



EFMN

WWW.EFMN.INFO The European Foresight Monitoring Network

Future Challenge for Europe: Providing Security and Safety to Citizens

Foresight Brief No. 134

Authors: Anette Braun (braun_a@vdi.de), Nils Elsner (elsner@vdi.de), Andreas Hoffknecht (hoffknecht@vdi.de), Sabine Korte (korte@vdi.de), Sylvie Rijkers-Defrasne (rijkers@vdi.de), Olav Teichert (teichert@vdi.de) – Future Technologies Division at VDI TZ

Type of Brief Overview

Date of Brief : Feb. 2008

Purpose

As stated in the recent EC Communication on ‘Reforming the budget, changing Europe’ (SEC (2007) 1188), the European Union has a key role to play in ‘providing security and safety to citizens’. Especially in the aftermath of 11th Sept. 2001 security related issues are becoming an increasingly important facet of global society and have an increasing impact on economy and science. The issues are manifold and include protecting citizens and state from organized crime, preventing terrorist acts, and responding to natural and man-made disasters. Civil security issues are becoming more and more important to governments and national economies across the globe, and the EU is no exception. The EC sees security research as an important policy objective, which started in 2001 with a Preparatory Action on Security Research (PASR) and is now the tenth theme of the FP7 Cooperation programme. Security and safety technologies are seen to have applications in many sectors including transport, civil protection, energy, environment, health and financial systems.

Analysing EFMN Documents: TextAnalyst

A selection of 160 foresight and futures studies was taken from the EFMN database. These were studies with different backgrounds, scopes, themes, horizons and on different scales. The semantic data-mining tool ‘TextAnalyst’ was employed to analyse the texts. First, out of the 160 studies, a small number of relevant studies was selected that had titles strongly related to the researched topic. TextAnalyst analysed these texts and found the most relevant keywords and semantic relations between the most important words. These terms were compiled into a keyword list for the researched topic. This list of keywords was used to analyse all 160 selected studies. The TextAnalyst yielded all sentences containing any of the keywords, with an additional hyperlink in the text file allowing to view the context in which the sentence occurred. The TextAnalyst also gave a semantic relation between the searched keywords and other words. The related terms thus identified were added to the list of keywords. The summary of sentences that contained one or more words from the list of keywords was

manually read in the original context and if the sentence or the section where the sentence occurred was regarded as providing new or additional information, this section was copied into a text file. In order to avoid any extreme out-of-context copying of sentences, statements that were part of a scenario description were not added to the file. After this analysis of the 160 studies, a text file was created containing sections of the original studies with information related to the selected topic and the reference to the original document.

The dictionary for the analysis presented here consisted of the following terms: anticipation, crisis, defence, defence, emergency, enemy, intelligence, military, NBC, NRBC, prevention, protection, risk, safety, secure, security, surveillance, terrorism, terrorist, threat and weapon. This analysis is exclusively based on the review of 36 foresights and future-oriented studies completed between 2000 and 2007 – most of them in 2004-2005. While most studies were carried out at a national level in Europe, the pool of sources also included seven studies conducted at the EU-level, eight Japanese national studies, the global study AC-UNU Millennium project, the supranational study on information and communication technology (ICT) in the Nordic countries, and one Finnish study of regional scope.



Limitations of the Analysis

Attention should be paid to the fact that, while all 36 studies address certain safety and security issues, they are not all equally detailed. In particular, whereas some foresights (e.g. the UK Foresight) provide an in-depth analysis of the state-of-the-art of technology, as well as a detailed forward look, the significance of some one-sentence statements, as they are typically made in Delphi studies such as the 8th Japanese National Foresight, may be more limited. Such statements have been considered very carefully so as not to bias the analysis. From the above, it follows that the following analysis – based on a restricted number of foresights – neither intends to be exhaustive nor to provide an overview of security and safety-related issues weighted according to their importance for future EU policies. However, it might provide some interesting insights about future safety and security threats – as predicted in foresights – as well as how future technological, societal or economic developments and policies might help to combat them. Since some of the analysed foresights are quite old, this means that some of the proposed actions could already have been implemented.

