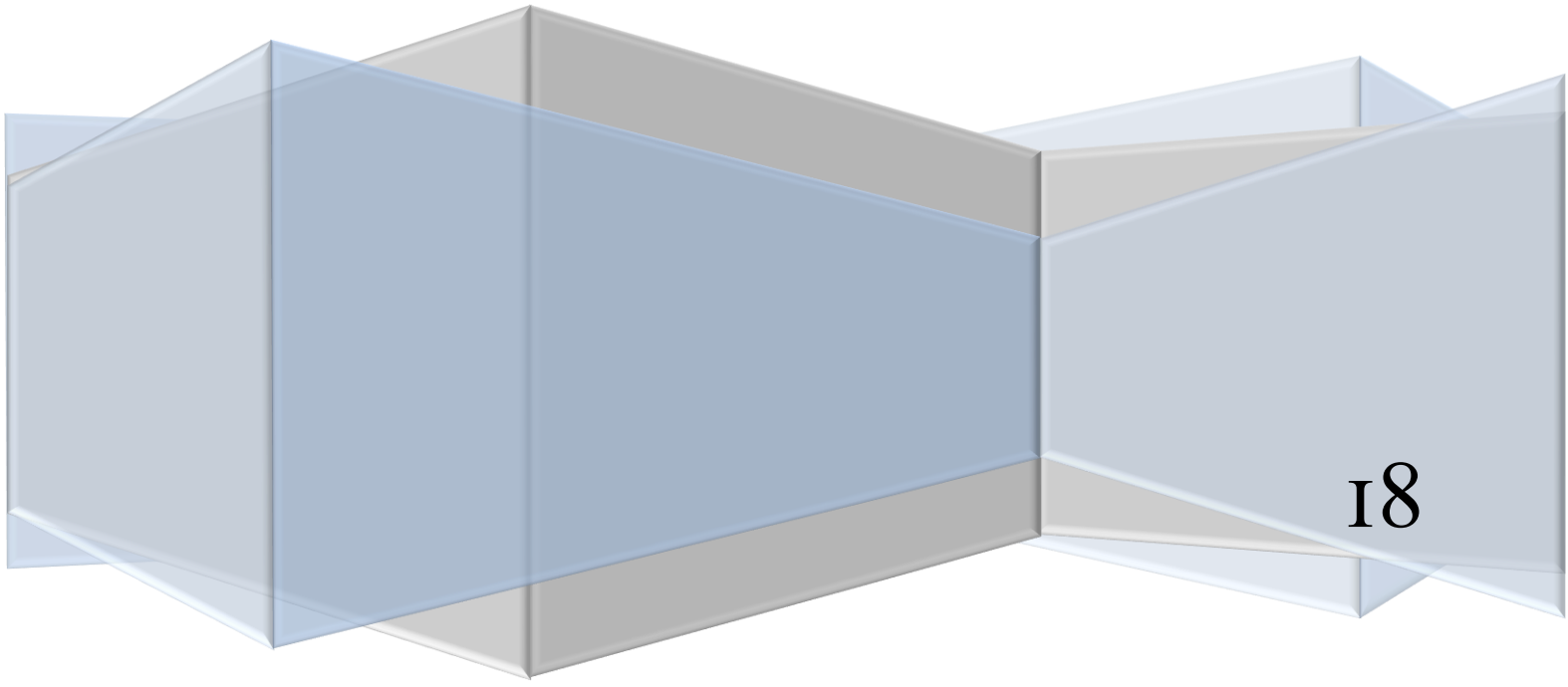
European Commission

Proceedings of the Security Research, Innovation and Education Event (SRIEE) 2017

Security Research Conference at SRIEE 2017

Unit B.4: Innovation and Industry for Security



18

EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

Directorate B: Migration, Mobility and Innovation
Unit B.4 : Innovation and Industry for Security

SECURITY RESEARCH CONFERENCE at SRIEE 2017

Blu Hotel Olümpia Conference Centre, Tallinn, 14 – 15 November

On 14 - 15 November, the 2017 edition of the Security Research Event (SRE2017) took place in Tallinn, organised by the European Commission in collaboration with the Estonian Academy of Security Sciences and Ministry of Interior Affairs and in the frame of the Estonian Security Research, Innovation and Education Event (SRIEE).

The event brought together over 400 participants from a wide range of security stakeholders such as researchers, industry representatives, public security providers and practitioners (i.e. fire departments, police, border guards, intelligence agencies, etc.), and policymakers from across Europe. In a dedicated exhibitors' area, a number of EU financed projects displayed innovative security systems and services they have developed.

This year's Event had a particular focus on how to reduce the gap between research output and the market so that innovative solutions can ultimately meet the operational requirements of security practitioners and other end-users. The round-table discussions addressed a wide range of challenges, facing security research in the future, from prevention of terrorist attacks to improving multi-country disaster response.

