REPORT ON THE ESSEN SECURITY INNOVATION SYMPOSIUM 2010

Andrea Jerković / Alexander Siedschlag
Programme Chair

Summary

The *Essen Security Innovation Symposium 2010* was staged at the international lead fair *security essen*, offering multifaceted presentations and discussions of relevant civil security topics. Leading experts from politics, business, industry, and research gathered in the city of Essen/Germany, the Cultural Capital of Europe 2010. 34 speakers from 13 countries in particular enquired needs for security innovation at the interface between social and cultural systems.

The Symposium facilitated the creation of networks of different stakeholders and experts and aims for new civil security concepts and insights, relevant to communities and the public. Moreover, the participants discussed how security research can best provide useful results for end-users from industry and economy and combine their efforts in recent and future projects, also considering the convergence between security and safety. Other topics discussed included the creation of trust between security providers and the public; public communication about security; including the public as a partner in official security strategies; developing and assessing security scenarios and related technological needs.

The issues of standardisation strategies for security in the European area of fluent borders and the cross-national interoperability of standards were also addressed, as well as the problem of making security and increase in citizen security by projects funded with public money measurable on a comparative basis. Many of these aspects were related to the area of disaster management and civil protection, also reflecting new policy challenges emanating for the European Union, its member states and industry from the Lisbon Treaty.

The Symposium was realised by the *European Security Conference Initiative (ESCI)*, the symposium platform of the *CEUSS | Center for European Security Studies at Sigmund Freud Private University Vienna*. ESCI has been organising international security conferences since five years, based on latest insight but clearly practically oriented. The focus is on assembling expert knowledge from different segments of the security sector, policy and think tanks, thus identifying need for action from a pluralistic perspective.

Presentations held at the Symposium is available in a dedicated paper room.

5 October 2010 – Main Theme: European Challenges of Civil Security

Keynote Speeches on Security Research in the European Union

Thomas Kutschaty, Minister of Justice of the state of North Rhine-Westphalia, stressed in his opening speech the fact that the *security essen* fair, with its focus on civil security, has already succeeded to meet the growing demand for security technology and contributes to the ambitious but necessary goal to raise standards of security. Demand is especially high in the domain of IT security and the managing of sensitive data, challenge for both public service and private companies. In many ways, this huge event represents the informational backbone of modern society. Dependence on virtual assets has grown to a degree where an offline-phase of for example *Facebook* means temporary loss of access to our digital identity.

The importance of the internet as the communications hub, as Minister Kutschaty reminded his audience, requires all stakeholders to apply specific rules regarding data security, even more so when the conflict between individual freedom (and responsibility), and the obligation of the state to provide for security is exacerbating. Minister Kutschaty also stressed the question of awareness: How much and to what extent are people willing to publish on the Web personal information? Are they aware of the possible ramifications? Authorities are expected to make publicly available important information, which presupposes high security requirements and standards, especially when some information is targeted at a specific (limited) audience, such as information on the land register. Today, protective systems in place are subject to constant attacks, which necessitate increasing employment of data security specialists. Data security, as Minister Kutschaty put it, often means an armaments race between the experts and criminals in action and reaction.

Minister Kutschaty found *security essen* to be the ideal venue to illustrate for the public the risks and challenges of data security. And, of course, as he said, security also means business: The global market share for security-related products and services is estimated to have doubled at 231 Million Euros by 2015. It is vital to acknowledge and address the challenges posed by an interconnected and interdependent world: Security does not stop at national borders. This is why Minister Kutschaty especially welcomed the *Essen Security Innovation Symposium* as an international gathering of the expert community side to side with the international lead fair *security essen*.

Klaus Keus from the Joint Research Centre of the European Commission started his speech by also remarking on the comparably rapid growth of the security market, at the same asserting that security essentially comes down to a multidimensional challenge. He went on to explain that often security is reduced to a question of technology, but in fact it means and entails much more: There are political, market, technology, process, and social dimensions of security. According to Keus, the grand challenges are sustainability and growth, knowledge and the innovation society as well as the increasingly blurring line between safety and security. Indeed, Keus argued, it would become more and more difficult to see one without the other in areas, such as crisis management, disasters, nuclear safety and security, consumer protection, and public health.