Safety & Security: A Crosscutting Issue

Safety and security issues are generally related to all kinds of natural and human-induced (intentional and non-intentional) disasters or risks, which can affect individuals, societies or nations. Important technological and political tasks in the context of the protection of citizens and vital infrastructures have addressed a broad spectrum of issues such as future threats and vulnerabilities of critical infrastructures in key sectors (e.g. information systems, financial systems, industrial plants, public buildings, transport systems and infrastructures, communication networks, energy infrastructures, food distribution systems, etc) or the impact of terrorism and organized crime on the development of civil societies.

From the selected studies two major areas were identified bearing future risks for society: civil security and IT security. The area of civil security can be divided into subsections as follows:

- terrorism and crime prevention,
- ensuring the safety and security of critical infrastructures,
- food and chemicals safety, and
- threats from climate change and natural disasters.

Civil Security

Terrorism and Crime Prevention

Terrorism is expected to become a growing threat to all parts of society in the future mainly for two reasons. Firstly, due to the increasing dependence on computer networks, modern societies have become more vulnerable. Secondly, the proliferation of

NRBC (nuclear, radiological, biological and chemical) weapons, the proliferation of ballistic, tactical and cruise missiles, and, on another level, the proliferation of small arms, the use of technological objects (e.g. civilian aircraft) as weapons and the transfer of technical know-how have multiplied risk factors for our societies. Also terrorist activities are becoming networked and are increasingly seeking points of entry into international business and, through corruption, into public administration.

The threat from terrorism must be counteracted by increased international cooperation on all levels and increased spending for security.

Another aspect raised by the study by the Finnish Committee for the Future is that because of continued synergy among, and miniaturization of, everything from chemistry sets and pharmaceutical manufacturing to genetic and nanotech engineering terrorist attacks will be much simpler to conduct in the future. Eventually an individual (single individual being massively destructive, SIMAD), acting alone, will be able to create and deploy a weapon of mass destruction.

In the broader context of terrorism, general crime prevention is an important aspect. The Japanese studies suggest that the security provided by governments will deteriorate in the future; thus people must provide for their own protection. Means like physical access control and burglary alarm systems for private homes are seen to be possible substitutes. The British study ‘Strategic Futures Thinking’ concludes that new technologies, such as DNA profiling, will prove increasingly vital in criminal trials as will more sophisticated detection, surveillance and monitoring devices in the wider field of crime prevention.

Safety and Security of Critical Infrastructures

Energy and transport infrastructures (so-called ‘critical infrastructures’) are crucial to economy and society. Therefore, it is hardly surprising that their safety and security is addressed in different foresights – at a national and supranational level. The Finnish foresight ‘Finsight 2015’, for instance, stresses the fact that modern societies have increasingly become vulnerable in the sense that any malfunctioning or failure of critical infrastructures may paralyse the whole society.

The foresights identify several threats to critical infrastructures:

- Critical infrastructures increasingly rely on ICT applications and they more and more depend on the reliability of broad and complex ICT networks. Protecting critical infrastructures is therefore closely related to protecting the *ICT networks* they are based on. In this regard, ICT liability has to be ensured; it will also be particularly important to prevent criminal intrusion and the misuse of networked-based infrastructures.
- Of course, on a global scale, terrorism is expected to remain one of the main threats in the future. Several foresights such as the Fistera study and the UK Foresight therefore focus on threats to aviation and possible means to combat them based on better identification systems (e.g. embedded codes in airline tickets and in luggage, allowing

matching them with the personal identification provided at the point of embarkation). Indeed, the terrorism threat is expected to give further momentum to the development of specific markets such as imaging technologies (allowing for instance the detection of suicide bombers in case remote identification and containment become reality).

- Transport safety for citizens also implies reducing the risk of accidents. Thanks to the diffusion and increasing affordability of ICT, use of intelligent transport systems based on telematics as well as video-surveillance systems are expected to become more widespread to improve transport safety, for instance, by reacting in case fatigue, recreational drug use or medication impair the performance of the driver of a car or the pilot of a plane. Intelligent transport systems may also help maximise transport and logistics efficiency leading to benefits in terms of increased productivity and economic growth.

