Technological Forecasting & Social Change 101 (2015) 226–237

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

Emerging technologies in civil security—A scenario-based analysis

Antje Bierwisch [*], Victoria Kayser, Erduana Shala

Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Strasse 48, 76139 Karlsruhe, Germany

ARTICLE INFO

Article history:
Received 19 January 2014
Received in revised form 23 May 2015
Accepted 21 June 2015
Available online 13 July 2015

Keywords:
Foresight
Scenario technique
Security technology
Technology assessment
Societal needs

ABSTRACT

Civil security is a major issue on the European policy level and for the European market as a future lead market. Civil security technologies and their implementation are generally characterized by high complexity, multi-stakeholder involvement and a high level of regulation. Due to these characteristics and the influence of societal aspects, it is extremely difficult to evaluate the future developments and applications of emerging security technologies. This is why only a small number of studies have addressed this issue so far and empirical insights into these aspects are still scarce. Our paper addresses this research gap by applying scenarios to consider different societal aspects and their impacts on emerging security technologies and their applications. Based on quantitative and qualitative data and are used as the evaluation background for emerging security technologies. The results show that this approach is suitable to consider technological and non-technological drivers and barriers, and to derive measures and recommendations. The paper contributes to research on technology innovation systems from a challenge-oriented policy perspective and gives new impulses for future research, especially in the field of civil security.

1. Introduction

Civil security is a central topic in security policy programmes and for domesticstrategies. At European level, the "EU Internal Security Strategy in Action" (European Commission, 2010a) addresses the following identified key challenges to the security of the European Union: serious organized crime, terrorism, cybercrime, border security, and the management of natural and man-made disasters. Today, civil security is an essential aspect of European security policy since hazards, threats, and risks of heterogeneous origins are transferred into the same risk context. Furthermore, the issue of security research as an element of the grand societal challenges also plays an important role within the European Framework Programme for Research and Innovation, HORIZON 2020 (European Commission, 2014). At the moment, there is still some concern that European security research funding focuses exclusively on business and technology and not on solving societal challenges. A foresight approach may be one way to not only address the grand challenges of the future, but also consider such evolving concerns.

Civil security technologies are generally characterized by high complexity, multi-stakeholder involvement, and a high level of regulation. Due to these characteristics and the influence of societal aspects, evaluating the future developments and applications of emerging security technologies is a difficult and complex process. Existing methods of technology evaluation have two major weaknesses: they tend to focus on technology or user aspects rather than on analysing the problem in an integrated way and are often not future-oriented in a long-term frame, but only analyse the current situation. A foresight approach based on a systemic innovation understanding and the integration of heterogeneous aspects like ethics, the market situation, or the level of European integration could add further value (Dosi et al., 1988; Edquist, 2005; Lundvall, 1986). The evaluation process should consider technical details as well as the demand originating from society and the expectations concerning technologies. Especially where security technologies

[*] Corresponding author. Tel.: +49 721 6809 374; fax: +49 721 6809 330.
E-mail addresses: antje.bierwisch@isi.fraunhofer.de (A. Bierwisch), victoria.kayser@isi.fraunhofer.de (V. Kayser), erduana.shala@isi.fraunhofer.de (E. Shala).

http://dx.doi.org/10.1016/j.techfore.2015.06.014
0040-1625/© 2015 Elsevier Inc. All rights reserved.

are involved and, for example, the development of security measures, societal needs and concerns are of the highest relevance since the technologies might be rejected otherwise. A systemic approach that encompasses diverse aspects is suitable in the context of the evolving concept of security and preventive security policy (Bierwisch et al., 2012). These aspects include, for instance, demand and social aspects, political and framework conditions, industrial systems and infrastructures, the education and research system and their dynamics.

We chose the scenario approach combined with quantitative methods like patent and publication analyses as well as market studies to meet the challenges listed, derive actions and reflect upon emerging technologies in the light of different futures. The methodological approach used in this paper was primarily developed within the European research project ETCETERA.[1] In this project, global security scenarios provide the basis for evaluating the development and application potential of emerging security technologies. Each of the developed scenarios postulates a possible and realistic future situation regarding the global and specific key factors of the development and application of security technologies. For example, societal changes, the attitude in society towards technologies, market developments, global dynamics, civil security, European policy, and current trends in different fields of technology were taken into account. This means the approach focuses not only on the technical feasibility of new technologies; it also integrates different stakeholder perspectives by considering ethical and societal concerns at the early stage of technology research and development. This kind of evaluation allows holistic integration of qualitative criteria, quantitative data, interdependencies, and different stakeholder perspectives. Ultimately, this foresight methodology has the potential to support different stakeholders in policymaking, especially regarding critical topics that may determine and influence the future of societies.