In general, the discussions highlighted the relevance of a dedicated European funding scheme for security research with adequate allocated resources and demonstrated how the activities launched under such umbrella are already impacting in a positive way on the European security ecosystem. Discussants also indicated that an additional effort is required to enable appropriate bridging from research output to effective products and services to be used by the end-users. In this respect, the involvement of industry, academia, public authorities and practitioners in a co-creation process is *key* to success.

The SRE 2017 opened with welcoming messages and was structured around six round-table panel discussions on security research and industrial policy themes. In launching the conference, the Vice-rector on Research, Development and Innovation of the Estonian Academy of Security Sciences, Mr Marek Link, welcomed participants from 33 countries in Estonia. He noted that Estonia will soon celebrate its 100-year anniversary and the Estonian Academy of Security Sciences its 25th anniversary. As an education institution for Estonian security services, the Academy joined forces with the European Commission and the Ministry of Interior Affairs to invite such an important network to get together, share views and learn from each other.

Welcoming messages

The first opening message was delivered by ***Mr Jüri Ratas***, **Prime Minister of Estonia**. Mr Ratas started by welcoming participants and praising Estonia's Minister of Interior Affairs. He expressed his gratitude for being able to address such a distinguished and diverse audience. He highlighted that Estonia has developed innovative digital services in the country since the mid-90s and the nation has become dependent on these services. Such services make Estonian's people daily life easier, more efficient, and allow Estonia to save about 3% GDP. Therefore, developing and testing innovative methods is something Estonia understands well. He then continued with a few remarks about cooperation in security, the Estonian digital life and cyber security. On the issues of cyber security and the Estonian digital way of life, he said that "there are nearly 2000 e-services in Estonia, all easy to use. 99.8% of bank transfers in Estonia are made electronically, 95% of income tax returns are submitted online. Yet, there is also one cyberattack attempt per second in Estonia, and there is no reason to believe that this number will go down soon". He emphasised that the government must take care of cyber space in the same way as the security in streets. This starts with a modern and innovative education system, but it also requires basic cyber hygiene on an individual level. Its success, he said, is rooted in cooperation between the private and public sector, researchers and citizens. In conclusion, he expressed his hope that SRIEE 2017 would add to this cooperation, and wished all participants fruitful discussions and an enjoyable stay in Estonia.

The conference continued with a video message from ***Julian King*****, Commissioner for Security Union**, European Commission. In his opening address, the Commissioner also welcomed participants to the annual security event. He began by stating that the EU security union is about helping states respond to major security threats across Europe. He said that the security of one Member State security is connected to the security of all, and in many cases we are best equipped to counter these threats by working together. Europe is facing threats from terrorism, cyber, manmade and natural disasters that can endanger lives and security. Often these threats are cross-border and often the solutions need to reflect that. Security research and innovative solutions can substantially help us tackle such threats. "At this event", he said "participants will have a chance to see that EU research has already produced meaningful results. Three weeks ago, the final Horizon 2020 work programme was adopted. In coming years, we will not only need to implement the programme, but think about the research framework we want to see post 2020 and how we can arrive at results that make a difference. One challenge is to ensure that research can translate into real innovative products on the market". This could mean further developing and utilising instruments such as pre-commercial procurement, better understanding of the needs and constraints of procuring bodies, getting practitioners to participate directly in projects or harnessing the expertise of EU agencies, such as the European Border and Coast Guard Agency, to bridge the gap between research and end user needs. At the same time, "to ensure adequate funding," he continued, "we need to demonstrate how research contributes in practice to Europe's security and makes a difference to the lives of our citizens". In conclusion, the Commissioner pointed out that "innovative ideas can help shape innovative solutions and tackle new evolving challenges" and thanked all participants for their engagement.

The opening speeches were concluded by **Matthias Ruete**, Director-General of DG HOME, European Commission. Mr Ruete expressed his pleasure at being able to be in Tallinn and he thanked all parties involved for organising the event. Mr Ruete underlined that "security research is at a turning point. Europe has invested nearly 2bn euros, and launched over 400 projects since SRIEE started 10 years ago, noting that the EU and its citizens expect a return on this investment. Over 1bn euros are aimed at pooling research in ICT, space, health, and

energy to develop security research". He said that the European Commission will focus on preventing serious crime and terrorism, on better border security, and on protecting infrastructure against threats, including cyberattacks. Nevertheless, translating research outputs into tools and services is still one of the biggest challenges. One of the causes for the gap is the fragmentation of the security sector on the demand side and the fact that procurers are represented by a multitude of authorities at national and local levels. Industry invests, he pointed out, where there is market opportunity, and if it cannot predict whether research will result in opportunities, it will not invest and there will be no market uptake. This, however, leads to a research non-innovation cycle, where research is not taken up and, another research project is initiated. The result is that certain technologies that could improve security are not available for the end-users. He further stated that there is no silver bullet to bridge the gap; yet, there are high hopes to improve the situation through one tool, the pre-commercial procurement. Pre-commercial procurement or PCP, he said, "puts the users at the core of the project and calls practitioners together to see which products to commercialise. The practitioners define their technological needs and the project focus. PCP also ensures that industry products meet customer requirements. By spring 2018, the Commission expects to finance the first 3 PCP projects. In the 2018-2020 work programme the PCP will remain a key feature. All stakeholders need to be involved in security projects which have real added value. More needs to be done, however, he noted. "These discussions", he said, "will be about overcoming the gap between research and market. How we shape the security research programme for the years 2020+, those are the two essential questions". In conclusion, Mr Ruete quoted Goethe, who said that "Knowing is not enough, we must apply. Willing is not enough, we must do".

