Conference proceedings of the Leiden-Delft-Erasmus dinner debate on Safety and Security, 8 December 2015, at the 7th European Innovation Summit, Brussels

WWW.LEIDEN-DELFT-ERASMUS.NL

CONTACT
Drs. Jacqueline Dekker
Projectmanager Leiden-Delft-Erasmus
J.K.Dekker@tudelft.nl
T +31 (0)15 278 6777
M +31(0)6 18 54 68 10

Universiteit Leiden The Netherlands

TU Delft Delft University of Technology

Erasmus University Rotterdam

INTRODUCTION

Citizens around the globe consider safety and security to be of increasing importance as the world finds itself in more and more complex, regional and political turmoil and in armed conflict. Globalisation, global migration and the impact of new technologies with a global reach make safety and security an even more pressing theme. Hence, better insight into safety and security are top priorities for the European Union. This requires fundamental and applied research.

European Members of Parliament as well as Europe's national and EU policy makers require to maintain an open dialogue with researchers, scientists and engineers on safety, security and stability within the EU and beyond. Research, analysis and tools support EU policies on, for example, border security, including maritime borders, the fight against organized crime and corruption. The implementation of safety and security measures against possible biological, chemical and explosive unintentional or deliberately induced losses also represents a EU top-priority.

On 8 December 2015, a High Level formal dinner on Safety and Security was held, hosted by Member of European Parliament, Ms Cora van Nieuwenhuizen. The dinner was part of the 7th European Innovation Summit in the European Parliament in Brussels. It was organized by Knowledge4Innovation with the aim to actively engage researchers of the Leiden-Delft-Erasmus University Alliance in a dialogue with politicians and policy makers. Thematic discussions held at eight dinner tables of ten guests each have led to the attached recommendations and conclusions for Members of the European Parliament and EU Institution representatives.

Recommendations and conclusions of the Leiden-Delft-Erasmus dinner debate on Safety and Security at the 7th European Innovation Summit, 8 December 2015

THEME: SAFETY AND SECURITY OF ECONOMIC WELFARE IN EUROPE

Introduction: Prof. Matthias Haentjens, professor of Financial Law, Leiden University

Description

In the course of the most recent economic and financial crisis the vicious circle between banks and the sovereigns turned out to be the main cause for instabilities and insecurities for the European economies. As a reaction the Union legislator established the established 'Banking Union' with the 'Single Supervisory Mechanism' located at the European Central Bank and with the 'Single Resolution Mechanism' including a 'Single Resolution Fund'. Now the questions arises whether those measures were sufficient in order to prevent future financial and economic crises and, by that, future threats to the security and safety of the economic welfare in Europe. The table will address these issues and discuss future developments and reforms in order to protect the economic welfare in Europe.

Conclusions and recommendations

1. As systemic crises have real societal impact, financial market regulation and supervision is a matter of safety and security.
2. Providing safety and security in the face of globally integrated financial market calls for supranational (European) and international solutions. Financial institutions can no longer be allowed to be 'international in life, but national in death.'
3. In providing safety and security public interests must be carefully balanced with private & individual interests.
4. Providing safety and security in Europe calls for more 'countercyclical' policy thinking by scientists and regulators.
5. The many facets of financial markets integration call for an interdisciplinary approach both in defining the challenges that society face in this regard, as well in formulating sustainable solutions.