Concerning the search for possible standardization strategies in the security domain, Keus proposed a bottom-up approach from the national to the global level of challenges. He particularly stressed the importance of interoperability of systems and equipments as a decisive need from the user point of view. However he conceded that there is no single definition of interoperability. Either way, the fact that there are new and emerging security

application areas in public administration is a clear sign that more harmonized solutions are needed because law enforcement application areas are not isolated anymore. This, as Keus argued, shows the following two requirements:

- The cooperation between agencies, parties and actors across borders has to be stepped up.
- The growing interconnectedness between security and safety has to be considered.

Keus pointed out that the political vision and the framework conditions for security are set. This is illustrated by the Stockholm Program, which provides that EU member states' authorities and law enforcement bodies shall cooperate across borders to ensure a common standard of security and protection of all European citizens. Keus also mentioned that standardization and research are two sides of one coin:

- Successful standardization requires a new long-term accompanying approach
- Strengthening the alignment and systemization of research results into practice
- Pre-normative standards: they require the early involvement of standardization organizations
- In favour of technological approaches, research-related processes and procedures as integral part of standardization in security research are often forgotten

Keus also introduced the concept of Security Scenario Profiles (SSP). Within these, technology would be combined with social issues and procedural aspects. These profiles would have to be validated by operational need and criteria. The SSP could provide a way to actually "measure" security.

For the citizens, it would be important to know that security is being guaranteed (without the depth of all the details), so question should also be: How to gain citizens' trust in solutions put forth by security research? This also entails measures to raise the awareness and visibility of security. The rationale of the SSP is that concrete scenarios matter to the citizen – instead of an isolated technological solution. Therefore, in order to make security and its issues more visible to the citizen, the creation of the European Security Label has been proposed.

Luigi Rebuffi, European Organization for Security (EOS), elaborated why 2010 was a particularly important year for security in Europe: The adoption of the Lisbon Treaty has brought about new provisions on external border control, prevention and fight against crime, and disaster response. New civil and military capabilities have become available for the Common Security and Defence Policy (CSDP) of the European Union, a solidarity clause has been introduced and the Stockholm Program on internal security has been adopted. It is mainly concerned with privacy and fundamental rights and also paves the way for the Internal Security Strategy, for initiatives in law enforcement, for R&D activities, for EU certification scheme, and for an internal security fund (which is a new instrument that would hopefully provide a better focusing of resources).

The EU Internal Security Strategy, as Rebuffi reminded the audience, for the first mentions the link between safety and security by stressing that the challenges posed by the two are interrelated, for example in the area of transport. The Strategy also establishes five headline goals in the areas of organized crime, terrorism, cybercrime, border control and crisis management.

In the area of European industrial security policy, as Rebuffi maintained, an intensification of the link between security policy and security research should be sought as well as a deeper dialogue with users and operators to better determine operational needs. Validation and certification of innovative products are needed as well as standards both for technology and procedural aspects to achieve interoperability or compatibility.

Plenary: European Challenges of Civil Security

The plenary on *European Challenges of Civil Security* started with a presentation by ***Juha Hintsa's*** (Cross-border Research Association CBRA, Switzerland) on "A Focused Standard to Enhance Security in Supply Chains". As he explained, the challenge is to create a full sense of security and focusing on a standard in supply security. There is a need in the development of standardization for crime incident reporting in the European Union, the harmonization of the interaction between business and relevant authorities throughout EU for reporting of crime incidents as well as the streamlining and speeding up the process of collecting and sharing data on crime incidents for the benefit of both supply chain operators and authorities.

Talking about this comprehensive framework for analysis and design of supply chain security standards, Hintsa presented a 14-dimensions model for security in supply chains, including the following:

- anti-terrorism focus vs. anti-crime focus
- public sector drives vs. private sector drives
- physical security measures vs. non-physical measures (CCTV, processes, practices, training)
- local/regional coverage vs. global coverage
- cross-border security focus vs. inland security focus
- governance agency verifications vs. private sector verifies
- incident prevention focus vs. post-incident recovery

In the future, Hintsa said major efforts need to be invested in detailed analysis and modelling of crime types/taxonomy in supply chains, as addressed in the LOGSEC project in the 7th Framework Programme of the European Union (FP7).

Irina Comardicea presented ongoing work in the FP7 project SECURENV, reviewing and analyzing past environmental accidents and catastrophic events, identifying novel and emerging threats as well as the technological opportunities, developing potential scenarios involving environmental terrorism, and providing policy recommendations to EU-policy-makers as well as relevant experts and practitioner communities. As Comardicea said, the manipulation of the environment is nothing new; security and environment are being linked in space and time (see agriculture, animal domestication, plant cultivation etc.). Environmental crime is being perpetuated by organizational groups, doing it for profit. Unknown consequences and poor system understanding about the creation of artificially organisms, exponential technological advances as well as bio-hacking and democratization of knowledge are still open for many answers.