The SRE2017 continued with the six panel discussions of which two were High-level. The High-level panels focused on the identification of the needs and priorities of the future in the area of security research and the possible measures to address the lack of market uptake of research outputs.

High-level panel 1 – From research to practitioners and end-users

Panellists:

Elena Santiago Cid, Director General, CEN-CENELEC
Éric Freyssinet, Chief Digital Strategy Officer, French Gendarmerie Nationale
Joseph Stahl, DG REGIO, European Commission
Clive Goodchild, Technology Planning Manager, BAE Systems Industry
Moderator: **Matthias Ruete**, Director-General, DG HOME, European Commission

The first High-level panel enabled discussion between policymakers, researchers, standardization bodies and practitioners on the improvement of innovation uptake, exploring different avenues from start to end-users. The discussants emphasized the anticipatory nature of research highlighting how the security dimension needs to be embedded from the start in any technological development.

The discussions touched on identifying needs on the practitioner's side so that research can actually respond to them. It was highlighted that for the industry to invest, the operational side has to express the need of byers and end-users such as law enforcement authorities who have to be involved in all stages of the process, from conception to the market. However, the real challenge is on how to link real procurement with real user requirements. When it comes, for instance, to user requirements and prioritisation on CBRN, the issue is complex. In

CBRN, users have been heavily involved and brought together, and as a result more than 300 user requirements for CBRN have been produced for regions and countries. One idea towards prioritisation of end-user requirements could be experimentation as well as not to work in *silos* since there are tools to help them organise such as search publications and research projects. In this context, projects should be made with practitioner networks, demonstrate technology and get communities talk to each other at cross-border national level. Some further suggestions for creating a market uptake addressed research. In particular, it was emphasised that research should have shorter life cycles, so that standardisation looks for mechanisms to integrate standardisation early enough and anticipate what can happen with the technology in terms of security. For example, as regards the interoperability of security systems in white zones, there are ongoing security research projects, financed under H2020, which look at anticipating interoperability problems that can cause security problems in public areas. Moreover, panellists also referred to the need of creating a market which is developed in safety, thus bringing security and safety together. One of the take away messages was to integrate security in the early stages of development of a security service or product. The main conclusions which stemmed from the first High-level panel can be summarized as follows:

Main conclusions:

- Practitioners need foresight tools to assess technologies for their own needs.
- They have to consider how to measure the impact of these technologies on society at large.
- Structural funds can be used through smart specialisation strategies, clustering of regions, projects and financing of networks. They can further support innovation and identify priorities at regional level which can also have security features.
- Security is increasingly coming into the safety realm, but often different sets of standards exist for each. Thus, policymakers, researchers and industry must strive towards standards that integrate the two in the future.
- We need fast-track innovation through, for instance, cyber-security flexible solutions and not really wait for long PCP processes.
- Getting the product to the market requires anticipation of the needs of practitioners and end-users, e.g. on interoperability as well as acceleration of legislation, procedures and getting the communities work together.

High-level panel 2 – The future of security research

Panellists:

Dan Chirondojan, Director for Space, Security and Migration, Joint Research Centre, EC
Jean-Pierre Serra, Vice-President Defence and Security, Airbus Defence and Space
Wolfgang Burtscher, Deputy Director-General, DG RTD, European Commission
Alberto de Benedictis, PASAG-member (Horizon 2020*)*
Moderator: **Teri Schultz**

The second High-level panel highlighted how EU security research is an essential cornerstone of EU security policy that needs to deliver results for the benefit of the citizens. It emphasised that citizens want security and economy, and the EU security research helps serve both those needs. Focused research provides the tools for adapting to challenges such as societal resilience and protection of infrastructure which citizens and businesses use every

day. 50% of all public finance in security research is done at the EU level, and only eight (8) Member States have national security research programmes, which means that EU funded and conducted security research is more important than ever. Consequently, when referencing to security, it is necessary to foresee that the EU budget needs to account for the new challenges and the citizens' expectations. In essence, there is already a broad recognition that security has to be a cornerstone in the next Multi-Annual Financial Framework (MFF) discussions.

