Conference Report

eu-LISA and Frontex joint conference

EU Borders - Getting Smarter Through Technology

17 October 2018
Tallinn, Estonia

eulisaconference.eu
eulisa.europa.eu
frontex.europa.eu
eu2018.at

Printed by Ilotrükk in Estonia
Luxembourg: Publications Office of the European Union, 2019

Photo Credits: Sven Tupits

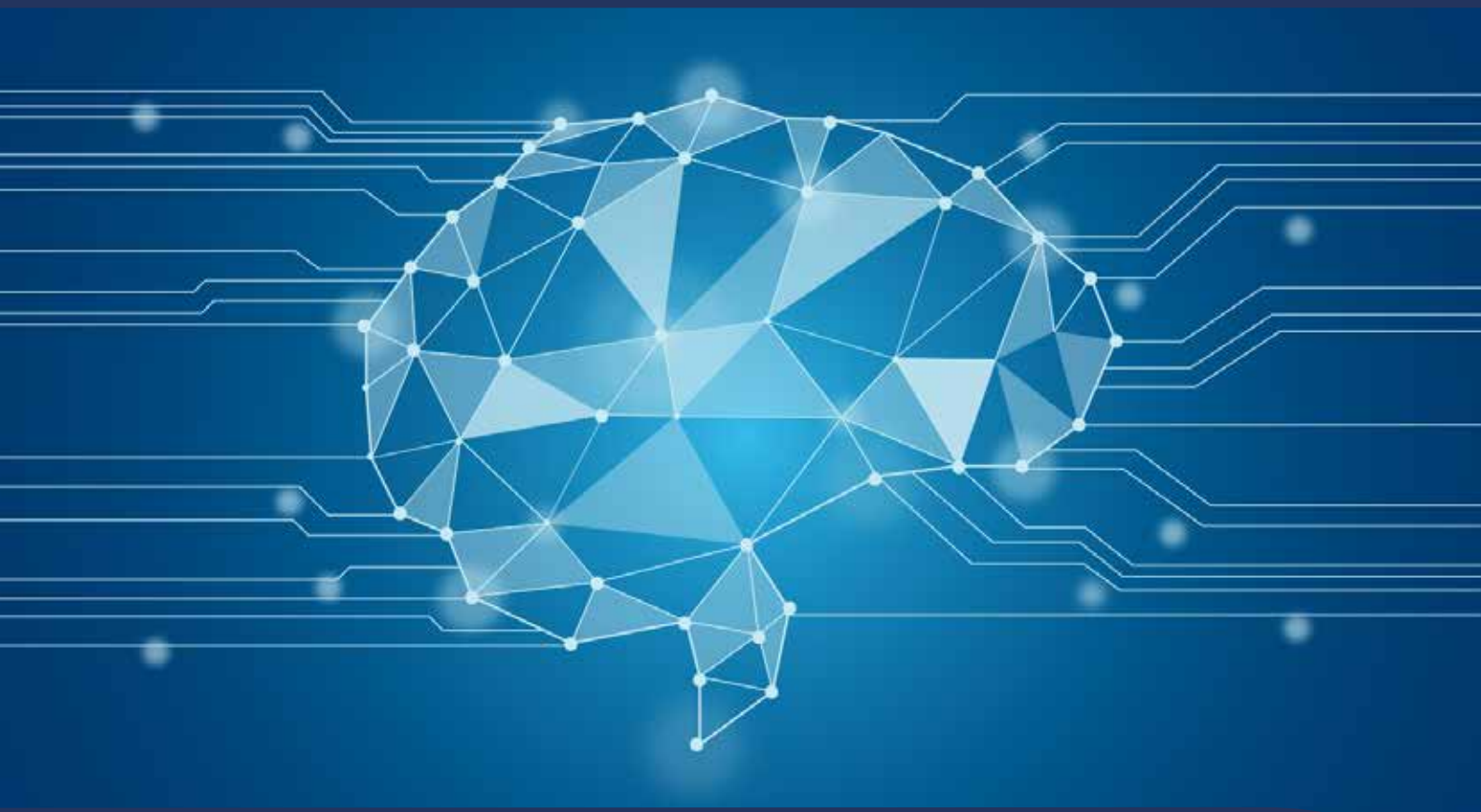
This report is based on audio/video recordings and notes taken during the Conference. It does not purport to reproduce in extenso all debates and intervention. The opinions expressed are those of the speaker(s) only and should not be considered as representative of eu-LISA's official position.

ISBN 978-92-95208-79-7
doi:10.2857/993255
Catalogue number: EL-01-19-006-EN-N

Conference Report
eu-LISA and Frontex joint conference

Content

Keynote Addresses



Krum Garkov,
Executive Director of eu-LISA

Mr Garkov started his address by welcoming all participants and guests to the conference. He stated how proud he was to witness the increasing levels of participation at each consecutive event – it is an indicator that the topics chosen for discussion are timely and of relevance to a broad range of participants, he suggested. This year, the conference was organised in cooperation with Frontex and under the auspices of the Austrian Presidency of the Council of the European Union. Mr Garkov stressed his belief that this is a powerful demonstration of what the joint efforts of the institutions and Member States can achieve to address challenges that the EU faces. He went on to thank all of those whose tireless efforts and work contributed to the organisation of the conference.

He continued by stating that the free movement of people has become a tangible symbol of European integration. This conference is a symbol of the best that we can achieve together, but it is also a reminder of why we cannot risk splitting apart. Today, European unity is being strained. People are going through a very difficult time, facing the threats of terrorism and organised crime and dealing with the continuous migratory pressure on Europe. He added that a recent Eurobarometer survey showed that almost each respondent in one way or another was concerned about the security of their country and migratory issues. As an EU agency, eu-LISA has since its conception played an important role in working towards developing timely and adequate responses to those challenges. The Agency has become a key contributor to the successful implementation

of policies in the areas of internal security, border management and migration management. Mr Garkov added that this contribution is growing from year to year. He went on to say that today there are some who believe that Europe is not doing enough – they want a more integrated Europe, with more solidarity between nations. At the same time, some believe that the EU is doing too much, and their answer is to renationalise these policy areas. However, he suggested that in the past few years we have seen examples of present threats and how they cannot be answered by a single nation. Therefore, he put forward the argument that the answer is not to unwind integration or to hold an unattainable vision of what integration should be.

In his opinion, the answer is to complete our union in the areas where it can and should be completed; to succeed, ambition and pragmatism is needed. In the years to come, Europe will face dual challenges – on the one hand, it will want to be open, as it is a part of a globalised world. More and more people are coming to Europe for work, study, business, and to seek protection in the aftermath of instability. On the other hand, citizens expect adequate levels of security and the upholding of the highest values upon which Europe has been built.

Mr Garkov went on to explain that due to the rapid development of technology, Europe has seen many new opportunities for economic growth and improvements in the everyday lives of its citizens. At the same time, this has created new threats – cybercrime cases increase each year, terrorism remains a threat, and cross-border organised crime continues to adopt new and different shapes. He opined that an essential element of an adequate response to these challenges can be summed up with the key words of skills and technologies – equipping law enforcement, border guards and migration officers with the right skills and sufficient technology prepares us for the challenges of tomorrow. Mr Garkov added that today we see a transformation of the justice and home affairs domain, leading to a very rapid convergence in internal security, border management and migration management from operational and policy points of view. At the same time, the ongoing digital revolution will accelerate in the coming years. Therefore, he argued, the EU should continue to explore the capabilities of technologies to make border management, internal security and immigration management stronger and smarter.

Mr Garkov sees three pillars that are necessary for reaching that goal – first, promoting and supporting technological innovation; second, developing cooperation between EU agencies, Member States and the private sector; third, reinforcing the common legal framework. All of these were issues to be discussed at the conference, he noted, explaining that the conference would focus on external borders and how to make

their management more efficient and smarter by both using technologies and redesigning business processes. He added that the conference would now be part of the movement of conversation from the vision stage to discussions on more practical implementation – initiatives such as EES, ETIAS, and interoperability. He reassured the listeners that although all this might sound excessively technological or even technocratic, what is at the heart of the discussion are people. This was the case because the main concern is how to meet the expectations of the EU citizens who are concerned about threats, security and migration and expect us to deliver on shared values. He concluded by stating that eu-LISA will do its part to assure the smooth functioning of the Schengen area and in addressing present and future challenges in internal security, border management and migration. His final message to the participants was to think big – after all, who has ever heard of Alexander the Average?, he joked. He urged the participants to use the opportunity to share experiences and ideas because it is the best way to address present challenges and to prepare for future ones.

Fabrice Leggeri,
Executive Director of Frontex

Mr Leggeri began by greeting the distinguished guests and colleagues and welcoming everyone to the conference. He went on to note that Frontex was delighted to have worked with eu-LISA to bring together such a highly specialised and diverse group of specialists, who represented not only a wide variety of countries, but also industries and the research community. Mr Leggeri continued by outlining the challenges – there are 600 million legitimate crossings of the EU's external borders per year, and their number is growing. According to Mr Leggeri, by 2025 the number of border crossings is expected to grow to 887 million, with a third of those being undertaken by non-EU nationals. In this reality, he said, it is more and more difficult to rely on traditional means of border control. Surveys show that public concerns about the security of external borders are growing. Mr. Leggeri noted that Frontex vulnerability assessments provide high quality information about gaps in border security among Member States. He went on to explain that these assessments provide support in identifying and eliminating weaknesses in Member State capabilities to face threats and challenges. He called on those gathered to ask a critical question: how is it possible to facilitate travel while improving the detection and identification of persons who might be a threat? For Frontex, he said, the answer is clear: new staff and technology are needed. According to the Frontex vulnerability assessments, there is a shortage of border guards for effective control at the EU's external borders. The likely increase in the coming years will help to improve the situation, nevertheless. According to Mr Leggeri, Frontex already supports the border control work with relevant and up to date information. At the same time, he suggested, training capabilities must be further developed so that the deployed officers have the necessary capabilities to do their

job. There is much left to do to make sure that there are sufficient guards at all sections of the external border and that they have the tools they need.

Mr Leggeri then turned to technology, stating that in order to address the challenges, it is imperative to harness the power of transformation that innovative new technologies can offer. One example that demonstrates this is the EES, he noted, which will register the crossings of non-EU nationals across external borders and automatically calculate their authorised stay. It will greatly improve the quality of border checks, allow for systematic identification of overstayers and strengthen internal security and the fight against terrorism by allowing law enforcement access to travel history records. However, improving the quality of checks might not improve the quality of travel or the work of border guards. The impact of the EES on guards is another major challenge, said Mr Leggeri, before outlining three new tasks for guards associated with the new system – first, adaptation to the new processes that the border guards will have to implement; second, dealing with the registration of biometric data – face and fingerprints and the impact on travellers at borders; and third, reconfiguring sometimes outdated infrastructure to incorporate new technologies such as self-service kiosks and e-gates. With these challenges in mind, he noted that Frontex had recently organised a workshop on the harmonised implementation and operationalisation of the EES with the participation of 23 Member States, 3 Schengen-associated countries, the European Commission, eu-LISA, and the new EU-funded project Protect. Mr Leggeri added that together with eu-LISA and CEPOL, Frontex is currently working on aligned and coordinated training of the relevant communities. Of course, the EES is not the only area where technologies play a predominant role, he noted. Frontex and eu-LISA, together with Europol, the European Commission and European Member States, have also started working on establishing ETIAS, which is due to become operational in 2021. Member States currently have little information about visa exempt travellers, he stated. ETIAS will help to fill this gap by providing for pre-travel screening. He reminded that Frontex is tasked with establishing and running the ETIAS central unit, giving the Agency a central role in the operationalisation of the system. Mr Leggeri explained that in addition to providing information about ETIAS to the general public and running a help desk for consultation, the central unit will have to review specific travel authorisation applications and match the information to that in databases. The unit, he noted, will also define, implement and evaluate the risk indicators used in screening ETIAS applicants. He added that this work will be crucial when considering the impact of the system on privacy, data protection and fundamental rights in general and, as a result, adjustment of indicators may sometimes be needed. A final area he mentioned in the context of advancing digitalisation was return, the repatriation of irregular migrants, overstayers, or failed asylum seekers to non-EU countries of origin. In cooperation with Member States, Frontex has developed a model return case management system, the so-called Recamas, to address the challenges associated with the current myriad of individual return systems. Mr Leggeri went on to outline a number of the system's benefits: more comprehensive and efficient return

case management, the harmonisation of individual systems, the application of common EU standards in case management, and the improvement of data quality. Last, but not least, he mentioned that the Recamas system leads to swifter and more accurate statistical reporting, enabling policymakers at national and EU levels to formulate more targeted programmes and strategies for return.

Mr Leggeri concluded by noting that although we speak about individual systems, these systems must also be able to speak to each other – this is the essence of interoperability. Frontex believes that interoperability has a key role to play in ensuring that border guards, migration officials and police officers have the necessary means for reliable identification and screening. Interoperability, according to Mr Leggeri, will also help fill insecurity gaps. At a more analytical level, Frontex is counting on eu-LISA to develop a tool that would provide all the relevant EU agencies with the necessary statistics and metadata to refine research and analysis. For example, it is necessary to assess how many people from one particular country have overstayed or moved from one country to another, which will allow for better identifying trends. This, in turn, will also provide a strong evidence base that will allow for better risk assessment. Also, policymakers will have better information to shape future immigration policy.