THEME: GOVERNANCE OF SECURITY

Introduction: Dr. Bibi van den Berg, Associate professor of Law and Digital Technologies, member of the Dutch Cyber Security Council, Leiden University

Description

The internet has become a critical system in our economic and social lives. Due to its open and flat character is has grown to be the number one enabling technology of our time in only a few decades time, reaching a global character and connecting people all over the world. The same factors that were at the root of the internet's success, however, at the same time raise important questions for governance, regulation and law enforcement. Because of its global reach the internet knows no borders. This clashes with the ways in which we have traditionally organised governance and law and regulations in the physical world, viz. mostly along territorial lines. Whose laws apply in cyberspace? Who gets to rule this global domain? And what legitimations do states and non-state actors (e.g. companies) have to claim control over this domain? A related issue is that of jurisdiction and attribution. Due to its flat and open character it is relatively easy for individuals with bad intentions to commit criminal acts and remain anonymous, even from the other side of the world. Anonimity and the network character of the internet make it very difficult to track and trace perpetrators, let alone arrest them and get them extradited. With the rise of the importance of the internet as a vital system in our everyday lives, however, it is paramount that we find ways in which to overcome these thorny issues. One of the key obstacles in the area of cybersecurity governance and regulation is a lack of clarity at the conceptual level: we use concepts such as 'cyber warfare', 'cyber terrorism' and 'cyber espionage' to distinguish between different types of cyber security threats, but it is very difficult to make clear distinctions between these categories, both theoretically and practically. This is a point of concern, because we cannot develop adequate protections and responses (laws, regulations, policies) if we cannot pinpoint the problems we are seeking to solve. There is a clear role for the EU to make steps in taking the governance and regulation of the internet forward, to ensure a safer internet for citizens, organisations and businesses.

Conclusions and recommendations

1. Municipalities need to play an important role in creating awareness for citizens. Education is crucial! But also the 'drop outs' or older people should be educated. The Hague would like to be a testbed for this and host the International Cyber Council.
2. Municipalities can empower the government. It has to be taken into account that different cases need a different approach. Critical infrastructure is a governmental issue.
3. PPP is crucial. The different roles have to empower the country and make sure the welfare and prosperity is provided. Trust is crucial.
4. We worry if the EU has the "power" and the "speed" to answer the difficult question we already have and lay ahead of us. Harmonisation of laws is key?
5. Survival of the fittest! Not only within a country (smart cities) but also between countries.
6. We suggest we start with international norms. Laws are too slow.
7. The EU needs a level playing field changing the mind set! Politicians/leaders also need a change of mind set.
8. All EU countries need a Cyber Security Council (Public/Private/Academia): with mandate!

THEME: TERRORISM AND COUNTERTERRORISM

Introduction: Prof. Edwin Bakker, Director of Centre for Terrorism and Counterterrorism, Leiden University

Description

Terrorism has arguably been one of the defining factors of our age. In many parts of the world, including in Europe, it has been one of the most important threats to peace, security and stability. But what exactly is the nature of this threat? What can be done about it or how can we at least limit the impact of terrorism and the radicalization process that is thought to precede it? Specific questions that need to be addressed in a European context are at least threefold. The first question deals with measures to tackle foreign fighters: European citizens who travel to the Middle East, fight in the Middle East, and in some cases return to Europe to continue their fight at home. Second, what to do with the potential security threat posed by those who stay at home, but clearly sympathize with extremist ideologies. A third pressing question that requires a pan-European approach is how to deal with radicalized individuals released from prison. Can extremists and terrorists be successfully re-integrated into society? What measures are available to curb recidivism rates? The table will address these and related issues and discuss future developments in the field.

Conclusions and recommendations

Background of "Jihad fighters"

In the Dutch case although the socio- economic backgrounds of jihad fighters is very varied, most of them come from broken homes and have low self-esteem. It could be that they are disengaged with the society around them. The perceived "ideals" of IS give them a new form of engagement. Research also showed that the trigger an individual actually embracing radicalisation is often connected to a life changing event. In order to prevent or to contribute to the prevention of radicalisation of young people the local fabric of a neighbourhood plays an important role; the local religious leaders, the local neighbourhood community policing; the local schools and other local organisations. There are also positive effects from urban renewal activities: clean streets, green parks, newly built housing, public transport.