While looking ahead, policy makers have to become ascertained of two key elements with respect to research: the first is sufficient flexibility when framing work programme calls. The discussions have already indicated that security risks are changing rapidly, so each research programme has to adapt rapidly. The second key element is how to ensure deployment. Whereas the message delivered so far is that Europe is doing well in terms of deployment, it can, however, get more successful if end-users, SMEs, etc. are better involved. When it comes to the involvement of SMEs, they are strongly represented in security projects, which are cross-border. SMEs and security is indeed a quite successful match. So, when it comes to SMEs developing new security applications and business models, they can be a source for good examples of deployment of research. But then, the problem is on how to deploy security research in the public instances. There is the role of public procurement, but it needs to be examined to what extent a European regulation could be the driver for innovation and if the right legislation could actually trigger stronger research and innovation and harvest the results.

Panellists agreed that there is no simple answer. All relevant stakeholders need to stay together, communicate and try to anticipate. Nowadays, it is difficult to act during a crisis, and instead of being reactive, Europe should become more proactive. For the future, partnerships, creating trust and building a new paradigm which is mission-oriented where consortia can decide how to best address a mission are the keys to moving forward. In conclusion, it was emphasised that the most important thing for security research is that policy makers have to take into account the existing capacities to develop innovative solutions in the framework of a European autonomy. There is a lot of competence in industry, for example, to export products, but there are also international rules. The difficulty for the industry is integrating governance from other countries to export solutions and do business. Europe has to fully liaise both with Member States and consider international rules.

The second High-level panel's conclusions can be summed up as follows:

Main conclusions:

- EU security research is an essential cornerstone of EU security policy.
- Security research is already among the most innovative, SME friendly and end-user oriented programmes of Horizon 2020.
- Flexibility/agility is very crucial to counter the constantly evolving threats faced by the EU.
- More needs, however, to be done.
- We need to create a true partnership between research, policy and the citizens through a constant dialogue.
- We need to deliver results for the benefit of the citizens.
- To make this happen, we need both a significant budget for security research in FP9 and in the MFF discussions as well as the necessary tools to be flexible and agile to counter the constantly evolving threats, faced by the EU.

After the two High-level panels, four other panel discussions took place which addressed the following security challenges:

Panel discussion: What can research and education do for police?

Panellists:

Ciaran Carolan, Research and Development Officer eu-LISA
Thierry Hartmann, Head of Division, International Cooperation Department, French Ministry of Home Affairs
Kimmo Himberg, Director, Police University College, the Management Board of the European Law Enforcement Training Agency, CEPOL
Yves Vandermeer, Chair, ECTEG (European Cybercrime Training and Education Group)
Matthias Zeiser, Vice-President, Deutsche Hochschule der Polizei (Münster)
Moderator: **Teri Schultz**

This panel discussed how the gap could be bridged between police forces and the challenges they face, on the one hand, and researchers and the results of their work, on the other. Discussants emphasized that we need a better understanding of research, conditions of research and acceptance of research within the police forces. There is the general feeling that innovation is the task of academics who, should bring it to practitioners, who believe that their job is to, for example, just be a policeman. Yet, this is not true. The value of research for police work on the street has to be seen. Criminological research, for instance, has been there for hundreds of years, but we understand only a little of the root causes. In effect, some of the security problems could be better addressed because of such understanding. We have all heard the term anti-terrorism units and how these are equipped; however, they are perceived as after-terrorism units which should not have been the case. The real anti-terrorism units are actually the researchers trying to understand the causes of extremism – what makes a young person adhere to extremism and how to avoid that.

Panellists also commented on the duality of research and police work. The police science should follow developments in other branches, such as technical, social and other types of research. There was agreement that any bipolar setting should disappear by realising through practical examples that the merging of investigators and researchers can produce excellent results, in terms of efficiency for the security field.
When talking of police work, all over in Europe, there is a digital transformation going on and it is very true for policing as well. Things like big data, smart policing, information-exchange, drones, unmanned vehicles, these are all things that are increasingly relevant and this proves that digitalisation is increasingly important for policing. Such challenges lead to the realisation that increasing the awareness of technology and scientific reality for police is really important for their work. This is also reflected in the academisation of police education, but it cannot be achieved only by that. We need competent police officers to face the challenges, related to the speed of innovation, in areas such as terrorism, migration, demographic change or cyber. Using the outcomes of research in police practice is very important, and should cover a whole range, i.e. both technology-related, security research, as well as cultural, social, human sciences. Technology and society evolve so fast that an occasional training is not sufficient. There is a need for a continuous education of police officers.
Nevertheless, after educating students and future police officers, we have to find a way to keep them. The people need to understand that it takes time, a lot is invested in education and once graduates have the opportunity to share that knowledge, through giving some lectures,

they are happy and stay in police work. The question of valorisation, valuing the people, keeping them involved and working efficiently is very important.