Mr Leggeri closed his statement by saying that the stakes are high and the pressure is growing on us all to become smarter through technology. He confirmed the firm commitment of Frontex to work with partners in order to identify challenges and find rapid solutions to protect those in the EU and those traveling within it. The time for information driven border management is not tomorrow, it is today, he concluded.

Olivier Onidi,
Deputy Director-General, Directorate-General for Migration and Home Affairs, European Commission

Mr Onidi started by praising the organisers and previous speakers for setting the scene very well. He continued by noting that one cross-cutting issue of great importance at present in Europe is the strong expectations to professionalise and further Europeanise border management. Over the last few years, he noted, there have been rather dramatic developments – co-definition of obligations at the borders, professionalization of the actual work performed at the borders and introduction of systematic checks. However, there have also been immense efforts to pool resources – people, staff, equipment, but also new solutions and systems. In this vein, Mr Onidi explained, the technological dimension of borders is very important.

One area, where we have a large source of untapped resources is better applying and conceiving our technological needs. He commended Mr Garkov and Mr Leggeri for having grasped that subject and for showing how important it is to bring it forward. IT systems are a part of general technological solutions, he noted, pointing out that there have been large and significant developments in this regard in recent years. In particular, Europe has embarked on the development of new systems that were hitherto missing – the EES and ETIAS. At the same time, he noted, existing systems have also been updated and significantly modernised – systems such as SIS, ECRIS, EURODAC, and soon VIS.

Of course, he admitted, it is nice to have wonderful systems, but in the past the systems were defined in a somewhat siloed way, which has led to issues presenting as we move forward. Thus, work has been ongoing, he noted, led by Mr Rob Rozenburg, on fundamentally reviewing the architecture of information systems in the EU to make sure that available information is used and additional new systems aren't created in vain, to develop modern tools for detecting multiple identities and for making the best use of biometrics, etc. Mr Onidi suggested that all of this would be discussed, adding that a lot is also expected from the participants of the conference in terms of better appreciating the consequences of rolling out the systems. The conference was a perfect forum, he suggested, for discussing the implementation that will entail quite a lot of consequences for all stakeholders. He added that the industry will also be impacted because they are the ones who will have to deliver on time what is specified at the EU level.

Another set of questions he pointed out revolved around how to make better use of what we have today. He gave the example of EU PNR, noting that the deadline for implementation of the Directive by MS passed in May. How can the community now make the best of the information that comes from it?, he wondered.

Mr Onidi also requested consideration of whether

data analytics could play a role in the future. Could it, he asked, be applied so that one could do even better to make the data more illustrative for border guards and increasingly for police and law enforcement. He called on the audience to devote some of the discussion to this area.

He added that there is tremendous work being done on artificial intelligence in the EU and looking at how to use, combine and spread data is an area where there is a lot of potential. First, when considering the movement of people, he noted that if we look at vetting persons who come to the EU or screening their application profiles, machine intelligence has potential. He suggested that another important trend is mobility. Here, Mr Leggeri had looked at how to equip border guards with more modern mobile devices, he recalled. An extensive programme of action is needed, he suggested, and it should be devised together to identify how to help those who are mobile at the borders. Finally, Mr Onidi talked about the area of virtual border checks. He noted that Mr Garkov and Mr Leggeri clearly stated that with enhanced professionalisation at the borders, we have to be careful about passenger comfort at the border.

Of course, there are hopes that Europe will continue to be an attractive destination; thus security and comfort are of utmost importance for those at the gates as well as those crossing the borders. He added that the technology to make that happen is being developed and it should be used so that border checks are dematerialised.

He ended by looking forward to the ensuing discussions, considering that the conference provided the perfect setting for such debates. He also expressed his happiness that this conference was a joint effort of the Agencies. eu-LISA now has additional research capabilities and responsibilities and is equipped to develop and run systems, he noted; we have the European Border and Coast Guard Agency, which is better equipped not only to define needs and help to develop and deploy solutions. There is, of course, also Europol, a hub of information and analytics that can be a 'back office', making sure that whatever information is needed is available at the border. In conclusion, he thanked everyone for recognising the importance of technology in this area and expressed interest in following the discussions to come on the day as well as at the industry day planned for the following day.

Mike Fandler,
Head of Unit IV/2, Austrian Federal Ministry of Interior

Mr Fandler started by expressing his honour at addressing the conference as a member of the eu-LISA Management Board, as a representative of the current Austrian Presidency, and as the representative from the Ministry of Internal Affairs responsible for implementing technology in Austria. Recalling the main topic of the conference, making borders smarter, Mr Fandler expressed a desire to first talk about how things started before steering the discussion towards the future. He went on to explain that in normal life, he is the head of ICT department at the Ministry of the Interior, and shared a story. In 2015, he learned a lot through sitting with a team of experts in a container at the border for 8 hours, trying to get a realistic view of the situation and learn how to cope with 5000 people pushing into the territory. At that point, the technological solutions and implementation had to be quick. The team developed a successful logistical solution to cope with the mass of people at the borders and to structure the process, he noted. They had everything ready – there was a quick registration possibility, a supported logistics process, even a mobile application, and very nice features. Yet, the team's masterpiece solution was never used. Mr Fandler then admitted that the experience was a hard lesson in how good solutions cannot only be national; on the contrary, they have to be European. Mr Fandler described the next 'scene', when he was attending the meeting of the Commission's High Level Expert Group on Information Systems and Interoperability in 2016; at the time, he noted, he was not convinced that this initiative to improve existing systems and build up new systems such as the EES and ETIAS would become a reality in due time. It sounded too futuristic, maybe too smart, he suggested, yet now work on these systems and on interoperability is going strong. According to Mr Fandler, what he learned from these experiences is that we need joint action, good cooperation of all stakeholders and a common understanding.

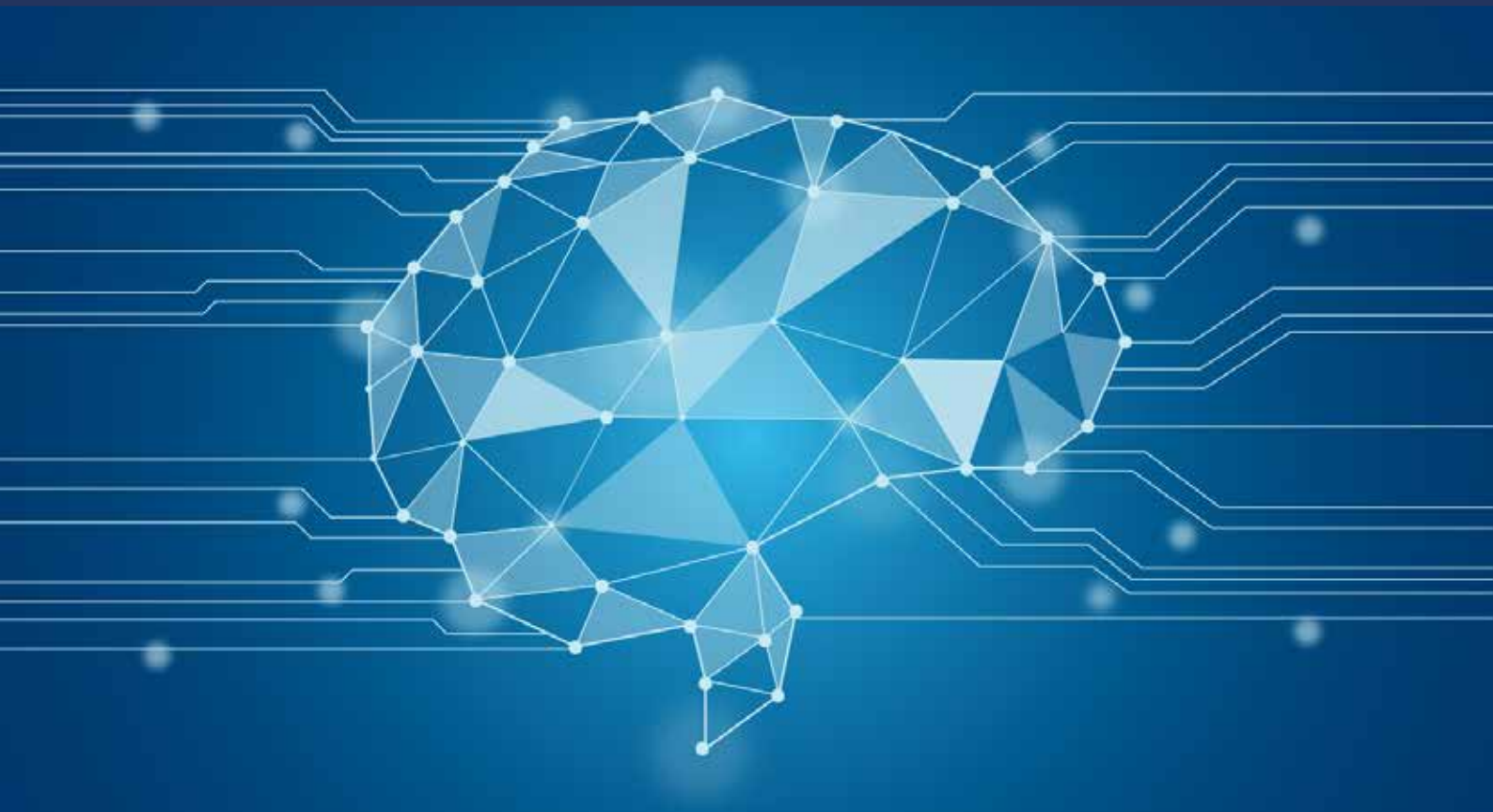
He then elaborated on the current priorities of the Austrian EU Presidency, which are derived from the mentioned situation and the addressed initiatives. The basis for the priorities is the following: we are facing mid-term challenges in asylum policy in the form of extremism, and the political situation in the EU is a challenging one. Thus, the Austrian Presidency sees the need for a proactive and comprehensive security policy, which means designing security, preventing threats and responding to threats. The vision is a citizen-focussed, crisis resistant, and future-oriented security union, he indicated. This also means addressing 5 key challenges and 4 cross-cutting issues that he enumerated. The challenges are: strengthening the EU's external border protection; developing a crisis-resistant EU asylum system; removing the breeding ground for extremism and terrorism; strengthening European police cooperation; and safeguarding digital security. The cross-cutting issues are: promoting and protecting our European values; fostering integrity in the EU Member States; strengthening cooperation, also with third countries; and strengthening cooperation with respect to internal and external security.

Mr Fandler then asked, speaking from the Ministry's point of view, what is the impact of interoperability on the national level? It is not only about comprehensive technical implementation with massive effects on national systems, but it also leads to legal and organisational challenges and has high impacts on the border control process, he argued. For the end users, he added, talking about national workflows, the processes must be very clear and easy to understand. The end-user must be able to make decisions in real time based on high quality information. For Mr Fandler, interoperability is all about having the right information at the right time and in the right place; the information has to be unique, secure, reliable and trustworthy. So he concluded that we need information driven and integrated border management, which, he noted, was to be discussed in the following panel.

Session 1:
Future of information driven integrated border management

Moderator:
Mike Fandler,
Head of Unit IV/2, Austrian Federal Ministry of Interior

Panellists:
Theofanis Syrigos, Chairperson of the Entry/Exit System Advisory Group, Customer Relationship Officer, eu-LISA
Richard Ares Baumgartner, Senior Strategic Advisor, Frontex
Luis de Eusebio Ramos, Deputy Executive Director of Europol, Capabilities Directorate
Marc-André Daigle, Director, Strategic Initiatives and GCMS Coordination, Immigration, Refugees and Citizenship Canada / Government of Canada



Mr Ramos began by explaining what kind of information is needed for integrated border management (IBM). He indicated that Europol puts the police officer, the analyst and the investigator at the centre of any IT development because the officers on the ground have to make immediate decisions. He continued by differentiating between types of information. From the front office, information has to be highly appropriate and easy to access via a user interface. In the back office, the work is more complicated, since this is where the interoperability package is applied – this is where AI can facilitate the work, he suggested. The police officers need, first and foremost, an accessible interface with actionable information, and in the background gaps have to be filled to make sure that actions are based on solid informational ground.

Mr Baumgartner continued with his view on the question of what information we need for IBM. He suggested that the answer is related very much to the decisions that have to be taken, as that defines the need for information and legitimates access. He then went on to enumerate the most important decisions from the point of view of border guards.

First, at the crossing, he explained, there are around 600 million crossings at external borders of the EU each year. Each individual crossing means a decision for a guard – not only about whether to let a person in or out, but also to know whom to refer to the second line. That means deciding who needs to be interviewed by a competent authority, who is a vulnerable person and needs to go through the asylum procedure, who needs care by an NGO, etc. Mr Baumgartner elaborated that integrated border management (IBM) is not only about border checks – it is also what has to be done before the border crossing to protect the Schengen area. This is where the Schengen visa applications are very important, he suggested, with 15 million applications submitted last year.