Marieta Vos (University of Jyväskylä, Department of Communication, Finland) stressed that technological solutions for security problems are not enough and the public should be more involved. The FP7 project CrisComScore she presented follows that aim, contributing to turning the general public into active players in various disaster scenarios. Planning for joint preparedness, communication strategies should be integrated, cooperation should also be about procedures for up-scaling, alert systems and national centres should be more involved. Concerning monitoring quality, there are some important questions: What information needs do people have in coping with the crisis and what do they perceive as challenging? What are the citizens' needs and perceptions? Following the discourse in the media and on the internet, and knowing stakeholder segments and communication climate (media use, information seeking and processing), what sources and intermediaries are seen as reliable? In the context of the aftermath of a terrorist attack, crisis communication has to pursue the goal to create a public that is better prepared. Thus, Vos concluded, the task for communication is to achieve a more resilient society.

Shlomo Shpiro (Bar-Ilan University, Department of Political Studies, Israel) presented on "Counter-Terrorism Crisis Communication Strategies for Recovery and Continuity" Seeking to achieve political or social change through violence, confusion and public fear, terrorists' main perception is especially influencing public through chaotic media coverage, influencing and impacting the private lives, and creating chaos by media pictures. Therefore, public authorities and corporations need a crisis communication strategy for the aftermath of terror attack. Shpiro presented the FP7 Project SAFE-COMMS that aim is to develop effective and flexible terror crisis communication strategies. This case study analysis consists of 25 recent terror attacks in 8 countries He cautioned that common strategy must be incorporated into wider crisis plans and trained in advance. The role of the public in security has been given a very passive and negative one. Consequently, it should be perceived as an extension, including the dialogue between public and security. Shpiro also stressed that it is necessary to incorporate communication strategies into wider crisis management plans and that such strategies have to be trained in advanced. The hitherto existing model of top-down communication from the authorities to the public has become obsolete. He also remarked on the imbalance between capability planning and intention planning, adding in general that too much focus was put on capabilities planning, and questions concerning actual trends and drivers for terrorists were rather neglected.

Parallel Working Groups

Working Group 1: Towards a Comprehensive Approach to Disaster Management and Civil Protection

Wolf Dombrowsky (Steinbeis Hochschule Berlin, Germany), chaired the working group, introducing it with the thesis that "Disasters are not an event. The reality is in many ways very different." According to Dombrowsky, we have to differentiate between modern disasters and disasters from the past. The modern ones are processes that people have never experienced before. Already experienced disasters can be seen as "stories of yesteryear." Disasters bear little relation to the settlement as well as norm structures. Dealing easily with human and technical resources, an anticipation of variations is needed. In summary, it can be said that if we know where we stand nowadays and what is coming up in the future, we can prepare for disasters that will happen in the foreseeable future.

In modernity, the range of insecurity is very broad – from traditional disaster and accident (Newtonian = mechanical events) to systemic failures, such as energy failures, power shortages etc. Disaster can be seen as a breakdown of something or as the instability of a process, i.e. money problems in the modern world (see financial crisis). A security concept can, therefore, be called comprehensive if it is adaptable to all the different levels of a disaster. People have to be taught to analyze their vulnerabilities and strengthen their resilience. The workshop's conclusion was that everything that can go wrong has to be an integrated part of safety and security concepts. Inter-agency cooperation is very much required: The division of labour approach is outdated today, and all stakeholders need to be brought together. Thus, a strengthening of the managerial component of civil protection has to be pursued in order to render any approach really "comprehensive".

Working Group 2: SecureCHAINS – SME's Access to European Security Research and Development

Juergen K. von der Lippe (vdlconsult, Germany) moderated the working group, explained the need to identify of weak spots in security technology supply and to search for and transfer of advanced security technologies provided by small sized enterprises which are then capable to fill the gaps. The workshop identified the need to gain a better understanding of the nature and the structure of the supply chains which provide security technology solutions. That covers for example the security of citizens, the security of infrastructures and utilities, the intelligent surveillance and border security as well as the restoring security and safety in case of crisis. As von der Lippe explained, the methodology of the SecureCHAINS has five steps. The first step is to identify weak spots in supply chains. The second step is the review of needs – which results can be used (national projects etc.). The third one is to get in contact with SMEs because it is very important to go into the field. The fourth step is to get all information and analyze all inputs. The fifth and last step is to build information that are understandable by SMEs and needed for new business and market integrations.