Food and Chemical Safety

Quite surprisingly, and despite their relevance for everyday life and everyone's health, issues related to food safety is rarely addressed by the foresights screened. Some, however, do highlight that ensuring food safety requires assessing the long-term impact of harmful chemicals (e.g. heavy metals) on human beings, crops, as well as livestock. Food safety is therefore closely related to preventing damage to the environment due to chemicals in general. Standardized and socially approved tools for the risk assessment of chemicals should hence be developed. In this regard, chemical analysis is expected to be facilitated in the future through the use of miniature chemical analysis systems. Regarding functional foods, the monitoring of the long-term consequences of their use is underscored as essential. The EU may have a role to play in assessing health claims and the safety of new functional food products entering the market. Providing transparent information on health issues, safe threshold limits for specific functional food products, as well as on storage requirements will also contribute to promoting food safety for the consumer.

Threats from Climate Change and Natural Disasters

Some studies emphasize the risk from climate change and natural disasters. Particularly in Japan the risk from natural disasters such as volcano eruptions, avalanches and earthquakes is addressed. The development of new predictive systems is proposed. Systems to observe disasters such as communications satellites, GPS, unmanned aircraft, and so on should be implemented in order to better understand situations after disasters have occurred and to be able to respond more swiftly.

Nearly all studies addressing climate change raise the issue of flooding – often in connection with the expected rise of the sea level. For instance the UK Foresight study claims that climate change will have a high impact under every scenario due to two threats. Firstly, the coasts are expected to be especially at risk: relative sea-level rise could increase the risk of coastal flooding

by four to ten times. Secondly, precipitation is expected to increase flood risks across the country by two to four times. Flooding in towns and cities will be one of the greatest challenges in the future. Building in areas at risk from flooding should be avoided or, if inevitable, space should be provided to accommodate flooding in river and coastal areas. In this context, the development of effective modelling capabilities to predict flooding and manage flood routes in intra-urban areas should be pursued.

The study by the Finnish Committee for the Future also expects that change in precipitation will result in water tables falling on all continents. Droughts in areas where 40% of the population depends on watersheds controlled by two or more countries call for new water management strategies that can mitigate the effects of migration, conflicts, etc.

The threat of storm surges in coastal areas will increase due to rising sea levels combined with changes in the number, location, and strength of storms.

Although flooding is seen as one of the main challenges of the future, at the same time, it is also acknowledged that predictions in this area are steeped in uncertainty, as in the case of climate change or demographic and socio-economic trends. Thus, one has to develop robust water management strategies that will yield satisfactory living conditions for a wide range of possible scenarios.

IT Security

IT security in general is seen as a major topic of the future. Society depends on vulnerable, complex information technology systems, which need to be protected.

One major issue is the protection of privacy in the sense of protection against loss of control over one's personal data. Already nowadays, Wikis and mostly blogs may contain data and information about an individual that could easily be disclosed to unauthorised others, given the low levels of security and privacy protection implemented so far. This risk will be enhanced in the future because of the widespread use of ambient intelligence (AmI) with its heterogeneity (in contrast to closed, codesigned systems), its complexity of hardware and software (introducing the dependability challenge), its distribution of knowledge and resources (co-operation and inter-connection), as well as the foreseen mobility needs (which introduces more vulnerability than in a static world). Radio frequency identification (RFID) implants in people can also cause a threat to privacy, since they permit easy and instantaneous identification and authentication of individuals. On the other hand, they can increase security, for example, by enabling parents to easily track down their children in case of abduction.

The major challenge is to balance privacy and security needs. There are various ways to protect privacy in the future. Legislation to protect data of a personal nature is one of them. Another is by implementing new security measures. The level of privacy and security will be defined more by the location from where data are accessed than by the place where they are actually physically stored.

Another fast-growing area will be the provision of trust and guarantee services in the payments markets. A suggested new measure is establishing a clearinghouse where banks can anonymously share information about security breaches. Also, telecommunication companies are increasingly offering payment services. The introduction of m-payment systems will require new risk management systems and co-operation between different providers. It also calls for improved protection

of confidential data provided by customers. Although wireless networks already provide a more secure network than the ones offered in fixed-line markets, there is need for further measures. Among those suggested are enhanced use of digital signatures (a kind of unique electronic stamp), authentication and encryption. One study suggests replacing binary network security (access or not) by more complex security mechanisms thereby granting differential access to different actors.

Three Prevailing Issues

Taking the limits of the applied methodology into account, the analysis of 36 foresights and future-oriented studies, which were completed between 2000 and 2007, yielded three major security and safety issues: terrorism, IT security and natural disaster protection in the context of the global climate change. Concerning terrorism, studies seem to perceive growing future threats to all parts of society mainly because of modern societies' increasing dependence on computer networks and critical infrastructures and also because of the growing proliferation of NRBC agents, ballistic missiles and small arms. In the broader context of terrorism general crime prevention is also an important aspect.