However, there are also the ETIAS applications to come too. He added that besides activities before and during the crossing, IBM also means the process after crossing – immigration management. Here he referred to the important events that trigger the decision for the border guards: the illegal border crossings, which last year were at 207,000 (down from more than a million in 2015), asylum applications (707,000), and detected irregular stays (435,000). These figures are registered and available through eu-LISA reports on EURODAC, he noted. Then there are also residence permits, long stay visas and residence cards, which based on the impact assessments prepared for the extension of the VIS amount to around 22 million applications last year. Lastly, there are return decisions, which will now be systematically included in the SIS, according to the new proposed regulation, he noted.

Having looked at what kinds of decisions need to be made, Mr Baumgartner continued by elaborating what kind of information is needed for those decisions. He explained that an officer has to consider several factors: first, the main element of information is the individual, about whom the officer needs to make a decision. So despite the technological solutions, that human contact remains the most critical element for making a decision. The second element, of course, is the travel document – the passport. The third element is the databases: besides the national databases, we may currently consider SIS II (which has now been equipped with AFIS capability), Interpol databases, e.g. the SLTD (stolen or lost travel documents database) and the VIS. Mr Baumgartner then went on to consider what the future will hold and, particularly, what this future will mean for border guard officers. First, he noted, it will introduce the obligation of enrolment at the external borders. Second, there will be new databases and information at the disposal of the border officer. However, one should also consider the new use of risk indicators, he suggested. Mr Baumgartner indicated his view that we are heading towards more risk-based border systems.

The ETIAS screening rules are one of the examples, yet similar indicators are also considered in the VIS proposal.

In conclusion, he said that we will have new information and more reliable systems that, although they do not necessarily provide for more data, enable making better decisions. The environment is getting more complex, nevertheless, which requires reinforcement of the consultation procedures.

Mr Syrigos took the floor next and began by explaining how to bring information to the people working with it to allow for better decisions. He argued that it is evident that the existing systems have already revolutionised decision making and added value, not only in the case of SIS but also VIS. It is clearly visible that since the introduction of the latter, rates of refusal of visas have increased because the officers have the tools to view the decision history and make better decisions. Mr Syrigos explained that now there is a need to go beyond – what is needed is better quality information and linked information, while the appropriate competent authorities have to have access to take proper decisions. This leads to better decision-making, better security, and more accuracy. As experience has now been accumulated, better decisions can be made, we can add quality and make systems talk to each other in a better way than before. Also, authorities and private stakeholders, such as carriers, can have a better view on the spot to take the steps that they need.

Mr Daigle spoke about the Canadian experiences of relevance to the discussion. He began by giving some context – Canada and the US came to an agreement in 2011 for managing integrated borders and securing the perimeter in an integrated manner. Based on this agreement, several initiatives were established, including the Electronic Travel Authorisation system eTA that launched in 2015 and an Entry-Exit system that will be launched in 2019. He noted that it has been interesting to see similar key considerations discussed here in Europe – considerations such as increased traveller numbers, the risk management approach, the use of technology and the requirement to ensure more accurate data for border officers. One of the major concepts for the Canada/US border context was intercepting pre-arrival, he explained. Via the eTA system, there is a pre-screening process

for passengers before travelling to Canada, he noted, so that the authorities have a better idea of possible threats in advance. The entry-exit system, he mentioned, will look at the whole continuum and monitor whether people have come, gone and/or overstayed their visa terms; it also includes information about the permanent residence status holders, he noted. The Canadian entry-exit system also leverages advanced exit information from the air carriers, which allows for creating better exit records.

Canada is also concerned about the service that it provides to people, he explained. The reality in this regard is very much managing expectations across the board, he suggested. Travellers and applicants expect technology to make travel seamless, he argued. Officers, meanwhile, expect readily available and reliable information. The American counterparts also expect integrity in the systems and decision making. The border management agency expects that information collected pre-arrival is fully integrated into all systems. Finally, the airlines also share responsibility, so that relationship has been a big learning experience.

Mr Ramos talked about how information is practically shared, explaining Europol's collaborative approach to IBM. He explained that the first step was to design a new integrated management system within the organisation, just like the process taking place at the pan-European level currently. While previously the information was in silos, Europol's new legal framework has allowed for that information to be integrated so that the dots between different grey areas could be connected. In the future, for example, when an

ETIAS application comes in, Europol wants to make sure that the response is based on a solid ground of information.

Mr Ramos then talked about completely rebuilding information infrastructure and filling the gaps. In terms of incoming information, he listed the Passenger Information Units (PIUs), Financial Information Units (FIUs), ETIAS and external experts as sources of information that has to be fully integrated in Europol, so that they could in turn give a full set of information to the guards at the border in a timely manner.

Mr Ramos then went on to elaborate on five ways in which Europol can contribute to the concept of IBM. First, Europol is fully on board with the Commission plans for interoperability of EU information systems for security, border, and migration management. They have full integration with SIS and have almost implemented a connection with VIS. Europol also wants to be a partner for the EES, PNR and ETIAS systems. The second line of work in which they can provide value is through their SIENA infrastructure. The new version is based on microservices, which will allow the design and building of new services based on the microblocks in a matter of days. In fact, these microservices could be shared with external stakeholders, for example, eu-LISA, he suggested. Third, Europol is developing new search and cross-checking capabilities, he noted -starting next year, Europol will offer Member States the possibility to search all information available in the Europol system through the QUEST service, which can be integrated into national case management systems. Furthermore, they are also going to facilitate searches on decentralised databases through the ADEP project. The concept is that one Member State can search for information from another Member State through Europol. The fourth topic that Mr Ramos elaborated on was redesigning Europol's analytical capabilities. The fifth and final one he mentioned was development of innovation-driven capabilities, meaning use of AI. Europol has already developed some services based on open-source technology in AI, he noted, for example, for facial recognition and natural language processing with pretty good results.

Mr Syrigos was asked by Mr Fandler about the EES and interoperability – how do you do it?, he wondered. Mr Syrigos began by indicating that it is a question that he faces every month at the meetings with Member States. He suggested that eu-LISA is well prepared for development of EES and interoperability based on experiences with VIS and other systems in place – they have to involve stakeholders and end-users, Mr Syrigos explained, cooperating, analysing and anticipating. When considering existing systems, he explained that they provide reports on data quality and enable business analysis, so that eu-LISA can bring important and actionable information back to the stakeholders to explain what has to be done to improve them. All those experiences are also used in the design of new systems. In terms of cooperation, Mr Syrigos elaborated that it is especially intense with Frontex and the European Commission; it includes organisation of extensive expert workshops about complex issues such as interoperability.

He explained that eu-LISA involves Frontex in questions about performance, for example, exchanging knowledge on when officers need something fast and efficient to do their job – one typified by eu-LISA's development of specifications for the EES work-flow engine in collaboration with MS and Frontex. The aim is to see how to parallelise services and give fast and accurate results directly to the front line, especially where there is a lot of pressure on the officer and there are long queues. According to Mr Syrigos, eu-LISA also reports to the institutions on what they observe and to the Advisory Groups, providing for better advice on designing the EES, ETIAS, interoperability, and so on.

Mr Fandler then asked the panel about money – a lot is being spent for these activities, however, for what purpose?

Mr Syrigos replied by referencing back to challenges mentioned by the keynote speakers. There are currently unprecedented developments at EU external borders due to instability in third countries, financial and humanitarian crises, he reminded. All this has brought the citizens themselves the task of tackling this issue. Mr Syrigos stated succinctly that we do spend, however, it is an investment in the future and in our children, in security. That means also investing in the third country nationals, who visit and want to feel secure here. We invest not only in security but in confidence, which means growth, stability and a better future, he argued.

Mr Baumgartner talked about why we need the investments, first confirming his support for the previous answer by his colleague from eu-LISA. He added that the initiatives underway at external borders are critical for the integrity of the Schengen area. A big budget is needed for developing these systems, he agreed; however, even in the midst of the immigration crisis in 2015, a study was carried out that found that the spending would be much higher if we didn't have Schengen. Another element he added was that having quality information at the border also means having quality decisions made. Mr Baumgartner supplemented his earlier intervention by adding that provision of actionable information plays an important role. Mr Baumgartner stated that Frontex can contribute by developing operational practices, best standards, training tools, etc., to help and control the roll-out of the information systems. The Frontex context is also highly suitable for testing solutions before implementing them in a larger context, he suggested. His last point was about cooperation – he feels that ETIAS is a wonderful initiative, because it will bring the agencies closer. At the national level, given their roles and activities, institutions will also have to cooperate better, so the whole undertaking is a great example of how to push for more cooperation at the EU level.

Mr Daigle spoke about cooperation, seeking to give some thoughts and advice. In the last few years, Canada has invested a lot into realigning and replacing legacy systems throughout the immigration system, he noted. A lot of the work

was in mapping information exchange and interoperability, and in this regard he stressed the importance of data integrity. However, he also stressed that investment in addition to money also requires an investment in time, so that a full data analysis is carried out. Over recent years, they also developed many information sharing agreements with foreign countries; in such initiatives, definitions and understandings of concepts need to be harmonised for everything to work well.

Mr Ramos elaborated that cooperation is key in these kinds of projects because all stakeholders should be on the same track to avoid overlapping and to fill the information gaps. This has to be done at the national level as well as the inter-agency level, he noted. He also argued that we have to look at how we are handling information for every single country so that there could be a unique response for officers in that state. Finally, more academia and private sector participants should be brought on board, he argued, as a lot of innovation comes from these instances.

Mr Fandler asked the last question of the panel wondering whether, with regard to the future of information driven border management, the future has already begun or are we still waiting for it to begin?

Mr Syrigos opined that the future has already begun. For some time now, a lot of effort has been made to prepare for and build this future, to anticipate and design systems. He added that the governance is in place, there have been extensive exercises with experts to address complex matters to anticipate and minimise risks, and therefore, we know what we have to deal with and that the new systems should close the remaining information gaps. Thus, the future is already here and we are already building it.

Mr Ramos replied that it is not about tomorrow but today. The proposal from the European Commission on interoperability is a reality. He referred back to Mr Onidi, who stressed that the discussion phase is over and now that we have a clear vision of where to go, we must look towards implementation. The community needs to work on realities and delivery of the new systems, he stressed. He feels that in the day-by-day work, we are making it happen.

Mr Daigle agreed with the previous answers, arguing that the future is here. In terms of design thinking, he pointed towards data modelling, the

use of AI and data analytics as part of a general digital transformation. He asked, nevertheless, whether we are there from a cultural perspective, to fully use such possibilities He suggested that he is not quite sure of the answer to this question, yet felt that at least the appreciation is there and efforts are being made. With this in mind, he expressed his anticipation of next year's conference to hear about developments.

Mr Baumgartner suggested that the communication from the European Commission on new information systems for borders and security was a tipping point because we started looking more at user-centric systems. At that point, there were a lot of different systems, which had been shaped according to their respective policy environments in a manner that is completely at odds with IBM. He referred back to the border continuum discussed earlier – the same person who applies for a visa will cross a border, he could apply for asylum, for a residence permit, become an irregular migrant or just go back. With interoperability, we are getting different layers of information about a person and gradually the capacity to make the right decisions is increasing. That is a clear sign of what could be the future, he concluded.

Mr Fandler thanked the panellists for being so well prepared with material to support their messages. He said that he feels 'safe' between these institutions, because everyone is working together for a better and safer Europe.

Mr Garkov challenged the panel by stating that we will have a critical mass of information systems and data, but not necessary information, and thus wondered how to turn the data into information that will fuel future IBM?

