SRE event 2018
SECURITY RESEARCH

Proceedings of the Security Research Event 2018

On 5 – 6 of November, the 2018 edition of the Security Research Event (SRE2018) took place in Brussels, organised by the European Commission in collaboration with the Austrian Ministry of Transport, Innovations and Technology.

The event brought together approximately 800 participants from all over Europe and beyond, representing a wide range of security stakeholders such as researchers, industry representatives, policymakers, public security providers and practitioners (i.e. fire departments, police, border guards, first responders, etc.).

In a dedicated exhibitors' area, 50 EU financed projects displayed innovative security systems and services they have developed. Participants had the chance to touch with hand and test the different innovative security solutions and to gain more information about what is being developed under different areas of EU security research.

The event was opened by Director-General of DG Migration and Home Affairs, Ms Paraskevi Michou. Keynote opening speeches were held by Mr Norbert Hofer, Austrian Minister for Transport, Innovation and Technology, Mr Dan Nica, Member of the European Parliament and Mr Olivier Onidi, Deputy-Director General of DG Migration and Home Affairs.

The 2018 edition of the SRE focused on demonstrating the impact of security research. On the first day two high-level panels addressed the challenges surrounding dissemination and outreach of research results. One the second day eight technical panels focused on the specific areas Border security, Citizens awareness, Cybercrime, Maritime Security, Disaster resilient societies, Terrorism, Protection of public spaces and Radicalisation.

Discussions in the SRE 2018 have undoubtedly helped to raise awareness of the challenges surrounding effective dissemination and communication of research results and started tracing the way forward.

European Commission

eu2018.at

Bundesministerium
Verkehr, Innovation
und Technologie

KIRAS
Sicherheitsforschung

Migration and
home affairs

High-Level Panel 1 - Making Europe a safer place: Demonstrating the impact of security research – Challenges and barriers.

The first High-level panel examined questions relating to the challenges of communicating, disseminating and exploiting security research outcomes. All panellists agreed that the identification of needs on the practitioner's side is crucial for research to respond to them. There is a need to invest more in research, understand better the environment in terms of threats and increase the awareness of the state of the art of technologies. EU Agencies appear to be best placed to collect and aggregate the requirements of the end user community and can play a relevant role when evaluating prototypes of new solutions.

The panellists stressed the need of triggering a capability development process and the need to bridge the gap between the Technology Readiness Levels (TRLs) applied to research funding and the TRL needed for the innovation process. One proposed solution to possibly address the "missing link" between the research programme and the procurement programme was the establishment of innovation partnerships.

Generally, industry will not invest in research if there is not a market opportunity. The notion that there is a market opportunity is what makes innovation more relevant and effective.

The main conclusions from the first High-level panel can be summarised as follows:

- Security represents a huge market in the EU, but it is divided in silos. Harmonisation is strongly required.
- An effort needs to be done to improve attractivity for industries so to avoid research results ending to the 'valley of death'. A consolidated European security market could facilitate this process.
- It is important to continue supporting a collaborative research effort. The role of Agencies is crucial, and so is the collaboration between Member States to create joint security requirements.
- The tracking of existing and new technologies cannot be solely done through projects. A platform for research with the Member States can be a useful tool towards this direction.

High-Level Panel 2 - Projects Afterlife: From the lab to real life.

The second High-level panel highlighted the need for a general agreement on common operational requirements as this would considerably accelerate standardisation processes and thus would be a key enabler for an EU security market. Furthermore, the panel highlighted the relevance of building bridges between security Research and other funding Programmes such as the European Regional Development Fund (ERDF). In this respect, the ERDF addresses security through the Smart Specialisation Strategies, supporting innovation, start-ups and scale-ups. There is already an ongoing pilot on cyber-security, which brings together different regional perspectives across the EU.

The discussants agreed that research would support the objective of preparing for possible future threats. Vulnerability and Risk Assessment mechanisms would help anticipating such needs. The elaboration of a Capability Development Plan should be under the enhanced mandate of the European Border and Coast Guard Agency (EBCGA). The EBCGA 2.0 Regulation brings in the concept of Border Management Capabilities, both to address the challenges of today, but also of tomorrow. In such a context, the EBCGA has already started working on conducting a Capability Development Process.