Recruitment

The expert and appealing use of social media plays a strong role in recruiting Jihad fighters as well as other methods to appeal to or inspire youngsters. However, where does the fundamental democratic "right of freedom of speech" become a call for criminal activity and terrorist acts, making the voices into members of a criminal organisation with a terrorist objective ? In court this is very difficult to prove and there is a strong need to develop jurisprudence all over Europe. In the Netherlands and in Sweden there have been court cases in which jihadists have been convicted, which could serve as interesting examples to other EU Member States.

The state (national or European)

There is also a need for the state to be more unequivocal / unambiguous in upholding some principles of the state of law or non- legal values: Dutch nationals fighting in other countries for foreign rulers; the monopoly on violence by the state; freedom of religion and speech. It should work both ways: equally for issues the politicians and public opinion consider sympathetic good causes.

Europe: the whole situation of radicalization and terrorism has outgrown national borders and jurisdictions. The fact that the internet and social media are the main communication channels makes this a European affair per se. The adoption of the European Security Agenda in April 2015 marks the speeding up of European actions. On December 2, 2015 the EU adopted a package of measures to step up the fight against terrorism and the illegal trafficking of firearms and explosives. The package includes two main elements: a proposal for a Directive on Terrorism and an Action Plan for reinforced control of illicit possession and import to the EU to ramp up the fight against criminals and terrorists accessing and using weapons and explosives in the EU.

THEME: CYBER SECURITY

Introduction: Prof. Jan van den Berg, professor in Cyber Security, Delft University of Technology

Description

Despite the growing attention paid to cyber security, we are startled by new cyber incidents on an almost daily basis. An important condition for a genuine improvement of this unpleasant phenomenon is getting improved (local and global) cyber situational awareness. This relates to better insight in (upcoming) cyber threats/attacks as executed by all kinds of cyber actors (e.g., in the dark web), increased insight in Internet traffic patterns, in anomalous behaviour of computer processes (e.g., related to financial transactions), in computer systems' vulnerabilities as exploited in previous and possibly future incidents, among others. It is clear that a better overall picture of what's going on in cyberspace can only be achieved by effective (big) data & information sharing between all kinds of stakeholders, which also poses a lot of dilemma's related to, e.g., security versus privacy, transparency versus reputation loss, security costs versus benefits. Scientific studies using various scientific approaches are needed related to these cyber security challenges. Topics to put on the research agenda include computer science studies (e.g., on cyberspace monitoring & analytics, development of an ontology of key cyber & cyber subdomains/critical infrastructures terms, effective detection of software zerodays and of vulnerabilities in SCADA systems), institutional economics studies (e.g., on the design of incentive structures for cooperation between cyber security actors, design of national and international cyber governance institutions), law studies (e.g., on rights and duties of cyber stakeholders, on rules & regulations on law enforcement, cyber warfare, and international cyber security cooperation), and ethics studies (e.g., on balancing privacy and security, and on privacy and big data). The outcomes of this studies will provide decision support for relevant cyber security actors and politicians in order to create a safer cyberspace.

Conclusions and recommendations

1. Politics should facilitate Public-Private-Partnerships (around Cyber Security) at European level (important for trust and standards). We have to be able to provide European alternatives to products and services from other continents, to reflect the European legal and cultural identity.
2. To enable adequate Cyber Risk Management, the creation of Cyber Situational Awareness is key at:
    - IT level
    - socio-technical level
    - governance level

Parliament needs more cyber awareness too. The role of the state as provider of security should include cyber. We need "Basel" type of requirements for cyber. Are we making optimal use of SME's in agenda setting, PPP etc? Do we help SME to find the right doors? Do we make enough effort to include SME in consortia? This is important because SME provide the lion share of the European productivity.