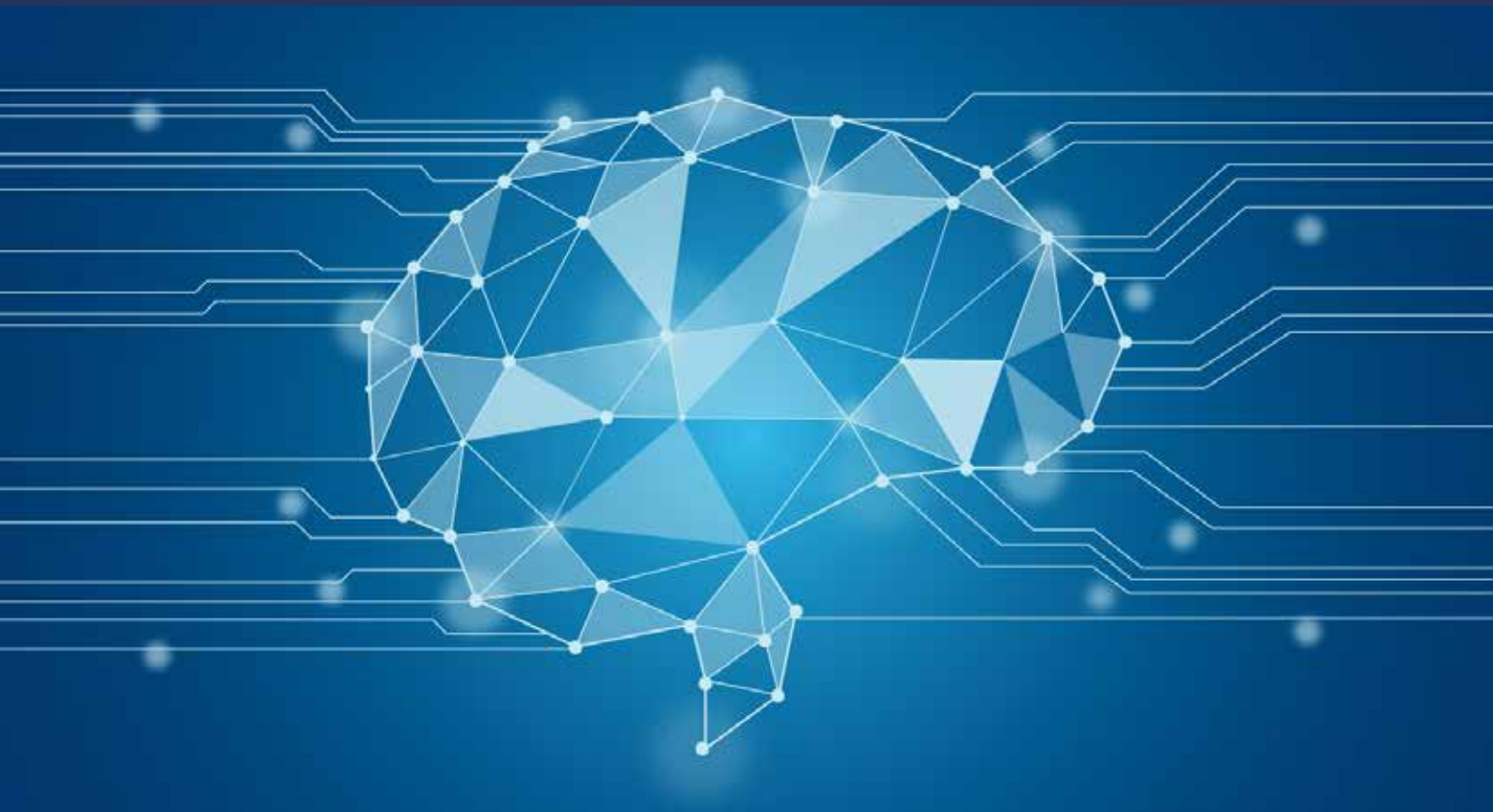
Mr Ramos answered that there is indeed a huge amount of incoming information from a lot of different sources and in different formats – scans, internet information, video, audio, etc. Developing capabilities to properly manage the data is a key issue, he agreed. The key is the person handling the information and the crux of the community's approach has to focus on ensuring that that they are always capable of making the right decisions. He added that we can offer them systems and elaborate on the data within such systems, as well as focussing the tool towards the person using the system. Thus, perhaps we might get accurate decisions with 80% confidence, he suggested; to succeed better beyond that, we additionally need to focus on the human skills, which are also crucial.


FRONTEX
LISA
FRONTEX

Session 2:
Integrating technology into external border management – View of the end-users

Moderator:
Javier Quesada,
Head of Research and Innovation Unit, Frontex

Panellists:
Nicolas Goniak, Advisor, European and International Affairs, French Ministry of Interior
Fares Rahmun, Project Management and Software Development,
Federal Office of Administration (BVA), Germany
Pasi Nokelainen, System Manager for Border Checks, Finnish Border Guard Headquarters
Pedro Figueira, IT expert, Foreigners and Borders Service, Portugal



Mr Quesada began by giving a brief introduction to all panellists before enquiring as to what each would like to present and discuss in the opening part of the panel.

Mr Goniak was first to answer and said that the main focus is not so much on IT solutions but rather physical borders – the western border to Normandy, especially in the context of Brexit.

Mr Rahmun noted that we know relatively little about ETIAS and that his focus will be on what needs to happen on the central, but also Member State level with regard to ETIAS in the coming years.

Mr Figueira said he would revisit the main challenges relating to the Entry-Exit system as well as bring specific examples from Portuguese sea borders.

Mr Nokelainen stated that his talk would mostly focus on the processes for the definition of the systems as well as the legal basis.

Mr Goniak began by describing the border between the UK and mainland Europe and how it will be affected by Brexit. The border between the UK and France is rarely spoken of, he noted, because the entire system is designed to facilitate a swift and seamless flow of passengers, goods and vehicles. He elaborated that due to the customs union there are no systematic checks on goods at this border crossing. To ensure this, there are bi- and trilateral agreements in place between France, the United Kingdom and Belgium. Mr Goniak further exemplified this by highlighting that when travelling from Calais to Dover, passport checks are performed only once in the country of departure.

There are 15 BCPs across the channel through which 35 million travellers cross the border every year – approximately one third travel through the Channel tunnel using personal vehicles, one third via Eurostar and one third on ferries. Mr Goniak

added that though this traffic is seasonal, it is also very dense. It is not uncommon to see up to 20,000 cars and 10,000 lorries crossing in each direction per day. He put the numbers in perspective: the Schengen border between the UK and France sees more than 35 million travellers a year, while the border between Finland and Russia sees 9.2 million annual crossings and the border between Poland and Belarus/Ukraine 8.9 million.

Mr Goniak further referenced another aspect of the France-UK border that gets a lot of coverage in media, particularly around Calais. Some 20km of the border must be checked for illegal activity as there are a lot of people that want to illegally cross the channel on board trucks, lorries, etc. He added that it is not only a question of migration and IT systems but it is to a great degree about public security. Elaborating, he noted that according to Frontex figures from 2017, France has the 5th highest number of people travelling to conflict zones globally and the real danger lies in these people returning. These travellers return by land, air and sea and they have to be spotted by any means necessary, he argued. In order to do so, you need access to information systems that the United Kingdom may lose access to after leaving the European Union. Mr Goniak suggested that this puts much more pressure on the French authorities.

He continued by explaining that on the cross channel route there are 3 formats of check: checks on trains for foot-passengers, checks on vehicles (trucks and personal vehicles travelling via the channel tunnel), and checks at 15 sea borders for ferries. Each of the border crossings presents different challenges. For example, for trains departing Gare du Nord there are 10 million annual travellers, but only a border area that's 15 meters wide. The problem is real-estate – there is simply no room in Paris for more booths or gates. Mr Goniak also added that third country nationals cannot go through e-gates currently. He added that luggage is also a problem in such tight spaces. In addition, there have been systematic checks on trains since 2017 but it is hard to accommodate frequent travellers to make their crossings easier because they have to concentrate on third country nationals. He noted that issues for land borders are quite similar and mostly have to do with space – for example, the capacity issue

to accommodate trucks in the parking lots at the border crossing points. He repeated that with the current migration pressure there are a lot of third country nationals trying to board lorries.

Mr Goniak continued by alluding to the fact that with EES, third country nationals will register their finger prints and facial image the first time they're entering the Schengen area. He elaborated that for travellers coming from Britain to mainland Europe that will mean registering in manual booths. This means these travellers – mostly from the United States, Canada and Arab countries – will spend approximately 2.5 times longer in border checks. On the other hand, once these TCNs have been registered they can go back through e-gates. The biggest problem presenting here, he suggested, is space. The ideal solution would be one kiosk that would encompass a number of systems requiring with the lowest amount of interaction – biometrics and passport scans only for multiple checks.

Finalising, he looked towards the future somewhat. Noting that Eurostar set up a pilot project in 2017 for iris checks for registered drivers, he suggested that such technological solutions along with RFID could replace the travel document inspection in the future – a valid replacement for traditional identification – legislation permitting, he suggested. He further shed light on the potential developments in case of a No-deal Brexit. In this case, British citizens become third country nationals with a visa requirement. For the French, it would mean going from 4 million issued visas to about 11 million.

In any case, he summarised by saying that after Brexit the number of TCNs crossing the French border will go up from 5% to 50%.

Mr Rahmun challenged our knowledge of ETIAS and whether we actually know anything. He conceded that what we do know about border management is that there are a lot of systems in place, such as VIS, API, PNR, EES and now ETIAS. What do we actually know about the European Travel Information and Authorisation System, however?, he pondered. What does it cost? The legislation only reveals so much, he suggested.

One area of ambiguity related to the introduction of risk indicators in the system, which he suggested will pose a huge challenge. He added that there will be a new ETIAS watchlist, but it still remains open how authorities will work with that.

There will be a new central Frontex unit that will look at all the potential hits the system's search function retrieves. In case the ETIAS central unit believes the hit to be valid, it gets forwarded to the national unit . Mr Rahmun indicated that he feels that this is where the regulation stops and hands over risk assessment and decision-making to the national units In this circumstance, if they refuse a travel authorisation they need to have bullet-proof reasoning. Referencing what we already know from the Visa procedure, Mr Rahmun suggested that there likely needs to be a national case management system that enables consultation of additional national authorities in case needed.

Mr Rahmun then came back to the Member State national units. He further explained how the work will likely be structured: the colleague may have to talk to the applicant, and in case of further questions maybe to talk to the Ministry of Foreign Affairs, to a consulate, to Frontex and the central unit, to Europol, to eu-LISA SIRENE officers, etc. Regarding risk indicators, communication may be needed with PIUs and API HQ and maybe to public health authorities, to the courts, carriers and the border authorities. While there will be some software solutions to handle some of this (article 6 describes some of the technology provided by eu-LISA), he suggested that the tasks at hand were nevertheless significant.

Mr Rahmun concluded by saying that the approach to setting up an ETIAS National Unit is still a blank piece of paper. There's still a lot of work to do and questions to answer. Perhaps the conclusions might be that nothing needs to be done, but the questions need to be discussed, he stated.

Mr Figueira started with a recap of the biggest opportunities and challenges of the EES, which, he suggested, is certainly a step forward mainly because it makes it mandatory to systematically check everything and to collect biometrics. While there are still drawbacks – inevitably the workflow at the borders will become more complex – he proposed that some change in processes and their adaptation to the EES requirements rather than simple addition of another layer to the processes already in place might address most of the challenges. He also suggested that it is necessary to consider how the border guard can process the increasing amounts of data being provided. Depending on the solutions provided, the decision making process could become either simpler or more complicated, he suggested. Which outcome prevails all depends on the business processes next to the technology, he added.

Mr Figueira added that one of cornerstones of the new system is also the motivation of the border guards – they're the main actors of the EES.

Mr Figueira stressed the importance of the new devices for the enrolment process and their testing in the field. He brought two examples from the Portuguese borders. In the last years, there are a lot of big cruise ships during the tourist season, he noted. A cruise ship with 3000 passengers can dock at 8 o'clock in the morning leaving the visitors only 8 hours to visit the city. Surely they wouldn't want to spend those 8 hours waiting in a queue for entering or exiting the BCP. How can the passengers be admitted in 40 minutes to an hour?, he wondered. Another big difference to air borders is that sea borders lack the infrastructure. There are fewer e-gates, less human resources fewer border guards and fewer computers. Possible solutions could be on board controls on the ship during the journey, but currently this seems to be technically challenging given the equipment available. Another possibility is to use kiosks on board. Also, secure mobile devices could be used that can collect the biometric data. He added that the most important facet of these devices is the fact that they can be used offline. A different example brought forward was the case of a small marina. Such a BCP has relatively little traffic so, if needed, officers get sent there as there isn't enough work to justify a permanent border crossing point. This poses the problem that there's no second line check system available. The EES regulations need to be met in both cases. Mr Figueira proposed that solution could be with slightly different mobile devices, also capable of working offline, but able to implement the complete workflow. This use demands a slightly more complex mobile application that would be able to facilitate information from all systems as well.

Mr Figueira concluded by offering his final thoughts for a successful implementation of the EES: strong involvement of border guards, which can only be assured if the system is easy to use and is always available; a user friendly single interface tailored to the user; that everything that can be automated will be automated, albeit not necessarily making automatic decisions; and functional and easy to use devices.

Mr Nokelainen started by taking a look into his personal history with integrating technology into external border management. He mentioned that he used to be a visa clerk in an era where every single visa application was processed manually. A while later the first laptops arrived and it posed a huge change because it took away the need to ask for information via intercom from the duty officer sitting at the only computer, he joked. He added that shortly thereafter, officers received proper control booths with desktop computers, MRZ document readers and even an integration to the system to enter and query data. Then came the first full page scanners with the ability to query all the databases in one go; advancements have been rapid and significant, he noted.

Mr Nokelainen suggested that the implementation from the outset was bottom-up. Even though the initiative to make changes came from the top, the selection of the devices and the designation of approaches to implementation was mostly handled by the border guards. He added that at the time the focus was to put tools into the hands of the officers.

He continued that in the past years there has been a shift in the EU processes, how systems and legislation is prepared and how processes move forward. He added that it is interesting that many challenges are being discussed after the legal base is ready, the technology is almost ready and the implementation is underway; maybe these questions should have been asked before?, he suggested. Has the process gotten smarter, are we getting smarter or are we getting greedier for information?, he wondered.

Discussion:

A representative of Augmentiq indicated his impression that Member States could do with extra support in building the technological capabilities. Where does that support come from?, he asked. Second, regarding the challenges at the English channel, he questioned whether it was the regulatory environment that was more a blocking factor than technology. The concern is that the technology is moving at a faster pace than the regulators, he suggested. Thus, how can we make sure that the regulators keep up?

Mr Goniak fielded the question first by reminiscing about a talk at an ABC working group in Warsaw with a colleague from the UK border authority. It sounds absurd to have ABC gates for both entry and exit in one trip, but the regulatory body hasn't caught up, he noted, meaning that such configurations are needed.