The purpose of this paper is to illustrate how foresight methods, particularly the scenario technique, can be used for the evaluation of emerging civil security technologies. One objective of this paper is therefore to outline how the technical and non-technical drivers for and barriers to these security technologies can be identified at an early stage of technology development. Their impact on the future development and application potential of these technologies is also discussed. The specific research focus is on whether and if so how societal needs and concerns regarding technologies and their applications can be identified, addressed and taken into account at an early stage of the technology development process.

The paper starts by outlining the methodological background and briefly describing the core elements of foresight and the scenario technique. This is followed by the description of a security framework and specific aspects concerning emerging security technologies and the security market. The third section is devoted to the methodological approach as used in the ETCETERA project for the assessment of emerging security technologies using global scenarios as a systemic evaluation background. Based on this, examples of the results are presented and discussed in the fourth section. The paper concludes with a summary of the key messages.

2. Framework: foresight and evaluating emerging technologies

The consideration of user aspects and societal needs is a crucial element when evaluating technologies. According to the main perspectives of innovation (processes), a balanced view of both technology push and market pull is an essential factor for the success of a technology (e.g. Di Stefano et al., 2012; Mowery and Rosenberg, 1979; von Hippel, 1976). Currently, the technology development side within technology evaluation tends to focus on technological aspects, cost optimization and saving potentials. On the user side, there has been an upsurge over the past decades in the techniques used for analysing acceptance (e.g. Davis, 1985, 1989; Lin, 2003). Here, many different aspects like usability, privacy issues or health concerns are considered. But these techniques have two main limitations: First, their results focus mainly on a buy or use decision, and second, they lack long-term future orientation. The latter is important when assessing the application and development potential of emerging technologies. Another specific aspect for the selection of the evaluation approach is the nature of the security technology and the security industry field as mentioned above. A systemic approach is suitable for the specific challenges associated with security technologies. This is why we decided to use a foresight approach that combines the integration of technical and non-technical aspects, a long-term horizon, and the systemic analysis perspective.

Our approach is described in more detail in the next two sections. Section 2.1 introduces foresight principles and the scenario method and Section 2.2 addresses the specialities associated with security technologies.

2.1. Foresight and the scenario technique

For this work, the technology foresight concept (e.g. Martin, 1995; Martin and Johnston, 1999; Miles, 2010) is necessary because of the research focus in this paper—evaluating emerging technologies regarding their future development and application potential to enhance the European security market as well as the resilience of society. The technology foresight approach applied in the ETCETERA project is based mainly on the scenario technique, one of several foresight methods (e.g. Burt, 2007; Postma and Liebl, 2005; Schomaker, 1995).

Foresight is defined in many different ways. One suitable definition for the purpose of our paper is the following:

> *„[…] foresight is the process of developing a range of views of possible ways in which the future could develop, and understanding these sufficiently well to be able to decide what decisions can be taken today to create the best possible tomorrow."* (Horton, 1999, pp. 5)

Horton emphasizes the necessity of thinking in different possible futures in order to adapt to possible future developments by appropriate decision making in the present. We hold that foresight is a process that supports the exchange of information and discussion about technologies with future relevance for the whole of society by involving stakeholders. This method can lead to a common understanding of the concerns and needs of different perspectives with regard to emerging technologies. Furthermore, foresight can indicate

[1] ETCETERA—Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda, FP7 co-funded project Contract No. 261512.

advice and recommendations for innovation policy activities and policy planning.

In terms of technology-oriented foresight activities and programmes, technology foresight is one type of foresight activity. Technology foresight is defined as

> *"[…] the process involved in systematically attempting to look into the longer-term future of science, technology, the economy and society with the aim of identifying the areas of strategic research and the emerging generic technologies likely to yield the greatest economic and social benefits."* (Martin and Johnston, 1999, pp. 50).

So its main objective is to identify technologies with high potential/benefits for the future. This is of special interest regarding security technologies that often trigger heterogeneous problems and concerns among different actors. The attempt is also made to systematically assess

> "*[…] scientific and technological developments which could have a strong impact on industrial competitiveness, wealth creation and quality of life.*" (Georghiou, 1996, p. 359).