Working Group 3: Cybercrime and Information Security

The working group was led by ***Maximilian Edelbacher*** (AVUS Group, Austria) and focused on police work that has changed dramatically while the basic forms of crime have stayed the same, such as cheating, greed, etc. The really novel threat is in the domain of cybersecurity, that is in the form of identity theft. Cybercrime means a danger for non-tangible assets and shows that vulnerabilities and threats have changed. Possible means of prevention include:

- Someone starting to work with a computer needs to show proof they have an anti-virus software.
- Awareness-building measures are necessary.
- More customers-orientation with new, smaller, more flexible products would improve usability.
- Information sharing will continue to be important in the future.

Unfortunately, there is no single definition that can be found for cybercrime and the term must be seen company-specific. In data transfer by public institutions, often no encryption is used, which provides a simple and open market for hackers who thus can easily seize the private data.

Working Group 4: Integrating Safety and Security?

The working group was led by Markus Hupfer (EADS Deutschland GmbH, Germany) and focused on two leading questions: What does security mean? What is the difference between Security and Safety? In the discussion on the (different) nature of safety and security, several aspects came up. Security, the discussion concluded, is all about someone trying to infringe laws. Security normally has to do with governments (borders, national security, etc.) as being charged with providing it as a public good. Safety, however, is all about people and individuals; safety frames an issue in an operational sense (safe operational processes etc.) A strong connection was noted during the discussion between safety and security issues.

The Duisburg disaster case (Love Parade) was also critically discussed and it was noted that it was precisely the security measures that actually caused the fatalities (basically, opening the gate at the wrong time). Building on this discussion, application scenarios for security and safety aspects were addressed in the sense that it is never possible to implement safety without the right security measures. The leadership of a country also determines how security is understood in a country. Security is a part of safety, and it should not be forgotten that in the English language there is a distinction between the two terms safety and security but in many European languages not. In order to run security in reality, one must combine the two terms together. Only if there a new combination of these concepts is being created can a system operate according to the standards by which it must function.

Panel: Future Scenarios for European Critical Infrastructure Protection

The afternoon panel on “Future Scenarios for European Critical Infrastructure Protection” was introduced and moderated by ***Carlos Marti Sempere,*** Ingenieria de Sistemas para la Defensa de Espana, SA (ISDEFE). This panel started with the following question: Why does Critical Infrastructure need to be protected? The answer to that followed immediately was: Because of strong interdependencies and significant impact on society. Protection needs to face man-made and natural incidents. Moreover, the European Union Treaty leaves the Member States with responsibility for implementing adequate measures, and EU policies rather focus on the identification of European Critical Infrastructure. To the challenges of Critical Infrastructure protection belongs that those infrastructures are often owned, operated and/or managed by private companies. States therefore need to provide incentives for private companies to invest in protection, while the broad number of assets does not allow full protection and integrating protection with other business process remains essential. The protection of Critical Infrastructure can be mastered more cost effectively in a broader context.

Human factors we discussed to play a particular role in early detection of risks and threats to Critical Infrastructure. Also stressed was the importance of identifying vulnerabilities in Critical Infrastructure, benchmarking new measures and implementing on the level of the state of the art (organizational arrangements, procedures, technologies). Critical Infrastructure measures and capabilities need to cover prevention, protection, monitoring, early warning as well as detection, reaction, and consequence management. In research, we need a more or less comprehensive methodology and a representative set of scenarios – context scenarios and planning situations to deal with “unknown unknowns”?

6 October 2010 – Main Theme: EU 7th Framework Programme Security Research

Information Day

During the information day, ***Christiane Bernard*** and ***Maria Spulber*** from the Research Executive Agency (REA) presented the current call in the Security theme and addressed relevant technical as well as thematic issues, such as ethical aspects. ***Klaus Becher*** (Knowledge & Analysis LLP, United Kingdom) and ***J. Peter Burgess*** (Peace Research Institute Oslo, PRIO, Norway) shared with the audience their experience as evaluator and, respectively, project co-ordinator. Highly demanded bilaterals were available for discussion of project ideas with REA officers and a brokerage session was held.