Mr Nokelainen said he doesn't feel that there are regulatory masterminds somewhere unknown – in fact many of those present at the conference are involved in regulatory processes, he noted. It is the agencies, the member states, the technical and legal people that are involved. He suggested that future alignment between technology and regulation boils down to how the cooperation and coordination works at the national as well as the EU level.

A representative of the European Boarder and Coast Guard Agency added his view to the reflection, mostly focusing on the roles of the

National and Central Unit. He also posed a question on whether ETIAS and PNR will belong to the same working environment? What are the views of the panellists about this issue and how could the system be implemented in a smart and coordinated way?, he asked.

Mr Rahmun answered by saying that these are all questions that need answers very soon, so the discussion about use cases must start now.

An audience member suggested that these details haven't been discussed before EES but this likely made sense in his view. The idea is to make the European component so strong that the national component can be much narrower. He also suggested that the key should be in experimentation, and in this regard the French and Portuguese colleagues have provided a great example in hinting at solutions and bringing along partners.

Mr Nokelainen answered by saying that the EES has been already in discussions for the last 10 years, with extensive feasibility studies.

Mr Figueira answered by saying that the Smart Borders pilot was conducted in 2015 and, therefore, we can't be sure if all the findings are still current. He elaborated by mentioning the example of Lisbon airport, where the traffic has increased by 15% each year; thus, maybe the findings are not anymore applicable once the EES enters into practice. He added that the problem is that the technology and reality keep moving while studies are ongoing. Germany is a good example, he suggested, as the pilots initiated there in 2015 continue while they have run exhaustive tests of the kiosks. It is important to stay as imaginative as possible within the legal framework and the focus must remain on the end user.

Mr Nokelainen responded by saying that the need is to be innovative rather than imaginative. The key is planning and seeing what can be done with existing technology, since there is no more time for further pilots before EES.

Mr Rahmun added that in his opinion the key phrase should be "Think big". Let eu-LISA and the other agencies take care of the big tasks, he proposed.

Mr Goniak summarised by saying there is no guidance for land and sea borders, because there is no one solution fits all approach. There is no uniform tender for mobile solutions, for example.

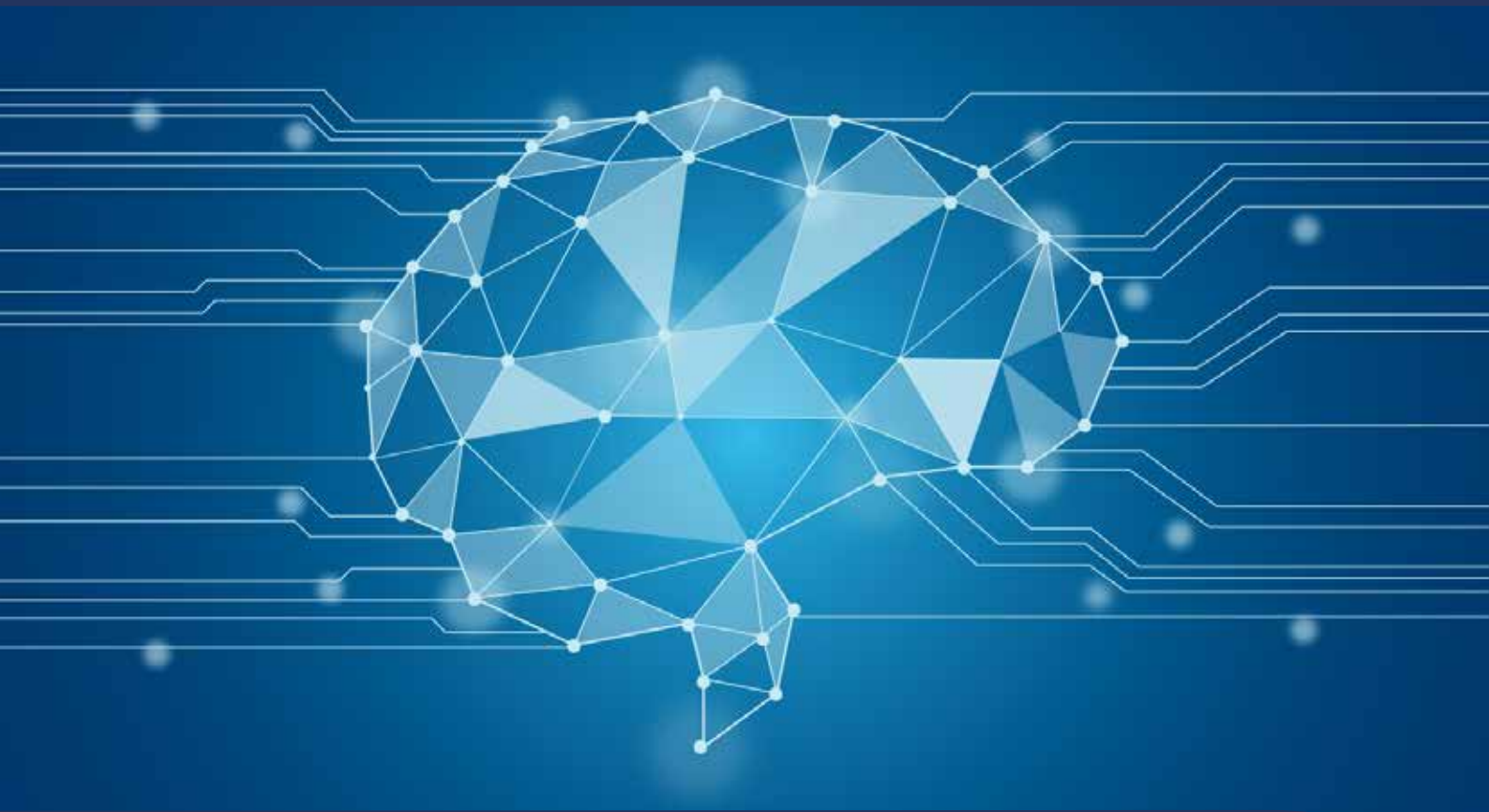
A final question was posed by **a former Head of the UK Border Force** who expressed his experience that the working relationship with the French colleagues has been very good. He wondered whether there are possible bilateral treaties to concluded with regards to registered traveller programmes.

Mr Goniak indicated this is a political discussion that needs to be had.

Session 3:
Interoperability – adding maximum value for the border management community

Moderator:
Mare Haab,
Head of the External and Internal Communication Sector, eu-LISA

Presentations:
- *Interoperability – state of play and upcoming challenges*
  Rob Rozenburg, Head of Information Systems for Borders and Security Unit, DG Migration and Home Affairs, European Commission
- *Interoperability and privacy rights implications*
  Owe Langfeldt, Acting Head of Prior Checks and Consultations, European Data Protection Supervisor (EDPS)
- *Implementing interoperability – a collaborative effort already underway*
  Ciarán Carolan, Head of the External Affairs and Capacity Building Sector, eu LISA



Ms Haab opened the panel by introducing herself and the panellists.

Mr Rozenburg began seeking to outline how interoperability will add value for the border management community. He presented his view with an illustrative slide. The border guard or other authorised official has the national interface in front of him or her, a single search interface, which will not change, he noted. This interface, he stated, has access to the national systems and the national SIS copy, which also won't change.

With interoperability, there will then be one single line to Strasbourg, to the European Search Portal (ESP), which will enable access and organise the querying of the relevant information from 6 systems (according to the legislative proposal). He explained that the ESP will be developed in a way that it has a connection to the existing systems (SIS, VIS, EURODAC), to the two systems that have been politically agreed (EES, ETIAS), and to ECRIS-TCN, on which agreement was anticipated in the subsequent month. All six systems, he noted, are run by eu-LISA. In addition, ESP will link to Europol data and Interpol systems. He indicated that it is important to underline that it will be configured in a way that the border guard will only see information to which he/she legally has access. In other words, queries will be based on user credentials and thus be both precise and tailor-made.

He went on to mention the shared biometric matching service, a back office service for the 5 systems that make use of biometrics (ETIAS does not have biometric data) and the Common Identity Repository (CIR) which will have information from all eu-LISA systems except SIS. The last elements described were the Multiple Identity Detector (MID) and the Central Repository for Reporting and Statistics (CRRS), which he noted was also sometimes referred to as the 'data warehouse'.

Mr Rozenburg continued by reflecting on how developments in interoperability might help the border guard on a daily basis. The ESP, he noted, will make queries speedier and easier, but more importantly, he suggested, the query will be done on a systematic basis. To elaborate, he noted that we know that the fingerprint verification against VIS that should be undertaken for people with visas is not done systematically in all Member States although it is a legal obligation. The check against SIS is also not done at all borders in every case as it should be, he suggested. According to the Schengen Borders Code, Interpol should be queried automatically, but it is not always happening, he noted. The ESP, he argued, leaves no room for personal choice, thereby ensuring that all information will be brought to the border guard quickly, making their work easier and faster. Also, it is politically important that the ESP will allow Member States to trust other Member States, he argued, through its assurance that everyone is running the same types of border checks. Speaking of mutual trust, this is a move towards full confidence, Mr Rozenburg opined. The MID provides further benefits, he suggested, in particular by helping to guard against identity fraud. He elaborated by noting that information on a discrepancy will be displayed even when border guards do not have access to one of the databases in question - so even though the border guard cannot check ECRIS-TCN, for example, they will still be made aware that something is wrong and have the opportunity to send the person to second line for further investigation.

He also enumerated further benefits – the provision of reliable information and statistics to inform risk assessment, for example, regarding which nationalities are responsible for the most overstays, etc., and the improved support provided by eu-LISA to Member States for maintenance and system update.

Mr Rozenburg then referred back to Mr Fandler, who had suggested that initially interoperability had sounded very futuristic and hard to attain; while much work is still needed, he noted, perhaps the real miracle that happened over the past year is that there is very strong political support in both the Council and the Parliament for this kind of architecture, he suggested. Trilogue negotiations, he explained, were set to start in the following week. The LIBE committee, which is responsible for this file in the EP, had voted on amendments earlier and concluded on a text that should be endorsed by the Plenary. While outstanding points remained – the Council wanted to have a closer look at the operational side and questions of business continuity side, while Parliament was noted to have continued concerns about data protection and the need for more safeguards and oversight mechanisms, he expressed a view that there would be agreement on the political level before the end of the year with the help of the Austrian Presidency and the rapporteurs in the Parliament.

Subsequently, there would be a need for work delegated acts to elaborate finer details before eu-LISA could start its development work, he noted.

His last point concerned the big challenge faced by the Member States. He emphasised that instead of having a siloed view and concentrating on the details, Member States should take a broad look and have national preparedness plans for the whole body of challenges to come. The first aspect he suggested that needs addressing is governance – in this line of work, he suggested that all stakeholders and relevant ministries, the IT community and practitioners need to be involved. Some Member States have inter-ministerial committees set up, others have national coordinators, who run the operation as a mega-project. He encouraged Member States to think about such matters already. The second important element he spoke about was finance and related points such as availability of office space and staff. This, he noted, requires support from the political leadership and the ministries of finance. The challenge, therefore, is to make sure that the support in the Member States exists so that all necessary work can be carried out. Mr Rozenburg also pointed out that planning is a very important element – timelines need to be prepared to see how the work looks also taking into account updating of national systems which are already in place. He suggested looking at infrastructure, and investments in technologies such as e-gates to see how everything could be aligned into one big operation. Finally, he called on Member States to think about the issue of training, which also might seem like something that could be postponed but in reality needs attention already. He argued that the hundreds of thousands of people who will work with these systems should already be kept updated on what will change and how so that it will not be left to the final moment. Mr Rozenburg finally mentioned the operational handbooks to be developed by the Commission, noting that there is some consideration to integrate everything related to future developments into just one handbook to facilitate user operations.

Mr Langfeldt spoke on the topic of data protection and its implications for interoperability. But he first gave a short introduction to the EDPS' work and the concept of data protection generally. He emphasised that data protection is not, fundamentally, about protecting data but rather it is about protecting people or persons, public or private. When taking decisions, organisations should consider that they

have to have good reasons for doing what they do and be transparent about what they do so that people know what is happening and why. Data protection also means being accountable for what you do. So in the end, data protection is about responsible data use – thus, he reflected, the term data protection is actually not that well chosen.

He continued by outlining the EDPS' work on interoperability. He mentioned that the EDPS was a member of the HLEG on information systems and interoperability, had continuously engaged with the EU Institutions at all stages and had had prepared a reflection paper in November 2017 and an official EDPS Opinion 4/18. The main message conveyed throughout, according to Mr Langfeldt, is that interoperability is a political rather than a technological choice and that choices made now in this regard will affect further development. There is no going back to silos thereafter, he surmised. He then spoke of the principles of necessity and proportionality and outlined that there is a risk of blurring of purposes when law enforcement and migration purposes intertwine and law enforcement access is extended. Another point he stressed was the importance of data quality in the underlying systems, noting that it is the responsibility of the Member States to make sure that the data is accurate and correct.

Mr Langfeldt then spoke on the importance of being transparent, before reflecting on it be viewing it from two angles. The first angle, he noted, relates to policy development, whereas the second pertains to the traveller's view. On the policy development side, he suggested streamlining of rules for law enforcement access and clarity when adding new possibilities (for example, cascading queries vs hit/no hit access to other systems). For travellers, he suggested that with regard to the MID, further clarity is needed regarding the consequences of links. For the affected persons, information should be provided on how to challenge links and decisions taken based on these links.