Discussants emphasised that it is necessary to work on a scenario-based approach to facilitate the interaction with all actors, including users, industry, researchers, etc. Procurement will be a key enabler.

The EBCGA can play a very important role in procurement, in partnership with the Member States. Yet, there is a need to study the legal specificities on the use of the Pre-Commercial Procurement (PCP).

The main second high-level panel conclusions are:

- The EU Urban Agenda contributes to the protection of public spaces through the establishment of a partnership between EU cities.
- We need to streamline all the sources of funding to build capabilities: EU research funds, funds of Agencies, other security funds like Internal Security Fund and the Integrated Border Management Fund (IBMF).
- To facilitate the market uptake of research, a two-fold approach is necessary: a top-down approach, based on needs and focussing on operational perspectives, harmonisation and standardisation, and a bottom-up approach, which is pushed by technology requirements.

Panel discussions

Panel 1 – Citizens Awareness.

The primary question posed by the panellists was “Who is the citizen”: security research is expected to contribute to the protection of citizens through concrete solution oriented projects. As such, and citizens need to be involved in the process as early as possible so for them to be aware of these solutions and agree that they are effective.

Convincing scientists and practitioners to engage citizens in security research might not be straightforward. Consequently, structured processes need to be established so to ensure appropriate participation and in order to build trust among citizens’ communities and authorities towards the envisaged technologies. This requires a shift of society’s mind-set, but could prove to be an effective way to enhance preparedness, and improve disaster resilience.

An interesting discussion emerged around the role of children that are often overlooked in disaster management processes, although their input can provide very valuable insight better planning of emergency prevention and responses.

Panel 2 – Terrorism.

The very heterogeneous panel that included policy makers, practitioners (law enforcement) and industry led to a very fruitful discussion on the role of security research in the domain of counter-terrorism. The operationalisation of the security research outputs in this domain remains very complex. As emphasised in the panel, research is essential for understanding terrorist threats, technological possibilities and risks of technology; it helps identifying needs and skills, building strategic autonomy for the EU industry and developing an adequate EU policy.

The area of counter-terrorism is a very closed environment in terms of methodology which, to a certain degree, prevents opening up to the research and industrial community. Trust is needed to overcome this barrier, and trust-building activities between research, industry and Law Enforcement are a promising way towards an applied research success in this domain.

The way that Law Enforcement understand research is technology driven and short term – they need immediate solutions. Matching longer term research with operational reality is a challenge. As a consequence, for research in this domain to be useful, it is absolutely necessary for it to be user-centred and proactive. In order to keep pace with fast developments of terrorist threats, incrementalism and agility are necessary means to reach solutions that would be useful at the end.

Panel 3 - Border Security.

The importance of EU funded research for the understanding of the challenge faced at the EU borders and for the systematic development of border management capabilities cannot be overstated.

Research has actively contributed to a better policy making in this field. Likewise, during the past years, policy priorities have steered border security research towards real and urgent needs. There is still the necessity to better anticipate the needs of tomorrow, to plan research accordingly and capitalise on its results.

Seamlessly integrating research planning into a wider capability development planning is paramount to identify the needs of tomorrow, to ensure that research outcomes respond to urgent needs and to facilitate the development of EU industrial capacity in alignment with policy and operational priorities.

Research requires time and it cannot always be accelerated. However, it can be anticipated. Programming research according to a systematic assessment and programming of capabilities can improve the impact of EU funding on mid to long-term objectives. Under the umbrella of a Capability Based Approach, research would not only respond more accurately to the needs of MS and EU authorities, but it would also facilitate a better understanding of current and future challenges by all stakeholders and have a notable impact on the harmonisation of the EU market. It should be noted that technology is not the only enabler of capabilities. Therefore, the role of the human factor and of non-technological research should not be disregarded.

EU funded border security research provides an ideal framework for working together in building a common vision. This refers to the end-users, who need to express requirements in operational terms without prescribing a solution. Industry needs to integrate users in the development cycle. And, finally, policy should be more agile to capture successful research results and bring them to life after the end of the projects by facilitating the access to other instruments, including procurement and standardisation.

Panel 4 - Disaster resilience and risk reduction.