The panel also explored how research and education could help identify the needs of law enforcement agencies and develop solutions that can support these actors in their daily job. Law enforcement should be able to permit individuals to be part of natural innovation, to give free reign to the people and enough space to discuss innovation. We have to overcome the contradiction that law enforcement organisations have only top-down processes, since innovation is a bottom-up process, and thus, it is more organic. So, to better integrate research and innovation, it should be part of the job where individuals in an organisation should feel free to bring in innovation.

Law enforcement agencies need to move from competition to coordination, from training to education. The only competitors are the criminals. Technology is always changing and experts need to keep their knowledge updated. If experts are kept in one country, after two years, their expertise is expired. So, expertise is valuable, but if it is kept within the academic sphere, it becomes invaluable, so cooperation needs to be further promoted.

In this context, policy making was also added to the discussion. There is never enough money, so setting priorities for policymakers is of utmost importance. Cybercrime is manifold, so if someone steals one's iPhone, it is cybercrime, attacks on companies are cybercrime, it all runs together, but the approaches need to be different. Therefore, on the ground, there have to be processes in place for different exercises. One solution is collaboration between researchers and police forces at both national and international levels. Such cooperation can work, but it needs time and there is time pressure. It is possible to anticipate crime, but good cooperation is at all times needed.

The main conclusions which can be drawn from that panel discussion are:

Main conclusions:

- We need competent police officers to face the challenges, related to the speed of innovation, in areas such as terrorism, migration, demographic change or cyber.
- Using the outcomes of research in police practice is very important, and should cover a whole range, i.e. both technology-related, security research, as well as cultural, social, human sciences.
- Technology and society evolve so fast that an occasional training is not sufficient. There is a need for continuous education of police officers.
- Building an EU capacity is crucial; a way to obtain it is to have less competition and more cooperation, less training and more education.
- Research and end-users are not two distinct poles anymore. This bipolar setting is disappearing nowadays, and there is a good intention of all parties to create bridges by, e.g. research-driven education of police forces as well as internationalisation of their education.

Panel discussion: Preventing and responding to terrorist attacks

Panellists:

Demosthenes Ikonomou, Head of Unit, ENISA
Üllar Lanno, ENFSI and the R&D Standing Committee, Director of the Estonian Forensic Science Institute
Patrick Padding, I-LEAD coordinator, ENLETS
Priit Suve, Professor, Estonian Academy of Security Sciences
Moderator: **Erkki Koort**

The panel discussed whether the solution to terrorism is more police or should there be more intervention on the social part. Terrorism demands enhanced control, fewer liberties for citizens and more centralised authorities. Strategies are needed in policing which are based on partnership and networking. To improve, we have to advance our knowledge in completely new ways in criminology, policing, and policymaking. With regard to these issues, ENISA presented that it has already established a cooperation group, which consists of response teams that cooperate through the exchange of information and experience on incidents. Today, there is more cooperation in law enforcement; however, there should be more cooperation with the civilian sector too. In terms of research, most of the work needed has to do with establishing the forms of cooperation; however, there are other areas where further research would be necessary such as cryptography and encryption.

Furthermore, as to the state of research in forensics and their relation to terrorist attacks, this depends on the country as forensic investigations are carried out in different ways. There are less than 35 labs from 28 countries in police forces, but large differences can be seen between them. One aspect, depending on the post-blast, is that there are several different disciplines; yet, ENFSI is gathered around the 17 different pan-European working groups. Second is that terrorism has changed, thinking back 5-10 years ago when explosives were the only way to express negative emotions, but now terrorists use rental cars and stabbing, so it is hard to tell what will be used next.

Additionally, Europe lacks capacity building for terrorist attacks though there are a lot of networks for specific domains. So, we need to bring networks together and make sure each delivers expertise to combat terrorism. First, we should understand that terrorism is not something substantial but rather transactional. For example, imagine the US policing initiatives before 9/11 and after. It is the same, but somehow completely different. The question is what kind of changes terrorism brings about, and in which areas, and how we should conceptualise it, especially going forward in policies and education. Another question is how it influences police behaviour. In this sense, terrorism is a transactional notion and therefore after each attack, the society is different and the notion changes.

Moreover, terrorism puts binary pressure on both states and organisations. We need more information, to know how people behave and how they are thinking, how people move toward radicalisation. If we at least hope to tackle these issues, then the police and state in general should build up trust between the state and its citizens. We need to use strategies in policing that are based on partnership and networking. So, there are different kinds of pressures as on the one hand, the authorities become more centralised and on the other, there are demands for being more connected with citizens and get adequate information from communities.

The participation of civilian organisations could be especially beneficial, but research is important as well and we need direct access to research, although police work is mostly very operational. Recent attacks show that any terrorist attack is a huge event. For example, at

Bataclan, a lot was going on immediately, so there is no room for research there, but we need to research how to take away the violence. Research, for example, into how to ensure swift and agile communication, which is needed in those situations. In the after-attack period, it will be very useful to look at what kinds of bombs were used, but also how we can restore safety and security and how to give citizens trust again. If the research is in place, we can determine the background and use it for forecasting following events. More synergy of the networks would be beneficial for thorough knowledge of the pre-, during and after-attack period.