Mr Langfeldt concluded by reiterating the point that choosing to implement interoperability now has implications down the line. If you build systems in this way, he argued, they can become more prone to further function creep. He advised that one should not become too greedy. He added that we are somewhat in a moving target environment as some systems are in development and others are in review; the responsibilities of the different actors have to be clear, he argued. Governance

and supervision is very relevant, he noted, so that everyone is clear on where accountabilities lie. In conclusion, he said that the data protection authorities are not interested in keeping anyone from doing their work; they just want to make sure that it is done in an accountable and responsible way in practice.

Mr Carolan began by noting that the EES, while being a large system in itself, is also an important and sizeable step on the road to implementation of interoperability. In this regard, he suggested that EES was a small technological step towards interoperable systems at EU level. Mr Carolan then went on to reflect on the EES both from operational and technical viewpoints. Operationally, the goals of EES were evident, he suggested – the system is about achieving enhanced facilitation and security. Facilitation is achieved through the extended use of automated systems such as self-service kiosks and ABC gates, while also being achieved through the abolition of document stamping. Security is enhanced, meanwhile through the introduction of biometrics, the enhanced checks of electronic travel documents, and the enhanced detection and reporting on overstay. Technically, however, given that EES is a first step on the road to interoperability, matters are more complex. The EES, he said, will involve development of many technical components and new capabilities that will be common across systems such as the initial Common Identity Repository, a website for carriers and third country nationals to query the information that is relevant to them, and the NUI. He added that there are thus implications for existing eu-LISA systems, most prominently for the VIS, which will be connected to the EES and will, therefore, have to improve its technical capabilities.

Mr Carolan then spoke about ETIAS, which brings all of the existing eu-LISA systems into play – the VIS, SIS II (future SIS) and Eurodac as well as new systems such as ECRIS-TCN, and some external sources such as the Europol data. Mr Carolan highlighted in this context that as we move to ETIAS, at least two additional things are happening: first, functionalities such as the website, the carrier gateway and the NUI are being repurposed for the function of ETIAS; second, there are elements coming into play from outside eu-LISA systems. While Europol, Frontex and Interpol and the communities that they represent are involved in use of EES, ETIAS is something different in the sense that the Agencies themselves become active contributors to the functioning of this system.

He reflected more specifically thereafter on to the topic of interoperability, which is the culmination of this development. With interoperability, he noted, all of the communities present at the conference will derive benefit from the platform in which systems and partners are working together and

infrastructure is being reutilised advantageously. Each component will not be just an ETIAS or EES component, but a technical component that is facilitating the job of the communities, including the border guards, making sure that they have the right information to do their job properly. Moving forward, he continued, what we will have is a platform leveraging interoperability, with ETIAS, EES, and existing eu-LISA systems working together to make the job at the border easier and more effective through information provision. He said that with the EES we are already moving towards interoperability; development of interoperability is thus already picking up pace.

Mr Carolan suggested to take a step back to look at what this all means, recalling the question posed earlier in the conference on how one can convert data into information. He contended that each of the systems already existing or planned provides information. For example, data on the entries and exits of persons is converted into information on whether that person is overstaying or not. Likewise, he added, each of the systems fills a particular gap in knowledge, whereby data provides information to a border guard, for example, on whether documents are legitimate, whether biometric data matches that in the systems, etc. What these systems allow the border guard to do is to process the person at the border and stop them only if there is an issue, i.e. if the information provides an indicator that there is cause to stop them. He then went on to explain that interoperability is predicated on the realisation that the information in these systems is complementary in many ways. By way of example, he noted that information on visas, entries and exits is relevant for whether travel authorisation is issued or not within ETIAS. By integrating these systems, we move from converting data not only to border relevant information but rather to border relevant insight. Mr Carolan pointed out that the obvious example is the multiple identity detector – fraudulent identities cannot be detected by one system alone. What interoperability achieves in this context, he argued, is that it gives information about potentially fraudulent or mixed up identities that can only be provided through integration.

Mr Carolan then went on to talk mention some specific figures, stating that according to rough calculations, interoperability will be massive: 130 M identities will be cross-matched every year, roughly 340 M multi-system checks will be launched at borders per year, yet the recall time at the border for information based on current system performance should still be 1.3 seconds. This will be available

at the border guard's fingertips in just a second or two, an outcome that he suggested is a massive contribution that only technology can facilitate.

In conclusion, Mr Carolan recapped that the EES and ETIAS will provide vital border-relevant information, filling gaps that currently exist in border management operations. Furthermore, he added, these systems are providing a foundation stone for Integrated Border Management. More importantly, he suggested, EES and ETIAS, are providing a substantial step towards interoperability. Through the merging of these systems, the systems will be more than a sum of their parts. Work is already ongoing on interoperability, he suggested, to the extent that the EES is the very beginning. This, he noted, was very much a community effort already underway.

Ms Haab then opened the floor to discussion.

The first audience member thanked Mr Carolan for making such a complicated topic simple to understand. He then asked Mr Carolan about one aspect of his presentation – carrier engagement. The systems are very much reliant on the carrier community, he suggested, who will be providing data to and using data from these systems. What thought has the Agency and its partners put in place to bring the carrier community to the table?, he asked, so that they understand the interfaces and the capabilities that they need to stand up themselves to work effectively with EES and ETIAS?

Mr Carolan first thanked the asker about the comment on simplicity – he believes that it is important to keep things simple, though they are indeed complicated to understand. He noted his agreement that carrier engagement will be significant in the context of both EES and ETIAS and suggested that this has been recognised by eu-LISA and no doubt by other relevant parties as well. He explained that eu-LISA had hosted an industry round table in Sofia in May, at which the carrier community had been brought to the table on the topic of the new systems for the first time. That work has been continued in the preparatory work for the EES, where it has been considered actively how to engage carriers more substantially in the EES, he noted. That work has been based on the existing regulatory framework, however, there has been some discussion on whether the regulations concerning the carriers need to be adjusted. Nevertheless, he reiterated that the carrier community has been engaged, and as work moves on into the technical development phase of the EES, this engagement will only be ramped up.

Mr Rozenburg stated that presently there is not much to add on the topic of legislative changes, however, he confirmed that this is indeed a real issue. Carriers already have a big responsibility today, he suggested, with having to transmit API and PNR information exchange and check visas. There will be more responsibilities in the future, of course, with ETIAS being the most significant, he suggested. Mr Rozenburg added that indeed contacts with the carrier community are close ones. Meetings happen on a regular basis and the European Commission has carried out a study on the possibility of a single router, a single communication channel for carriers and Member States, he noted. However, there is no final answer yet because it is complex issues and there are different regulations to consider, security and data protection matters to be borne in mind, and just financial and practical dimensions to be considered. He concluded that this topic is a work in progress.

A representative of Gemalto asked about the European Search Portal. He recalled the morning statement about having the right information in the right place at the right time and posed a practical question that had come to mind as a result – if I am a border guard at the border and a third country national comes and hands me his passport, will I have to actively go on the ESP system to launch a search or will the query be done automatically, as the passport is placed on the reader?, he asked.

Mr Rozenburg explained that once the passport is placed on the interface to scan it, the information obtained will travel straight to Strasbourg where the ESP will work its 'magic' and give the answer straight away. So in that sense, there is no additional thinking involved for the border guard. He also added that the ESP will be configured in such a way that only the necessary information will be forwarded, nothing more, nothing less.

A representative of Accenture asked about the multiple identity detector – are there 'confident links' done by an automated means and who adjudicates the adjudicators? he wondered.

Mr Rozenburg replied that the MID is a 'small box' but a complex animal at the same time. He pointed out that insofar as confidentiality and specific cases are concerned and where sensitivity pops up, particularly in relation to the SIS, there are specific rules governing those cases. A border guard might not always see all information or be aware of unconfirmed discrepancies, he noted. However, this is an area where negotiations are expected to continue because it has been identified as an important and sensitive issue by both the European Commission and the European Parliament, he noted. He estimated, that we are not yet at a conclusion on this topic.

A representative of the German Institute for International and Security Affairs asked about the intersection between data protection and technological infrastructure. The ESP is configured to have the border control officers only access the relevant information, which is reasonable, he suggested, but what are the technicalities of rolling it out in 27 Member States? When it comes to deciding on the authorisation, how will it work, he wondered – will eu-LISA just take what is reported up from the Member State instances or is it more a top-down process? Member States have different architectures in terms of authorisations and access so how are the authority levels decided? Also, on the topic of data protection, we have the GDPR and updated rules for EU institutions yet 19 Member States have not transposed directives into national law, so how will that impact open ended use of data?

Mr Carolan answered the first question by stating that the proposals for the regulations on interoperability include the concept of profiles whose exact nature will be decided by delegated acts subsequent to the approval of the legislation. Nevertheless, the general idea behind the profiles is that they will define the user, and will delineate the access rights that the person will have. There will be numerous profiles that will clearly specify who the user of the system is, what are their access rights and activities that they can perform. The

profile will be based on Member State-provided information and eu-LISA will implement the profiles from the delegated acts, which Member States will be responsible for associating to people. The supervision will be undertaken by the national supervisory bodies.

Mr Langfeldt answered the part of the question pertaining to data protection. He said that there is the regulation on the matter, which is directly applicable in law since May of 2018. Then there is the law enforcement directive which regulates processing for law enforcement purposes, he clarified. At the same time, even the predecessor to the GDPR has not been transposed by all Member States. Part of resolving that transposition question lies with the European Commission as it handles any infringement matters, where necessary, or alternatively entice the Member States to resolve any outstanding issues. Then there is a data protection directive applicable to institutions that was to come into effect in December 2018, he noted, and most of that overlaps with the GDPR, with those parts that are relevant only for the private sector having been removed. He then explained that the main answer is that the underlying principles of these acts are broadly the same. Of course, there are some exceptions when it comes to informing people that you are processing data. For example, there are some stages in police work, where it is just not done and thus the law enforcement directive provides for a little more leeway. The tricky part is at the border of these regulations, he noted.

A representative of Europol commented that there will be many information systems managing events and authorisations while we will also have the MID. He wondered, however, if there are there any discussions about a system managing identities at the EU level? Because the identity, in fact, is at the core of IBM and interoperability.

Mr Rozenburg answered that in the MID system, one very important player is the EBCGA, which even before the box becomes operational will be responsible for the huge task of cleaning up a possible legacy of false positives. So before going live, the data will be cleaned up. When the system is operational, there will be a lot of false alarms that can be easily identified and fixed at the EU level without bothering Member States. Then you only have the remaining problematic cases that need extra attention and those will go to the Member States, perhaps one or several Member States. Implementing and delegated acts are needed here, he noted, but he expressed his view that the response explained the overall mechanics.

Ms Haab then turned to the panel to ask for their final statements.

Mr Carolan began by stating that with the EES, we are already starting down a long road of partnerships, so he opined that at eu-LISA, everyone is very much looking forward to this long but interesting journey.

Mr Langfeldt reiterated the ideas of transparency - emphasising that it is vital to make sure that people know what is going on – and accountability – it is important to be able to say clearly how a certain decision was reached and not have a situation of computers saying no.

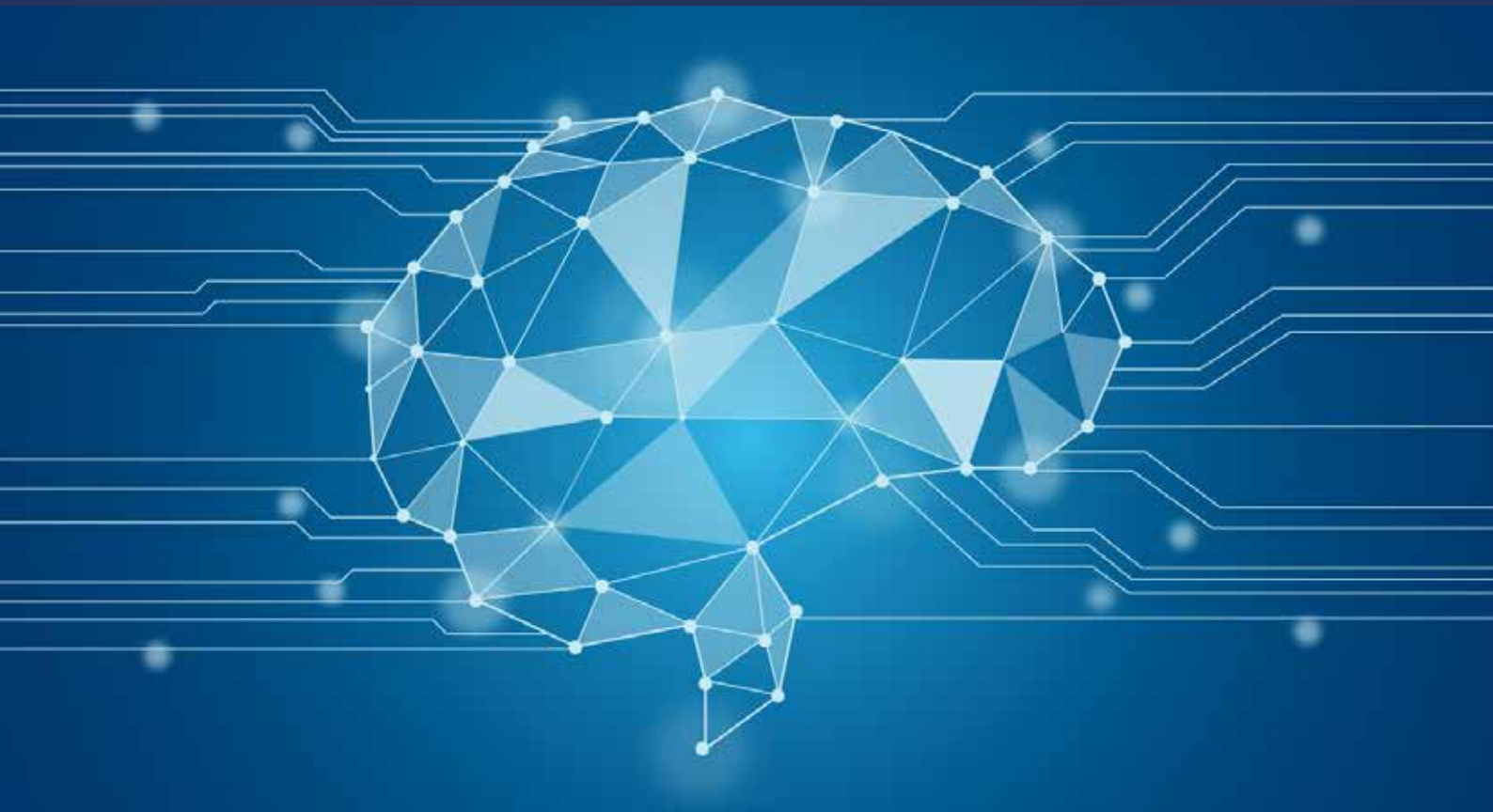
Mr Rozenburg concluded by alluding to the motto often stated at the European Parliament and the EDPS, that interoperability is not about collecting more data but using existing data in a smarter way.