THEME: CHEMICAL SAFETY AND SECURITY

Introduction: Prof. Genserik Reniers, Professor of safety of hazardous materials, Scientific Director of the Leiden-Delft-Erasmus Centre of Safety and Security, Delft University of Technology

Description

Multiple concerns arise in modern societies, namely increasing technological complexity, challenges of a global market, rising frequency of severe natural events and increasing societal vulnerability. The impacts on the population of such combination of new threats and hazards is potentially amplified by the strong multi-sectorial dependence of specific critical infrastructures. Chemical industrial parks, also called Seveso sites in Europe, store or process high quantities of hazardous substances. The involvement of Seveso sites/areas in crisis scenarios may escalate the impact of cascading events, either deriving from external threats as natural hazards or intentional interference (terrorist attacks), or by internal causes. Population and safety and security officers need an increased awareness of the potential impact deriving from such scenarios. Seveso sites have specific factors for the prevention of scenarios, as well as factors that influence resilience and response to crisis. The scope of conventional approaches to the safety and security of complex systems needs to be widened to include the specific scenarios involving Seveso sites/areas. The consolidated approach and tools available for the assessment of the impact of major accidents at Seveso sites, developed to address hazards as required by the Seveso Directive, needs to be revisited and integrated in a holistic assessment of external and internal threats. Consequence and impact assessment should be extended to consider cascading events that, through multi-sectorial dependencies and indirect impacts, may affect different entities of the society. Awareness needs to be created among population and safety and security managers of chemical parks.

Conclusions and recommendations

1. Member States should make national implementation plans regarding (chemical) security, based on EU security directive (which is not existent yet).
2. We are lacking methodologies (tools, methods and techniques) to integrate (cyber) security and physical security and to integrate physical safety and security.
3. Unlike the SEVESO directive that promotes full transparency regarding chemical activities, transparency regarding chemical activities and safety should be balanced with security in terms of responsible disclosure (related to the right to know act (Copenhagen 1998). Be careful who has access to what type of (chemical) information.

These recommendations become even more relevant in light of the acts of terror this summer in France, in which attempted terrorist attacks on the chemical sites of AirProducts (25/6) and Lyondell Basel (14/7) took place. These attacks are no weak signals any more, but severe warning signals. Therefore, an impulse is needed in chemical security issues, from an authority/legislative viewpoint, an academic/research perspective, and in industrial practice.

THEME: MICROBIAL SAFETY IN HEALTH CARE

Introduction: Prof. Margreet Vos, Professor in Medical Microbiology, Infection Prevention, Erasmus Medical Centre Rotterdam

Description

With increasing antimicrobial resistance in micro-organism the future will be quite different in respect to infectious diseases; the future patients will be older, more (immuno)-compromised with complex underlying diseases and as a result get more frequent and complex invasive procedures and antibiotic treatments. People are travelling more frequently and patients will be increasingly asked to get their treatment in different health care centers or even abroad due to insurance company policies and the free market principle. Infectious diseases are different from other diseases, because microorganisms always transmit to other persons or the environment. Therefore, infectious diseases are not just about the infected person, but involves by transmission the threat to others as well. Resistant microorganisms lead to difficult to treat infections. As different European countries has different infection prevention policies and therefore different numbers of infections by resistant microorganisms, for low incidence countries the future will bring an increase of the risk on resistant microorganisms. If we do not prevent these resistant microorganism in and between different countries, we all will end up in the pre-antibiotic era.

To prevent this, a few questions should be addressed:

1. What are the sources and reservoirs of highly resistant microorganisms (HRMO) and how can we prevent these HRMO entering the human field from the animal field, passing the country borders and entering health care institutes. How can we improve antibiotic stewardship in the human and animal field and prevent transmission in health care centers to keep the chance on infection low.
   Call for action: As microorganisms travel with persons and transmit to others, we all (countries, communities and centers) have a responsibility in sending and receiving microorganisms to and from each other.
2. To optimize the right and timely prevention measures, how can we keep each other informed about known HRMO-infected patients when patients are moving between health care centers and ambulant care, keeping in mind the privacy of the patients and their data. Is sharing between caregivers of information about carriers of resistant microorganism more important than the individual right on privacy?
   Call or action: How to overcome these privacy issues on selected patient data.
3. How should we design and build healthcare buildings which are optimized for a clean and safe healthcare environment. Can this knowledge ultimately lead to European guidelines on microbial safe health care buildings?