IT security in general is seen as a major concern of the future. Important issues in this field are related to the protection of privacy in terms of protecting against the loss of control over personal data and to the containment of future risks connected with the widespread use of ambient intelligence (AmI), RFID chips or wireless networks. The studies addressing natural disaster protection predict rising global threats of climate change causing flooding, storms and other weather anomalies in the future. Such studies also expect that the change in precipitation will result in water tables falling on all continents, which calls for new water management strategies capable of mitigating the effects of migration, conflicts, etc.

Sources and References

- 'Reforming the budget, changing Europe – A public consultation paper in view of the 2008/2009 budget review', Commission of the European Communities, SEC(2007)1188 final, Brussels, 12.9.2007.
- 'Meeting the challenge: the European security research agenda', report of the European Security Research Advisory Board, September 2006.
- 8th Japanese Foresight – Agriculture, forestry, fisheries and foods (2005)
- 8th Japanese Foresight – Electronics (2005)
- 8th Japanese Foresight – Environment (2005)
- 8th Japanese Foresight – Frontier (2005)
- 8th Japanese Foresight – Information and Communications (2005)
- 8th Japanese Foresight – Manufacturing (2005)
- 8th Japanese Foresight – Social Technology (2005)
- AC-UNU Millenium Project – Antiterrorism Scenarios (2005)
- Austrian BMVIT Safety and Security Research 2011 – EFMN Brief 33 (2005)
- Dutch NRLO – Functional Foods Position and Future Perspectives (2001)
- EC Ambient Intelligence in Everyday Life (AmI@Life) (2003)
- EC High Level Expert Group (HLEG) – Foresighting the New Technology Wave - Converging Technologies - Shaping the Future of European Societies (2004)
- EC IPTS – Digital Territories (2007)
- EC IPTS – The Future of M-payments (2001)
- EC IPTS-ESTO – Future Bottlenecks in the Information Society (2001)
- EC IPTS-ESTO Roadmapping Project – Healthcare Technologies Roadmapping – The Effective Delivery of Healthcare (2003)
- Engineering and Technology 2000 – Trends on Transports (2002)

- Finnish Committee for the Future – Democracy and Futures (2006)
- Finnish ESF – Uusimaa 2035 Scenario Project (2004)
- Finnish TEKES – FinnSight 2015 (whole exercise) (2006)
- FISTERA – Key European Technology Trajectories - 2nd Report (2004)
- French FutuRIS (2004)
- French Ministry of Defence – PP30 – Prospective Plan of the French Defense Policy in 30 Years (2004)
- Turning the Water Wheel Inside Out. Foresight Study on Hydrological Science in The Netherlands (2005)
- UK DEFRA – Climate Change Scenarios for the United Kingdom (2002)
- Greek National Technological Foresight (Whole Exercise) (2005)
- Ireland Marine Foresight (2005)
- Japanese Optoelectronic Industry and Technology Development Association – Optical Technology Roadmap (2003)
- Nordic Innovation Centre – ICT Foresight – Nordic foresight and visions on ICT in healthcare, security, the experience economy and production systems (2005-2007)
- Strategic Futures Thinking – meta-analysis on published material on drivers and trends (2001)
- UK National Foresight – Cyber Trust and Crime Prevention (2004)
- UK National Foresight – Exploiting the Electromagnetic Spectrum (2004)
- UK National Foresight – Flood and Coastal Defence (2004)
- UK National Technology Foresight Programme – Foresight IT 2000 (2000)
- UK National Technology Foresight Programme – Foresight Financial Services (2000)
- UK National Technology Foresight Programme – Crime Prevention Panel (2000)

About the EFMN: Policy Professionals dealing with RTD, Innovation and Economic Development increasingly recognize a need to base decisions on broadly based participative processes of deliberation and consultation with stakeholders. One of the most important tools they apply is FORESIGHT. The EFMN or European Foresight Monitoring Network supports policy professionals by monitoring and analyzing Foresight activities in the European Union, its neighbours and the world. The EFMN helps those involved in policy development to stay up to date on current practice in Foresight. It helps them to tap into a network of know-how and experience on issues related to the day to day design, management and execution of Foresight and Foresight related processes.