LISA
CRIMINAL ACTIVITY

Session 4:
Future outlook

Moderator:
Guido Brockmann,
Head of Sector, Test and Integration Services, eu-LISA

Panellists:
Michiel van der Veen, Chief Executive, European Association for Biometrics
Laurent Beslay, Scientific Project Leader , Law enforcement technologies and citizen, DG Joint Research Centre, European Commission
Paolo Venturoni, Chief Executive Officer, European Organisation for Security (EOS)
Sirra Toivonen, Senior Scientist, VTT Technical Research Centre of Finland Ltd, BODEGA project representative



Mr Brockmann started the panel by giving a brief yet thorough overview of the previous panels.

Mr Venturoni started by mentioning known challenges including human trafficking, terrorism and organised crime. He said that the European Union generally understands these challenges well. Yet, he suggested, an effective industrial approach is still missing in the context of responding to these challenges. He added that, for the EOS, the process of digital transformation is the most important facet that often gets overlooked in policy making and where such industry support is most needed. Digital transformation is important, he noted, because it allows authorities to deal with a number of complexities that are inherent to the new security environment, yet it also introduces new vulnerabilities and risks. Mr Venturoni said that the successful handling of the process allows for at least a minimal level of strategic digital autonomy, i.e. having a certain control over the technology employed. Mr Venturoni added that while the issues have been considered since 2012 and there has been talk of a competitive and well-functioning market, it hasn't materialized until now. He continued by proposing ways to get to that point: a structured dialogue is key, as is dialogue with industry, research, Member States and EU institutions. This dialogue is necessary to reach the goals set as otherwise the needs and capabilities cannot be identified, he stated. The process needs to be supported by a comprehensive funding framework capable of implementing the necessary synergies with other programmes such as Horizon 2020 and the Digital Europe Programme. He expressed his hope that in the short-term a pilot phase could be launched.

Mr Venturoni summarised by proposing a phased approach in which something needs to be found in

the short-term that will lead to the rapid deployment of interoperability solutions and in the long-term will lead to the development and deployment of an EU Integrated Border Management program. He added that an integrated approach can only work if all the numerous operational domains of IBM are considered.

Mr Venturoni concluded by mapping out the necessary technological ecosystem, consisting of: cloud technology; mobile and 5G; positioning and tracking; cyber security; airborne platforms; artificial intelligence; autonomous and remotely piloted systems; screening and detection; biometrics and radars.

Mr van der Veen started by noting that while concepts related to identity and biometrics are key for border processes, we must not forget that they're applied in a number of other domains as well, such as e-government, the financial sector and social platforms such as Facebook. Mr van der Veen stated that we live in a time where we don't have the choice anymore of whether to provide our personal information or not when using these services – now it's a decision of whether we want to use these services or not. The question is, as a citizen, whether you trust all of these systems for handling your data in a proper, decent and proportional manner? Equally, one could ask whether you trust the border systems to handle your data in the same manner, he surmised. Mr van der Veen continued by saying that this question of trust is especially true when it comes to biometrics. Biometrics are unique, he argued, because they uniquely link to a person more so than other identifiers such as an IP address. He added that there are reports available showing that personal data can be extracted from biometric data, such as race, age, and gender. He also suggested that biometric images can even sometimes be recreated using templates such that they are similar enough to fool the systems. It must also be emphasised that there is only one source of biometrics – a person only has one right index finger. If this data is compromised it cannot be renewed.

Mr van der Veen continued by outlining some challenges ahead of us bearing in mind his introductory comments. The first challenge mentioned was security. He said that introducing biometrics in the border check process means building trust and identifying an individual. Once the person is identified, we should be sure of the person's identity. Yet Mr van der Veen brought up the possibility of creating a fake identity and entering the trusted system, noting that such a procedure would lead to creation of a trusted fake identity. Currently, there are a number of known attacks including system attacks, presentation attacks, spoofing attacks and morphing attacks. The morphing attack, which he particularly focused on, could enable someone to enrol in a biometric system with a facial image morphed with a second person. With that tooling in place, it is possible to impersonate someone if the appropriate measures are not in place, he stated. Mr van der Veen added that privacy is an equally important topic. Privacy means having personal self-determination, he suggested – having control of your own data, having the right to authorise use of that data by other stakeholders, the right to opt out, etc. He added that there is an opportunity here to integrate privacy into the design of border systems. He further referenced a third challenge – inclusion. While the move underway is towards digital and the use of biometrics, he noted, we know that not everyone has usable biometrics while certain groups are not used to using new technologies. We have to make sure we are not excluding anyone, he stated.

Mr van der Veen concluded by saying that it is all about interoperability and integration. This needs to be addressed also on an identity level, he argued, considering what it means to have an identity in multiple settings? He called for action on a number of matters that can be done as a community of all the stakeholders – government, industry and academia. He first referenced the need for action in terms of capacity building. In this market, a lot of the knowledge is fragmented yet it is important to have a larger view, he suggested. He added that the regulatory framework concerning identity and biometrics also applies in the context of borders. Mr van der Veen said privacy by design is an important concept. He concluded his presentation by focusing on innovation – in Europe we can be proud to be leaders in innovation, although across the continent it is also fragmented and thus needs some work, he suggested.

Mr Beslay started by giving a brief overview of the Joint Research Centre, which was founded with a focus on nuclear research, and over time developed into other research fields such as food, climate, security, cyber security, and biometrics. He then went on to speak about biometrics referencing topics around the European motto "Unity in Diversity". To foster unity, we need to make a joint effort, he suggested, noting that it is similar with biometrics – unity will hopefully come without uniformity and fragmentation; we must respect our differences.

Mr Beslay brought forward the SIS as his first example, since it could be considered a hybrid system. It has a degree of diversity already built in, he noted, since users are both from law enforcement and border management domains. He illustrated the challenge by giving examples of recent research on age and ageing effects on fingerprints. The study was done in collaboration with the Portuguese authorities. Mr Beslay explained that the study showed the diversity in the quality of biometric data in various age groups, which is especially a challenge among early and late age groups. On average, the quality of a 70 year old person's fingerprint is equivalent to a 6 year old's fingerprint. He added that the second element they confirmed was the aging effect. The more time that elapses between the enrolment of the data and the check using that data, the less likely the match, he suggested. As well as showing the diversity of biometric data quality, he added that the study has also contributed to some legislative initiatives such as the proposed changes to the VIS.

He added that it is important to note that there is no uniformity, yet we have to adapt to the diversity and still benefit from the large-scale IT systems in place. Mr Beslay went on to suggest that there are solutions to mitigating these effects in the processes of analytics and enrolment. One of them is introduced in the report – the possibility to apply corrections within the matching process in order to account for age as well as aging. Taking care of conditions during enrolment and the procedures of enrolment also play a key role in mitigating these effects, he noted.

He summarised by alluding to several challenges that present – the enrolment of biometric samples before the age of 6 and after the age of 70; and the application of face recognition, especially considering the growing datasets and the question of which training datasets to use in an age of deep learning and AI and considering the possible impacts on performance amongst different genders, ethnicities, etc. Mr Beslay added that a line of exploration for the JRC is utilising the expertise of the community – conducting semi-supervised machine learning while taking into account the input of experts such as the border guards and forensic experts to develop a more inclusive system.

As an aside, he also noted that the JRC is working on fingerprint / latent quality metrics, as well as the image-based identification of tattoos.

Mr Beslay concluded by stating that he is confident that some of the required solutions are present

already in the room today. Now it is about working together and implementing the solutions.

Ms Toivonen presented the results of the EU-funded BODEGA project, which focused on the human factor in border control. She gave an overview of the project, which was a 3-year EU project started in 2013. It started at the time of the first proposal of the EES, and, she noted, during the 3-year project the development towards new systems and technologies and resulting new requirements for border checks has been rapid. Mr Toivonen outlined that the project's goal was understanding of the interactions among humans and other elements of the systems. She added that the optimisation of human wellbeing and overall system performance is also key.

The research approach was a bottom-up one, with the researchers visiting different countries and types of Border Control Points where both manual checks and automated checks were undertaken, in order to better understand what is needed and what are the future challenges. She added that the air borders are much more ready for this change than other border types. Currently, the other border types are more reliant on traditional processes and technologies, she noted. Ms Toivonen added that although new technologies and databases will be implemented, the responsibility of the border guard will remain a key factor. She added that the decision making will remain the task of the border guards and if there will be a need to override the technology it can become even more challenging than today. The border guards need to be prepared in a way that they will be ready to take further steps if needed. She elaborated by saying that, of course, there is trust in technology, but only when used in an optimal way.

Ms Toivonen added that enrolment will be a challenge because using the EES will be a totally new situation for the border guards. The question will be how to conduct intelligent risk analysis when these systems are available. She added that models show that the more technology is used, the more difficult this analysis gets. It might seem that the border guards' jobs get easier, however, we must ensure that the background interaction and work supports the decision making.

Another important factor is the wellbeing of the border guards, she noted.

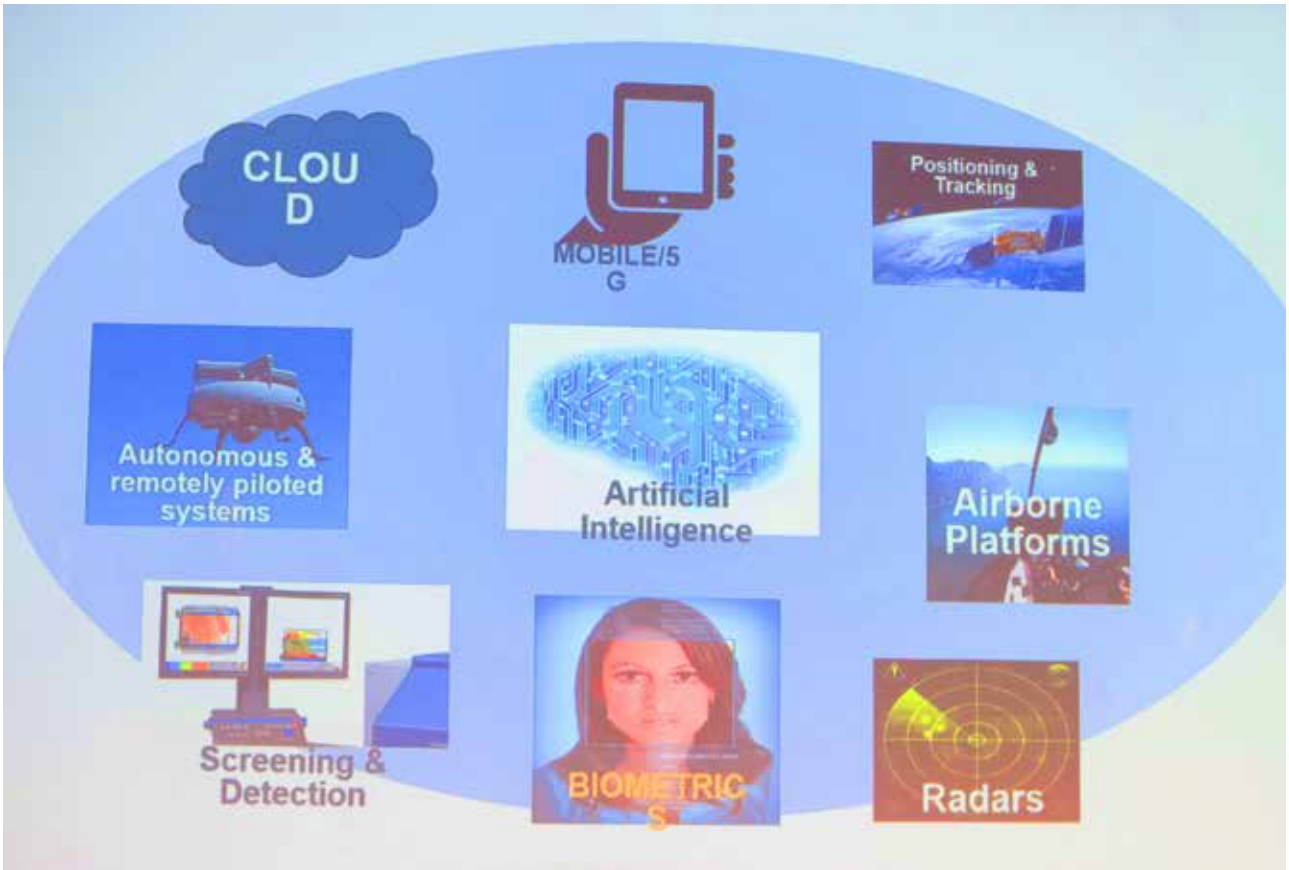
Ms Toivonen conceded that the development of technology is rapid and the border control follows these developments – biometrics, mobile technology, different ABC technologies, database interoperability. There are continuously more tools at the border guard's disposal and we must take a look at the interfaces of the technology, to ensure that the border guard knows how to

use the technology. She posed the question, at the same time, of how much of the technological background is relevant for the border guard, for example, questions related to how we come to a biometric score in order to make informed decisions. As the diversity of the systems increases, this needs to be addressed, she argued.