Conclusions and recommendations

1. To prevent transmission of microorganisms in health care centres we need safe-care-buildings. In different, but not all, European countries, national guidelines are available. However, up until now there are no European directives on designing a microbial safe building and environment of health care centres. This should be developed to ascertain a unity of quality.
   Discussion:
   Health care is the Member States initiative, EC coordinates. It was agreed that design forces people to act properly. But health care is a national responsibility. We should take the initiative. Question: who is developing standardisation.
   Conclusion:
   Needed: To start with a national (Dutch) initiative to guide the microbial safe health care centres and finally end up with an EU directive on microbial safely built health care centres.

2. To prevent transmission of microorganisms between health care centres we need information on patients carrying these microorganisms.

   Discussion:

   This initiate a lively discussion on privacy and population risks. Data protection is renewed now. It should start with a number of centres united in an electronic regional or even national health system that alarms all included centres. Another way to answer this issue is a study or goal on notifying each other with respect to restrictions as given by law. This remains an unresolved issue with a noticed urgent need for sharing information.

   Conclusion:

   Needed: A solution to overcome the privacy issues on sharing selected patient data with health care workers from different centres to prevent other patients from getting infected.

3. *To* assure quality in infection prevention in health care, we need a uniform quality standard like an ISO norm.

   Discussion:

   add again the proposed art.5 (as was in one of the concept-directives) on the point of safety/quality required in the directive of the right on cross border Medical Centres. This issue should be resolved in the same way as discussed for the first item; the Netherlands can have the initiative, to be successful, search for as many partners as possible in the member states. You have the right to take the initiative. New programme on antimicrobial resistance: point on this agenda.

   Conclusion:

   Needed: an international norm on quality of organizations of infection prevention in health care centres.

THEME: SECURE PORTS AND TRADE LANES

Introduction: Prof. Rob Zuidwijk, Professor of Ports in Global Networks, Scientific Director Leiden-Delft-Erasmus Centre Metropolis and Mainport, Erasmus University Rotterdam
Prof. Yaohua Tan, professor of Information and Communication Technology, Delft University of Technology

Description

The Leiden, Delft, and Erasmus Universities have joined forces in the Centre Metropolis & Mainport, where the focus is on the following themes: (1) Sustainability; (2) Synchromodality; (3) World Port City; and (4) Secure International Trade and Global Clusters.

The fourth theme puts forward the following two questions:

1. How to ensure secure trade lanes by means of data pipelines, e.g. cloud-based IT networks for data/message exchange, that support supply chain management and trade facilitation?
2. What is the role of the various stakeholders in supporting secure ports and trade lanes? What are synergies and trade-offs?

One of the LDE initiatives is the Executive Master on Customs and Supply Chain Compliance. Students involved in the program are tax and customs officials, from border inspection agencies as well as industry that engage in compliance issues. The above questions play a very important role in the program and in a number of EU projects in which LDE researchers have been involved (INTEGRITY, CASSANDRA, CORE, ITAIDE).

We invite stakeholders involved in securing ports and trade lanes both from industry and border inspection agencies to engage in discussing questions as the above.