Discussions during the information day elaborated that European research, should concentrate on making studies like roadmaps as well as making adequate qualitative and quantitative surveys. Relating to the citizens security and technological security solutions, research was stressed to must have an impact in and for the society nowadays. Societal impacts have to be measured and explicable for its appropriateness.

Parallel Session: SecureCHAINS – A Dialogue Between Technology Supply and Need

In this project-related parallel session chaired by ***Jürgen K. von der Lippe*** (vdlconsult, Germany), the focus was on the recognition of the weaknesses in the security procurement in the technological field. SMEs could, fill safety gaps by offering technological services to other enterprises. Even if the SMEs are not always able to comply the most innovative technology and research, their services should not be ignored. Among other things, the National Competence Center Aviation Security Research (NCAS) was presented, which „supports pro-active and future orientated innovation for a seamless passenger and freight flow in consideration of efficient processes and a high security level.“ NCAS is a running platform dialogue between end-users, institutions, and companies, which are operating with security technology. Thus, the technology must support the new products (innovations) and contribute to the safety of the air transport.

Closing Plenary and Keynote Speeches

The Closing Plenary of the Essen Security Innovation Symposium 2010 started with focusing on the roadmap building for security missions as presented by ***Pierre-Alain Fonteyne*** (Center of Applied Molecular Technologies, Université Catholique de Louvain, Belgium). Roadmapping, as he explained is pursued in the Integrated Mission Group's (IMG-S) Security Research Roadmap (SRR), includes "Foundation Topics", that is the identification of underlying technologies and capabilities that are not specific to only one particular mission but are essential for the successful implementation of functions and capabilities in or across several missions.

J. Peter Burgess (Peace Research Institute Oslo, PRIO, Norway) stressed that normative values are being present in Europe, but that security as a process changes values. Security in practice needs to be fragmented and individualized, and it is difficult to see how it fits into a comprehensive conception at the European level. However, security as a process

reproduces values, such as democracy, rule of law, and freedom of expression. The European Union is, therefore, based on mutual recognition, and on recognition of multiplicity. This, however, also includes the multiplicity of threats. Attempts to Europeanize security by seeking a general approach to eliminate root causes of insecurity, as followed by the Internal Security Strategy of the EU, still need to acknowledge the pluralism of threats, as Burgess concluded.

Michael Schreckenberg (University Duisburg-Essen, Faculty of Physics, Physics of Transport and Traffic) pointed out that any analysis of emergencies and mass panic not considering human factors such as psychological aspects is incomplete. As an example, he mentioned cultural coping with density. Panic, he suggested, needs to be debated and associated more with the issue lacking information, for people behave rationally, yet based on available information. Schreckenberg criticized most disaster management concepts for lacking provision for the case of a complete breakdown of communication and thus technologically based dissemination of information.

Wolf Dombrowsky (Steinbeis Hochschule Berlin, Germany), spoke on emerging research and training needs in the filed of emergency management and civil protection. He mainly identified related needs to exist in the fields of logistics and deployment, leadership, co-ordination, and common language. He was critical of the concept of end-user involvement into research processes and closeness of research to the market: If research develops the market, how can we define closeness to that market in advance? As Dombrowsky reminded to audience, we even do not know how national publics define security on a beyond-victimization level.

An important general conclusion of the Essen Security Innovation Symposium 2010 is that security research itself is directed towards and has an impact for the society as a whole. This societal impact has to be measured and explicable for its appropriateness. As security increasingly affects entire societies, the public and private sector will pursue similar goals in order to protect people and infrastructure. In particular, the role of the public as an active actor in civil security matters has to be enhanced and more clearly addressed by research and its practical ramifications. Both researchers and end-users need to become clearer about how to measure security, investigating innovate indicators.

Group photograph of the speakers and some participants of the Essen Security Innovation Symposium 2010

IMPRINT

Programme Chair

CEUSS | CENTER FOR EUROPEAN SECURITY STUDIES
Sigmund Freud Private University Vienna Paris
Schnirchgasse 9a
A-1030 Vienna/Austria

Phone: +43 (0) 1 798 62 90 50
Fax: +43 (0) 1 798 62 90 52
E-mail: mail@european-security.info
Website: www.european-security.info

Organisation

MESSE ESSEN GMBH
Congress Center Essen
Norbertstraße
D-45131 Essen/Germany

Phone: +49 (0) 2 01 72 44-567
E-mail: pco@messe-essen.de
Website: www.messe-essen.de