Therefore, technology foresight at a national level is seen as a strategic policy instrument used to generate an enhanced understanding of possible scientific and technological developments and their impacts on the economy and society. For example, this instrument can help to design suitable science and technology policies, align research and development with social needs and systemically develop long-term innovation systems (Salo and Cuhls, 2003). Both technology push and demand pull can be considered in technology foresight approaches and are part of the process applied in this work.

When dealing with technology foresight, a wide range of methods can be used like the Delphi method, publication and patent analysis, and roadmapping (Cuhls, 2008, pp. 12–13). In this case, we identified the scenario technique as suitable for implementing the outlined objectives like bringing together technological and non-technological drivers and barriers, or considering societal challenges and stakeholder needs. Scenarios are not a tool to be used for making predictions about the future, but to show how the future might develop and evolve. As such, scenarios are descriptions of possible, diverse and plausible futures. Thinking of possible future events helps to be prepared if they occur. To compile those future pictures, a complex system of influencing factors is developed and many different dimensions are integrated (Wilms, 2006, p. 39ff.).

Hence, scenario thinking is based on two main principles: multiple futures and network thinking (e.g. Gausemeier and Stollt, 2008, p. 50). On the one hand, the aspect of multiple futures allows different development possibilities for the future. This takes into account that the future is not exactly predictable. On the other hand, the future is described in complex pictures, so it is not sufficient to describe the environment as a simple system. Instead, it is necessary to take a systemic view into the future through networked thinking (Gausemeier and Stollt, 2008). The scenario method allows any desired scope to be set. Scenarios can be used for a specific context within an enterprise, for a region, state or even a global context, as was the case in the ETCETERA project (e.g. Godet et al., 1994; Graf, 2000, pp. 13–34). These global scenarios that cover various aspects the perspectives of different stakeholder are used here as a systemic evaluation background for emerging security technologies. As the ETCETERA project had a specific focus on security technologies, it was agreed to speak of 'global security scenarios' for the methodological process applied here. In this sense, global security scenarios focus on the surrounding factors which may have a direct or indirect influence on the future development and application of security technologies.

2.2. Characteristics of emerging security technologies—economic, political and societal aspects

As mentioned previously, the specific characteristics of emerging security technologies (particularly multi-stakeholder involvement, high complexity, a high level of regulation and certification and the influence of societal aspects) make it extremely difficult to assess their future development and application potential. This section briefly describes the characteristics of security technologies and the security market as well as the relevant framework conditions like societal requirements. These aspects are relevant for developing the methodological approach and for showing the circumstances and interactions of elements within an innovation (technology) system.

At a European level, the Internal Security Strategy addresses the identified key challenges for the security of the European Union: serious organized crime, terrorism, cybercrime, border security, and the management of natural and man-made disasters (European Commission, 2010a). Today, civil security is an essential aspect of the European security policy since hazards, threats, and risks of heterogeneous origins are transferred into the same risk context. For example, for the first time, civil security research forms a separate topic within the 7th EU Research Framework Programme. The objective of this research programme is to develop new technologies and suitable accompanying measures to more effectively protect Europe and its citizens from the threats and hazards mentioned above. At the same time, the programme aims to strengthen the competitiveness of European companies and the security industry.

The growing importance of security technologies, products and services is due to the fact that the concept of security has undergone a fundamental change over the last few years (Hough, 2004). It has evolved from its original application in a military context to civil security that increasingly integrates safety aspects. Because of the changing concept of security, qualitative and quantitative changes can be observed on the market level of security technologies (e. g. Bierwisch et al., 2012; Buzan and Weaver, 2009; Christou et al., 2010; Daase, 2011). There is a growing significance of the analysis of security technologies and systems and their cross-cutting functions. For example, energy and transport networks, internet and communications, food and water supply, and health care are viewed as fundamental fields of security. Therefore, security technologies are characterized by their cross-cutting nature and complexity. For instance, potential products and services are produced with the help of basic technologies like information and communication technologies, nanotechnology, optical technologies, sensors and biotechnology. This complexity is also reflected on the demand and supply sides. Besides economic sectors like the automotive industry, engineering, banking and insurance etc., the customer structure of the security market is also characterized by a significant share of government institutions and public policymakers (for further examples see, e. g. Bierwisch et al., 2012). Last but not least, the demand for security technologies is often established by legislative requirements (BMWi, 2010). Consequently, cross-institutional decision making processes and the involvement of different actors are major challenges in the security market.