Another crucial thing which was addressed was sharing the right information with the right people. Criminals do not trust each other, but they share a lot of information. The law enforcement does trust each other, but they still keep a lot to themselves. Establishing good platforms for information sharing is important. Terrorist attacks have sensitive information and sometimes it is of the highest confidentiality. In those situations, trust is a huge barrier to solving cases quickly. In terms of legislation, there is still a long way from leasing information outside the domestic area. When crossing the border, any control over the evidence is lost, even though all labs are accredited to the highest standard. Another critical issue is official domestic language. All documentation post- and pre-blast is in national languages, but there is an immediate need of translation. Lastly, an area which panellists considered it as one with high potential for research is encryption, as well as metadata. Metadata was outlined as a high-potential topic for fighting cybercrime and cyberterrorism, while keeping in mind data protection rules.

The main conclusions from that panel discussion can be summarised as follows:

Main conclusions:

- There are many LEA networks and working groups involved in preventing terrorist attacks.
- One of the biggest challenges now is to bring all these networks together to identify their research needs.
- LEAs and private operators react in very different ways to incidents, involving their data networks. Intelligence agencies turn inward, while banks and telcos turn outward to their peers to alert and deal with the problem. That makes difficult to exchange information between them.
- Building up mutual trust, accountability between LEAs and Member States it could well advance an efficient, agile, rapid communication and information sharing.
- Hybrid threats are difficult to be foreseen. Yet, they occur and thus LEAs should be prepared by identifying threats of such a nature.
- Preparedness, sharing of information, know-how and good practices in an inter-disciplinary manner across LEAs, prosecutors and first responders are important elements for addressing situations before, in and after terrorist attacks.

Panel discussion: Towards dematerialised border controls?

Panellists:

Enrique Belda Esplugues, Deputy Director General of Communications and Information Systems for Security, Ministry of Interior of Spain

Edgar Beugels, Head of Unit Research and Development, EBCGA/FRONTEX
Frank Heijmann, Head of National and International Trade Relations, Customs Administration of the Netherlands
Joanna Goodey, Head of Freedoms and Justice Department, FRA
Helen Neider-Veerme, *Head* of the integrated border administration bureau of the Police and *Border Guard* Board, Estonian Border Guard
Moderator: **Ralf Otto**

The panel discussed how border guards are working together with the industry and service providers to work towards dematerialised borders. The vision for dematerialised border controls focuses on eliminating physical border controls for both: the traveller, and the security agent at the border crossing. Work is underway on implementing these systems, utilising facial biometric identifications. The system relies on pre-enrolment of the users in four phases: data collection; identification of the travel document; capture of biometric data; checks in police databases. From the technological point of view, this requires highly reliable biometric algorithms, interoperable systems and databases, and an adequate processing and communication capacity. Borders should be managed in a holistic way; this means that the borders need to be considered from three aspects: a) control point for people; b) control point for goods; and c) as a protection system. The main investment at the moment is in biometrics, getting the parameters for the people. Finding technical solutions is easy, but the main questions are how to protect this data.

Panellists started by making the distinction between border checks and border security. Concepts were further elaborated by explaining that border checks mean actions that take place in the border crossing points, while border security means surveillance and securing the border between the crossing points. Furthermore, there are differences in border security for land and sea borders. On the sea, there is no physical border, which makes any comparison with border controls on the sea very complicated. This can be further contrasted when talking about land border security and the tendency in Europe to create physical obstacles in light of the migration crisis. Finding the right balance between control and trade facilitation is key. Conversations with the international trade sector resulted in three key requirements: pushing the control away from the border, not intervening in the chain of logistics, for instance, checks already during the loading of the container, and any other intervention should only take place when necessary.

In terms of land border security, the aim for border crossings is to make it as non-intrusive and fast as possible, regardless of the crossing point. In all cases, it should be remembered that it is still the traveller who is the owner of their own personal data and the decision to give this data is left to them. The current processes for border control, border checks and physical security checks have become ineffective, because everyone has to go through the same process; there is no distinction made between persons of interest and those that are not of interest. The key to becoming more efficient is an individual risk assessment. It must be determined before getting to the border who is of interest and who is not. To effectively use individual risk assessment, a valid input is needed; in the context of airport border crossings this already exists, albeit it is limited as regards advanced passenger information and personal name records.

With regard to surveillance situational awareness and their relationship to fundamental rights issues, panellists suggested that interoperability is a key aspect to having quality data while protecting fundamental rights. Data protection provides the guarantee of legality and reliability for the customer. There are also exceptions foreseen in the regulation for public

safety reasons. If work is up-streamed with fundamental rights, it is more likely that things will go right and will not end up in court. Whereas ETIAS is the solution for the average traveller, when it comes to asylum crises, the situation is completely different and fundamental rights need more attention.

