecedented insights for investigation or early-warning threat identification.

It will take a significant effort to get to this level of intelligence cooperation, especially with current technological and trust barriers. We cannot get there, however, unless we begin to tackle these barriers through engagement. Trust cannot grow in isolation, it must be cultivated. The creation of a new intelligence exchange, outlined here, would significantly help to raise the level of trust among partners and, in doing so, enable us to take greater action against emerging threats.

Bibliography

Dumbrava, Costica. *European information systems in the area of justice and home affairs*. Brussels: EPRS, 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603923/EPRS_IDA(2017)603923_EN.pdf.

European Union. European Presidency. *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area.* Working Document No. ST 8437 2016 REV 2. Brussels, 2016. http://data.consilium.europa.eu/doc/document/ST-9368-2016-REV-1/en/pdf

Europol. *Financial Intelligence Units – FIU.net.* The Hague: Europol, 2016. https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net.

Europol. *FIU.NET and MA3TCH*. Filmed [2016]. Vimeo video, 04:43. Posted [2016]. https://vimeo.com/145121509

EY. *Evaluation report on the implementation of the Eurojust Council Decision.* Eurojust Council document (11260/15). Brussels: European Council, 2015 http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejlegalframework/Evaluation%20of%20the%20implementation%20of%20the%20Eurojust%20Council%20Decision%20-%20Final%20Report/Evaluation%20of%20the%20implementation%20of%20the%20Eurojust%20Council%20Decision%20-%20Final%20Report.pdf

GLOBSEC Intelligence Reform Initiative. *Reforming Transatlantic Counter-Terrorism* (Bratislava: GLOBSEC, 2016).

National Information Exchange Model, *Developer Resources*. Washington, D.C.: NIEM, 2013. https://www.niem.gov/techhub/iepd-resources.

US-CERT. *Traffic Light Protocol (TLP) Definitions and Usage*. Washington, D.C.: US-CERT. https://www.us-cert.gov/tlp.

GLOBSEC
POLICY INSTITUTE

Klariská 14
811 03 Bratislava
Slovak Republic
Phone/Fax: +421 2 5441 06 09
info@globsec.org

www.globsec.org