Topic of the panel was the question how security research could better support civil protection policies and related operations and thus help improve the management of disasters, both natural and man-made.

In line with observations in other panels, the discussant stated that there is a clear need to overcome silos and build up synergies among research, capacity-building, market dimension and practitioners. One example here is the Commission's Joint Research Centre (JRC), which actively supports policies and research programming through knowledge centres.

Furthermore there is a need to involve users from the very beginning of projects in order to test ideas and build trust in a multidisciplinary motion. This will ensure a co-creation process of direct benefit to disaster resilience improvement.

From a practitioner viewpoint, the evolution of threats leads to new ways to respond. For example, recent forest fires rapidly turning into mega fires require not only new technologies, but also new ways of thinking and new preparedness strategies.

The fragmented market and scarce resources are a barrier to the use of technologies by first responders. One example of consolidating needs across national borders is the International Forum to Advance First Responder Innovation (IFAFRI), which identifies capability gaps in a bottom-up identification process and then pushes to technology development via market, research and standardisation, when needed.

A promising trend is the use of spatial technologies to helps forecast organisations and find responders in improving disaster preparedness and response, and to communicate better with citizen. Galileo, the European Union's Global Satellite Navigation System (GNSS), has the potential to become a powerful service in this respect, as it requires an agreement by Member States and the European Commission to use it publicly.

Collecting data in disaster situations is a critical feature. Besides technologies, first responders may act as data providers if properly equipped.

Panel 5 - Radicalisation.

Lively exchanges in the radicalisation panel underlined that multidisciplinarity is key for making the research projects useful in this field. Various issues were addressed from different angles, such as the role of research with respect to mid- and long-term prevention of radicalisation leading to extremism, and the role of policy in steering research efforts and making use of research results. Research should be included as a pillar of the policy work in this domain. After that, the discussion turned around most successful ways to maximise the impact of research in the field of criminal justice with a focus on radicalisation and extremism (e.g., in prisons).

As research on radicalisation contains a significant social science component, commercialisation of research results is generally not possible. This raises the question how to produce usable final product for research projects in this domain.

Difficulties of internationalisation and of data access in the EU further hampers research and communication in this area. The Radicalisation Awareness Network is an example of an organisation stimulating the collaboration between research projects and practitioners on one hand, and, on the other hand, making sure that research performed at EU-level supports activities aimed at harmonising radicalisation prevention initiatives (such as trainings) across EU borders.

Another question deals with how to determine the impact and effectiveness of developed programmes resulting from H2020 security research projects related to countering violent extremism. Hereby the specificities of radicalisation in the Western Balkans and the role of research in tackling these issues in an efficient way was discussed.

The panel drew the conclusion that building cooperation between practitioners, researchers and policy makers should start from the practitioners, as what is relevant in research is not always relevant for practitioners. In addition, it is not always evident how to manage different timeframes between practitioners (who need solutions quickly) and researchers. Involvement in each other's work is a way to bridge this gap.

Panel 6 - Protection of Public Spaces.

The panel discussion highlighted that the safe-city pillar is fundamental in the smart-city approach. There is a need to keep innovating and investing in research in order to continuously adapt to the fast changing threats.

However it was emphasised that cities alone cannot cope with the challenge. Law enforcement authorities, public and private operators, industry and citizens need to cooperate to safeguard the security continuum. The EU also needs to be supportive to ensure the transition from ideas to solutions, from research to deployment.

The collaborative framework enabled by EU funded security research allows a better understanding of each other's perspectives. Acknowledging that research needs to be user-centred, a better understanding of user needs will reinforce the competitiveness of industry at EU level, but also worldwide. To that aim, a structured dialogue between all stakeholders should be maintained throughout the innovation cycle.

The panel emphasised that technology can be very powerful in addressing the protection of public spaces, but we need to make sure that innovative solutions address security by design rather than as an add-on. The technologies also need to be inclusive, protect the privacy of our citizens, keep the openness of the urban spaces, maintain the identity of the cities and avoid creating new vulnerabilities. Security solutions are integrated not only by technology, but also by people. The societal dimension of research is therefore paramount to increase the acceptability of the new solutions.