As a last point, all panellists agreed that in dematerialising border controls, the role of end users is important and good research and technology should built in all stakeholders. An efficient involvement of the industry should be further endorsed as otherwise security research projects will not come to fruition. Research has two elements: addressing existing identified gaps but also addressing future needs. When this is connected to policy development where decisions are taken, the input of end users is missing. The end users, the side representing the demand, should get organised so that common requirements can be passed on to the industry. As a result, this also would allow the end users to be in the driver seat of development.

The main conclusions which can be drawn from that panel discussion are:

Main conclusions:

- Europe's border control community should organise itself to identify its research needs and carry out joint procurement.
- The end-users of technology should be in the driver's seat instead of industry.
- Dematerialising Europe's borders demands high quality of upstream data for cargo and passenger treatment. If you have good data, it will allow focused risk-assessment to catch terrorists, identify missing children, survey trafficked people or goods and deal with other security challenges.
- A number of research projects are already contributing to the development of a dematerialised border control vision.
- Compliance with fundamental rights' requirements is an essential part of a risk assessment screening process.

Panel discussion: Managing multi-country disaster situations

Panellists:

Sebastien Penzini, Programme Management Officer, Risk Knowledge and Analysis (United Nations International Strategy for Disaster Reduction)
Montserrat Marin Ferrer, Scientific Project Manager, Disaster Risk Management Unit, Joint Research Centre, European Commission
K. Phil Waters, Director, US Department of Homeland Security, Science & Technology Directorate
Jean-Michel Dumaz, Security and Defence Programs Director, FIRE IN Coordinator Managers)
Rob Testelmans, Policy Advisor Safety and Security, Emergency Planning City of Geel
Moderator: **Annika Nitschke**

Each panellist gave a presentation on the role of the different Centres or Networks which they represent in managing multi-country disasters. Under the umbrella of the Disaster Resilience Management Knowledge Centre (DRMKC), an increasing number of Commission services

collaborate to strengthen the link of policies to maximise the impact of more coherent implementation of these actions. Of course, a common idea is data – for analysis, policymaking and monitoring, to see if the policy is functional. The need for data comes together with the need for models. If the data reflect the past, what is already lost, the models allow forecasting new losses and developing timely mitigation and prevention measures. The DRMKC developed around three key pillars: fragmentation of networks, fragmentation of knowledge and the need for more innovation. A set of activities has been put in place, for example, the promotion of establishing scientific networks for creating and disseminating information. The second types of networks that are supported bring together scientists, practitioners and policymakers, which is an important part of bridging gaps. Special attention also goes to gathering knowledge and providing access to it. For example, FP7 projects related to Disaster Resilience Management have been gathered and mapped, and they are now available on the website. These projects have also been integrated with other previous ones. So far, there are more than 650 projects and close to 3000 organisations involved. The final reports of the projects are also available. Other activities include publications, for example, a recent one that is a comprehensive overview of what is known in disaster risk management up until now, compiled with the cooperation of 270 experts. They also publish and distribute newsletters to share information. After knowledge is gathered and analysed, gaps are identified, and tailor-made recommendations can be made to states. Their small projects support the transfer of knowledge and technology. Another key factor is providing space for more innovation through training, conferences and education.

The second presentation was on the International Forum to Advance First Responder Innovation. It started in 2014 and brings together leaders from 13 countries and the European Commission to focus on two main challenges: 1) a lack of a mechanism for first responders to identify and discuss shared capability gaps, and 2) the perception of industry that the first responder market does not provide incentive for them to develop innovative and affordable solutions. The Forum's approach is to work with first responders to develop a common set of capability gaps, and to characterise the global market, then giving that input to the industry. It has also developed a market analysis of the gaps, which provides the industry with opportunities to develop the technology. The next step was industry summits, where the gaps were discussed and information disseminated.

The third presentation was on the FIRE IN network which joins fire and rescue practitioners and provides a forum for discussion among various stakeholders to define capability gaps. Due to climate change, there are new hazards which responders have to face. The number of large disasters is likely to increase, and technological developments also pose new hazards and risks that have to be addressed despite the budgetary constraints. There are also networks that are similar for police and border guards. The network is in constant discussion with the industry so as to better organise their cooperation.

In essence, regarding cooperation, all panelists agreed that it needs to be enhanced among different disciplines, sectors, actors for a more efficient risk reduction, from the international to local levels. Knowledge transfer and research uptake by practitioners was considered as key for identifying gaps, aligning research and policies, and reducing market fragmentation. In managing the disasters, we need resilient societies, knowledgeable practitioners, technology, policies and laws. These can be at different levels, from local to European, global, etc. Knowledge has to be passed on through training, and research has to look at what gaps there are and what is needed. The most important thing is communication, to see what

has been learnt and what can be used in the future. The topic is complex, because it looks at prevention, preparedness, capacity-building, mitigation or recovery.
In 2015, about 100 million people were affected by disasters, whereas 22.000 people lost their lives. An estimated 300 billion euros of economic losses are as due to disasters yearly. In figures, 20 million persons were displaced due to disasters internally and cross-borders, so it is a topic that needs international commitment. For that reason, in 2015 UN Member States adopted the Sandai framework for Disaster Risk Reduction, aiming at decreasing human and economic losses, as well as strengthening state preparedness and regional assessment.