Conclusions and recommendations

Since the beginning of this century, the European Commission in Brussels has increasingly freed up resources for projects related to logistics and supply chains. Dutch parties are closely involved with such projects. Up until now, the developed and acquired expertise primarily made its way to participants in the consortium and, through educational embedment, to universities, universities of applied sciences and institutions such as Dinalog. The universities of Leiden, Delft and Rotterdam often assume a leading role in these projects, in close collaboration with the Dutch Customs authorities and business community. The Dutch participants in active European projects such as CORE (€50 million with a 60% EU contribution) and CASSANDRA (€15 million) aspire to dramatically increase efforts regarding the dissemination and utilisation of expertise, as this is both a Dutch and a European concern. In the Netherlands, activity will be concentrated on initiatives including the Logistics Top Sector innovation programme, which aims to boost national competitiveness through demand-driven research. With regard to Europe, it moves beyond improving competitiveness to focusing on intrinsic objectives such as enhancing transport chain circulation, transport system safety & security and improving the reliability of information about the EU's own resources. Participants of the Secure Ports and Trade Lanes round table have concluded that the Netherlands can fulfil a significant role in improving the reliability of information in the transport chain, facilitated by the development of a global logistics internet. Essentially a cloud solution, benefitting not only companies, but also governmental organisations such as Customs and the inspectorate. Universities can also offer a significant third party contribution to its success through the combination of research (return on investment within 1 to 4 years) and converting this research into education (return on investment within 5 to 7 years). Scaling up within Europe would be possible by sharing the model for innovation with other countries (France, for example, was mentioned) and the Europeanisation of the Customs and Supply Chain Compliance Master's degree programme.

THEME: SAFETY AND SECURITY IN CRITICAL INFRASTRUCTURES

Introduction: Prof. Pieter van Gelder, professor in Safety and Security Science, Delft University of Technology

Description

We live in a world of new technology; robotics, internet of things, wireless data via wearables, remote sensing from space, UAV's, social media and citizen participation for massive data collection, etc. At the same time we are being threatened by natural hazards, climate change, changing land use, security threats, cascading effects, etc. We can monitor flood disasters from satellites and update flood propagation models with social media messages from the public. We can measure ground accelerations via public participation with the xyz sensors of our smartphones, enriching instrumental data of seismologists. We can inform citizens during crises with geo-based text messaging, giving them much more information what to do, than old-fashioned sirens. Community policing via apps is possible to aid law enforcement with local residents. Our vision is that an integral, big-data based and multidisciplinary scientific approach, in a broader socio-technical context, incorporating technical, human and organizational factors, covering the full safety chain of proaction, prevention, preparation, repression and after care, as well as covering the full life cycle of plan, design, build, operate, maintain, dispose / reuse, can increase the overall safety, reliability and security of our critical infrastructures and as society as a whole. Empirical studies are needed to support this vision and to advise decision makers how to optimally use the abundance of various sources of data with the goal to increase safety and security. EU wide databases should be set up to collect data from large numbers of case studies, so that learning and evidence-based decision making becomes possible. Incentives should be developed to stimulate further public and private partnerships and to prevent possible negative influences of the big data trend.

Conclusions and recommendations

The EU critical infrastructures are all assets in our union which are essential for the functioning of the EU society and economy. Many of these assets, such as electricity transmission lines, flood defences, ICT communication, transportation systems, cross borders and disruption in one member state will immediately affect the functioning in neighbouring states. To keep the infrastructures safe and secure, the EU should enable:

- Harmonisation of technologies to protect infrastructures against threats (intentional and unintentional)
- Standardization and legislation towards safety and security of infrastructures (for instance by probabilistic criteria; to ensure a safety / security level of failure only once per 10.000 years)
- The use of big data, remote sensing, and public participation in data collection, as leading indicators for possible failure mechanisms developing in critical infrastructures.

Big data developments have an enormous potential to predict and detect possible undesired events, but at the same time it is realized that it may impact privacy and liberty of people. It is therefore recommended to investigate privacy preservation techniques and to find the balance between safety and security improvement versus privacy preservation.

Rather than the actual data of incidents itself, it is more important to see the connection between objects and incidents. Using DOI's (digital object identifiers) could allow a platform on which a meta analysis of data on EU level becomes possible. Questions related to open data are very important. Risk maps of dangerous infrastructures may inform the citizens to create risk perception and self-reliance in case of accidents. On the other hand, potential terrorists may also benefit from these open data sources. Also here, the balance has to be optimized and harmonized on EU level. Such overarching questions cannot be dealt with on a national level, because of the immediate cascading effects in case of failures.