She continued by stating that when assessing the human factor, a lot of different factors need to be accounted for, from the social and cultural environment, through regulations operational environments to infrastructure. Some human factors have been identified in this regard, including the motivation of the border guard, which depends on many factors, such as job satisfaction, professional development, salary, workload, both external and internal, skills, trust, and situational awareness. She continued by noting that research on performance has looked into both border guard performance and system performance. Yet, she added, there is a lack of good performance assessment of border guard organisations and thus it is difficult to assess how a development affects the whole system. There were very few places where, for example, worker satisfaction was measured, she noted.

Ms Toivonen elaborated factors that need to be accounted for when implementing change. For one, the border guard must still have the right to make decisions. Decision support systems are therefore important. She added that different analyses can be used even more effectively when more data is available. She added that ergonomic factors should be assessed when new systems are put in place.

She concluded by speaking momentarily about the travellers. She elaborated that new systems were developed within the project for educating travellers before the border check. She suggested that there is an opportunity in this regard to enhance the process of the traveller going through the checks.



Mr Brockmann started the Q&A session by asking about AI.

Mr Venturoni replied noting that AI is embedded in a lot of security applications. For example, in maritime security it is used to spot rogue ships, being built into surveillance drones operating in stand-alone mode or swarm mode. AI is also increasingly used in cyber security. Cyber security systems need to respond in real time, and AI will be the best way to combat this accelerated mode of attack. He added that while all of that looks good, the Digital Europe Programme funded by the Commission to the tune of EUR 2,5 billion doesn't even mention security as one of the research fields for AI. The technology is a leap forward, but every leap forward includes risks, he suggested.

Mr Brockmann asked about inclusion and how to assure 100% inclusion in facial recognition technology?

Mr van der Veen responded by saying that AI can be of great benefit for all modalities of biometrics including facial recognition technology. It can also help with the inclusion problem, he noted. Yet he suggested that it is uncertain whether a 100% inclusion even exists, and thus it is of key importance that a proper exception handling

protocol is in place for people that either cannot enrol or for people, for example, that have enrolled but have aged fingerprints. This doesn't negate the argument that AI will help us reach a better level of inclusion, nevertheless.


Reception

Mr Brockmann asked about traveller experience, how can it be enhanced in the context of cruise ships?, he wondered.

Ms Toivonen responded by stating that the notion of supervised enrolment inside ships should be investigated more closely. Perhaps with different types of surveillance technologies this could be possible, she suggested. Otherwise it is a difficult situation when 3000 passengers try to disembark at the same time. She added that after the first enrolment, they're registered and can cross multiple borders. This brings the question of EU wide cooperation and which country is responsible for the enrolment if it's done on the ship, she noted.

A representative of Gemalto commented on AI and biometrics and sought to negate the notion that AI will necessarily introduce bias. All leading vendors use international testing systems for benchmarking, he noted, and all datasets used include a range of ethnicities and ages. If a vendor built a system heavily skewed towards one group, they would fail the tests, he argued. Rather the opposite is the case, he suggested, noting that humans average 70% accuracy when looking at other ethnicities, while the algorithms average upwards of 99%. Mr Smallridge added that AI doesn't make any judgements based on the character and looks of the passenger.

Another audience member wonder whether, in light of geopolitical changes in the world, there will be more pressure towards a European Industrial Policy around security and border management. Is protecting local IP important?, they asked.

Mr Venturoni responded by saying that it is important, but that the supply chain is nevertheless global, especially in the digital world. Certain players on the international scene are investing heavily in certain technologies, including AI. He added that it is important to have control over the technology.

Another audience member wondered whether, in order to maximise the benefit stemming from AI use, we need to feed it more and more information, some of which might go against data protection principles. Is there a case that could be defended?, he asked.

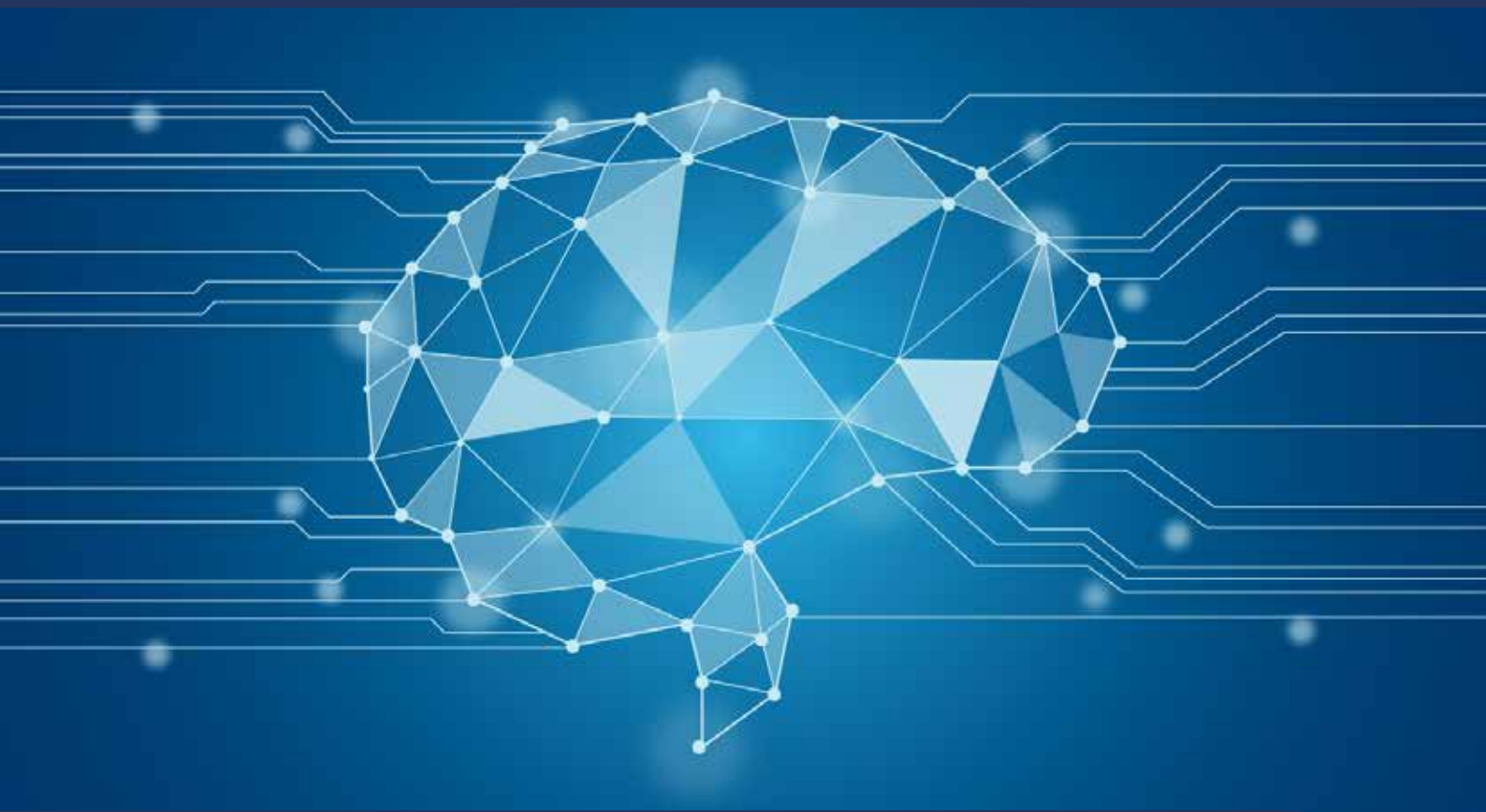
Mr Beslay started his response by saying that AI is extremely promising. There are a lot of newcomers in technology utilizing AI. There are many different approaches to using AI involving supervised, unsupervised and semi-supervised learning, he noted. In order to further improve the performance, transparency in terms of the datasets used is important. We need to be able to predict and have confidence in the performance. He added that the biggest challenge in AI is hiring people who want to work on AI. It is difficult to find clever people to develop these algorithms.

A representative of eu-LISA questioned how eu-LISA, Frontex, Europol and other agencies could best leverage the outcomes of research?

Mr Beslay added that collaboration is already on-going in various fields. In research it is absolutely necessary to understand the use case, which can only be achieved by strengthening interactions, he suggested. Communication needs to be two-sided.

Mr van der Veen added that so much deep knowledge is available in Europe yet it is often a bit hidden in certain research groups. The recent EAB conference in September brought together 18 research projects, and was jointly organized by the European Commission and the JRC, he noted. The conference was a signal that there is so much knowledge.

Closing remarks



Mr Fandler thanked all participants for the day full of expertise, talking and listening. He added that he will depart with a list of 10 steps for getting smarter through technology:

1. The time for integrated border management is now and not tomorrow. Interoperability starts to be realised now.
2. We need to convert data into information at the correct place at the correct time.
3. A strong involvement of stakeholders is needed.
4. Systems have to be highly integrated and user friendly because the last decision is always human.
5. New systems lead to more questions - be prepared.
6. Use the national room to move for experimenting with technology.
7. Interoperable EU systems for borders and security lead to mutual trust.
8. Interoperability is also a political choice.
9. Using existing data in a smart way.
10. Not Alexander the Average but Alexander the Great, think big, get smart.

Mr Garkov expressed hesitation to take the floor because he had enjoyed the day and felt that it was a pity that it must come to an end. He thanked all of the panellists and moderators for their insights, exchanges and future ideas on how to bring the new Digital Agenda further into our policy domain. He added a few personal takeaways from the day. He noted that the most important message heard from all panellists was that the future is already underway. It is great to see a consensus that the time to act is now, he suggested. What we do today to a great extent shapes the future, he noted. Mr Garkov added his feeling that a second important takeaway was that what we need to do is not something that can be delivered in isolation by EU agencies or Member States alone. We need to do it together, including all stakeholders including carriers, airports and land and sea border operators among others. Success will only possible, he suggested, if we make an effort to integrate all stakeholders and shape a common agenda that will benefit everyone in the end. A final takeaway that he conveyed was that the community has started a very interesting and challenging digital journey that will completely change the outlook of the information architecture in the Justice and Home Affairs domain. This is important, he stated, because it will be an exciting and rewarding journey. Mr Garkov concluded by saying that he is looking forward to seeing the next steps taken towards making border management stronger and smarter.


LISA
FRONTEX

The 2018 conference was exceptional amongst eu-LISA's conference series as it was co-organised with Frontex and received support from the Austrian Presidency of the Council of the EU. The future of technology-led border management proved to be a relevant and timely topic of debate for the panellists and audience ranging from border guard community to academia. This conference was our largest to date, attracting close to 200 participants!

Discussions focussed on future scenarios for border management, taking into account that in the coming years at least two new large-scale IT systems will be developed and implemented – the European Entry-Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). Undoubtedly, use of these systems implies significant change in border control processes. Efficiencies will only become apparent if the systems are appropriately utilised, technologies appropriately leveraged and border guards fully trained to deal with all eventualities. Engagement with the border guard community to enable their anticipation of future developments and their input during their development process will be key.

The main conclusion drawn from the conference is that the future is already underway – the challenging digital journey that will completely change the outlook of the information architecture in the Justice and Home Affairs domain has already started. The goals can't be reached in isolation based on work by EU Agencies or Member States alone. We need to engage all the stakeholders including carriers, airports as well as land and sea border operators.

Stay with us to follow the next steps towards making border management stronger and smarter!

Publications Office
Catalogue number: EL-01-19-006-EN-N
ISBN 978-92-95208-79-7

@EU2018AT
@EULISA_agency
@Frontex

/EU2018AT
/agencyeulisa
/frontex