All discussants stressed the need of running risk assessment, which is important at all levels. Hurdles to more effective work include a lack of communication and *silos* as it needs to be better understood that we live in an intertwined world. Another hurdle concerns the geographic level, going beyond the national level, cross-borders. Disasters do not know borders, so there are a lot of teams that go to other countries to provide support. However, for the right response, a lot of interoperability is needed. When aircrafts are involved, interoperability requirements increase as well. This is the case when forest fire response is needed. Both drones and conventional aircrafts could be used to address the interoperability issue. There is also the cyberspace, where each team has a digital space for sharing messages, but IT systems are often developed for one fire department, which does not communicate with other systems. The third hurdle is investment. Financial and economic realities force local governments to economise on various costs, including personnel. An even bigger factor is technological advancement, it provides opportunities, but at a price. By the time the lengthy procurement processes are over, the technology is outdated. Joint procurements and purchases, as well as use can be one solution for specific technology. Technology also does not fully respond to the needs of the end users, but if they were to organise in clusters and cooperate with research, it would function much more efficiently.
Europe is in a challenging time, so in this context, all stakeholders have to define priorities and means are limited, but disaster relief has been recognised as a critical issue for the well-being of the European citizens. Moreover, timescales have to be considered, because different instances work with different timelines. Research is a bit slow, and at times policy comes too late, because there are so many implementing bodies. There is a lack of synchronisation, but the DRMKC is involved in improving the situation and aligning the shift more. Another concern is how to better reach the end users. At the institution level, there are contacts with only representatives of organisations. When it comes to data, for example, that is gathered at the city level, the process should be more a bottom-up one, where aggregated data reaches EU institutions, so as appropriate policies could be formulated. Prevention as such is not attractive because it is done immediately and there is nothing to show. Also, reconstruction and recovery phases can provide more input to policymakers. So, one solution would be to shift disaster management to disaster *risk* management, and this is where the researchers should enter the cycle.

Gap assessments can provide the necessary input for resolving issues. Formal platforms are still needed. Some central aspects include: a common top-down/bottom-up approach, understanding each other, finding results of research, and the importance of standardisation for filling gaps. Changing ways of thinking is also important. We are moving from nationalist thinking to cross-border problem solving.

The main conclusions from that panel discussion can be summarised as follows:

Main conclusions:

- Disasters have no borders. Efficient risk reduction requires a strong cooperation among different disciplines, sectors, stakeholders, from international to local levels.
- Actions are required to bridge the gaps among research and innovation, policy implementation and uptake of knowledge by practitioners.
- Networking at multi-national level is essential for sharing experiences, identifying gaps, reducing market fragmentation, and aligning research and policy agendas.
- Practitioners should be given a voice to provide inputs to policies and industry.
- Multi-actors' cooperation in safety and security at international and EU levels can efficiently be leveraged through Horizon 2020 actions.
- A stronger involvement of the private sector is required. More than 80% of involvement in disaster risk management is expected from the private sector, so Public-Private partnership is essential.

Other elements that stemmed from the detailed discussions include the following:

- Security research is not only about high-tech development. It is also a crucial enabler to address the root causes of security threats.
- Pre-Commercial Procurement is an instrument that needs to be further explored so to verify if it can effectively allow to bridge for research to the market.
- Standardisation is key to drive procurement.
- Building a European capacity is vital, and the way to reach it, is through reinforced cooperation, trust and cross-fertilization among all relevant entities and domains.
- An after-life support of projects is required to ensure appropriate dissemination of research outputs and to enable possible new activities (e.g. further research or procurement) to be, as appropriate, consequently triggered.

Closing statements

After two intensive and interesting days of presentations and discussions**,** closing statements were delivered by:

Erkki Koort, Secretary General, Ministry of Interior of Estonia; Mr Koort mentioned that the added value of the conference is contacts, ideas and cooperation. He said that the "discussions helped create good ideas and innovation in our heads, and now it is important to get those ideas out by formulating them".

Katre Raik, Rector, Estonian Academy for Security Sciences; Mrs Raik highlighted that this event marks the end of 25 years for the Academy which currently hosts some 900 students.

Matthias Oel, Director for Migration, Mobility and Innovation, DG HOME, European Commission; Mr Oel said that the discussions demonstrated that we are doing well, but that we can do better. He underlined that "building European capacity is vital and the way to reach it is through trust, cooperation and cross-fertilisation among relevant entities".