The panel further elaborated that cities perceive different risks when investing in innovation. On one hand, it would not be advisable to pursue a radical change of paradigm at the first attempt. Research needs to be revolutionary but also evolutionary, building step by step on the legacy infrastructure and constantly adapting to a challenge that evolves every day.

On the other hand, it is difficult to promote investments when there is no benchmark or evidence of performance. Research should facilitate this benchmarking and validation of innovative solutions before their deployment in order to minimise the risk perception. EU cities can play a key role in the development of the next generation of solutions for the protection of public spaces by defining concrete needs, but also acting as a real-life test-bench for the assessment of practical and innovative technologies.

Panel 7 - Cybercrime.

Many aspects of cybercrime were tackled in this dynamic panel that brought together high-level European experts from Law Enforcement, policy, research and private sector. The discussions touched upon situational and tactical cyber-related analysis and the role of research in longer-term prevention and mitigation of new forms of cyber criminality.

The discussants analysed the main challenges and solutions for practitioners and researchers to keep up with evolving cyber threats.

Another important topic was the cooperation between the academic world and Law Enforcement, as well as the uptake of research output in order to make tools available to the cybercrime community. As in other panels, the question was addressed how to ensure that research responds to the needs of practitioners. Traceability of the commercialisation of European research projects in this domain was tackled too.

The panel highlighted possible ways (voluntary and mandatory) in which the private sector can contribute to the fight against different forms of cybercrime (e.g. online fraud, attacks against information systems) in cooperation with researchers and public authorities.

Its «borderless» dimension is an important characteristic of cybercrime, and specific to this domain. A possible response could consist of providing free tools to the specialised Law Enforcement Agencies (LEAs), but the sustainability of such an approach is questionable, as these tools have to be regularly updated in order to keep up with emerging threats. Moreover, there is the need that research is involved in preparing adequate and up-to-date trainings to LEAs. Finally, the panel discussed the main obstacles for the private sector to be involved in EU research projects and the main expectations of the private sector regarding these projects.

The panel concluded that in cybercrime, research is essential to understand threats and trends. However, sustainability is one of the most important challenges of research projects. Ways to accelerate projects and fasten the research cycle have to be exploited. Finally, cybercrime is a borderless crime, and the solution also must be borderless and free to LEAs.

Panel 8: Maritime Security.

Maritime security faces multidimensional challenges, from possible terrorist or cyber-attacks on infrastructure to different forms of trafficking, including drugs, arms, human trafficking and migrant smuggling. Therefore research needs a comprehensive, cross-sectoral approach, based on risk assessment.

The panel referred to the action plan of the EU Maritime Security Strategy. The plan includes the production of a "Civil-Military Research Agenda for Maritime Security", organised around nine topics:

1) Maritime Surveillance – Concepts, Systems, Sensors, Platforms;

2) Interoperability, Information sharing and Cybersecurity;

3) Environmental compliance, Energy and Life cycle;

4) Decision support systems;

5) Port and sensitive area protection;

6) Autonomous systems, Networking and Communications;

7) Sensor allocation and Modelling;

8) Maritime security studies;

9) Multi-purpose platforms.

The panel discussed the connections between the civilian and defence dimension of maritime security, and it explored the scope of future initiatives, considering ongoing activities, possible synergies in R&D programming, EU policies and instruments.

The panel stressed the need to complement surveillance capabilities with cooperation. Interoperability, information sharing and trust building among stakeholders are crucial.

One example is the EUCISE2020 pre-operational validation project, in which a large number of national authorities jointly procured research services, in synergy with other funding schemes, both European and national. The EUCISE2020 project achieved the creation of a cross sectoral community able to define common requirements, and led to new developments at the national level. In the upcoming months, the project will explore the way forward to arrive at an operational Common Information Sharing Environment by 2020, with a joint effort by different Commission DGs, including DG JRC, EU agencies, the External Action Service, Member States, and industry.

The panel identified Procurement of Innovation as an important tool. The panellist representing industry strongly supported Pre-Operational Validation as a modality for the public sector to strategically provide the vision for investments. The panellist representing the national (Portuguese) Directorate General for Maritime Policy commented on the positive participation in Pre-Commercial Procurement (the Marine-EO project).