Over the last years, Europe has developed its own security market and civil security has become more important in EU policy and funding. According to the Security Industrial Policy of the European Commission (2012a), the security industry is seen as a sector that will grow significantly in the next few years and will provide more jobs. Specific features of the current security market include its high fragmentation (also one of its main problems), the fact that it is an institutional market to a high degree, and its social relevance, because security is now viewed as a human need that has to be satisfied most urgently (European Commission, 2010b, p. 27). The market uptake of a technology is also difficult to predict because of the gap between research and the potential market. Within the next few years, greater harmonization and standardization will be needed to solve the fragmentation problem; the first examples include airport screening equipment and alarm systems (European Commission, 2012a, 2012b).

Finally, it is also an objective of the European Commission to integrate societal issues and concerns into technology development at an early stage in order to reduce problems with product take-up and lead to a more efficient use of R&D investments (European Commission, 2012a). Concepts discussed in this context are, for example, “responsible research and innovation” or the specific “privacy by design” and “privacy by default” (Cavoukian, 2009; von Schomberg, 2011). This is due to the special characteristic of security research and technologies—their societal depth of penetration. Emerging security technologies have the potential to cause changes and shifts in social structures, for example, through new forms of governmental or social control (Hirsch, 2008). Therefore, the fast technological innovations in this field and the associated social transformation processes result in new challenges that have an impact on the development and application potential of technologies. Furthermore, existing research findings illustrate that similar social challenges are perceived differently in different contexts. The same so-called threats and hazards like climate change, economic crisis, and terrorism may be discussed and handled quite differently. For example, integrating security measures in different countries at a specific location like the security scanner at airports has different impacts on social demand and acceptance (Nagenborg, 2005, 190ff.). It would be misleading to presume technological determinism when security technologies are considered as satisfiers for security needs. Security technologies neither evolve autonomously nor shape society, as they are the means to the specific end of security. As Nagenborg (2005, 2009) says, the legitimate use of a security technology in a particular place does not imply anything about its use elsewhere, and to quote Lowrance (2010), “[…] developing technologies is by no means value-neutral […]”.

In short, when evaluating security technologies, and especially the emerging ones, some specific points need special consideration. Firstly, security technologies have the potential to cause more problems than other technologies, especially in regard to policy, legislation, and society. This is due to the fact that security technologies address or affect basic needs which may also have the status of being a human right that has to be protected (Streeten, 1980). Secondly, special attention has to be paid to the market structure, the cross-cutting function of security technologies on the supply side and the heterogeneous community on the demand side. Thirdly, other aspects of security technologies concern the market fragmentation and the identified gap between research and the market.

3. Systemic evaluation of emerging civil security technologies

The development paths and proper fields of application are usually unknown for emerging technologies and are therefore an ideal field for foresight activities since they involve uncertainties and different problems and challenges. The decision in favour of such a methodological approach is also supported by foresight's possibilities to integrate influencing factors from different dimensions and to consider different stakeholder perspectives at the same time. By using foresight, the challenges of emerging security technologies can be identified and addressed at an early stage of the technology development process. This, in turn, allows market potentials to be recognized and exploited in a timely manner. The social and societal impacts concerning security technology research and development as well as related ethical and legal aspects demand a systemic perspective. Due to the high dynamics and complexity of the issues involved, a scenario approach is needed to analyse the security field. Only by combining this qualitative approach with quantitative methods like publication and patent analysis as well as the analysis of market studies can the analysis of such a dynamic and elusive sector be realized.

In the ETCETERA case presented in this paper, the special characteristics of the security field, security technologies and the security market are represented by global security scenarios which take heterogeneous aspects into consideration. An overview and a summary of the steps taken are provided in Fig. 1.

For each of the technologies, drivers and barriers are identified and then the technology as well as its drivers and barriers are projected into the future scenarios. Within each scenario, different combinations of key factors are encountered, so different evaluation frameworks result. From these frameworks, consequences are derived for considering which recommendations can be made at present and which possible measures and actions can be taken to prepare for future challenges. We developed a workshop concept for this assessment process (step 2 to step 6). This approach has three main building blocks. First, emerging security technologies are identified. The requirements concerning the identification of emerging security technologies are described in Section 3.1. The identification of the technical and non-technical drivers and barriers of the specific technologies is explained in Section 3.2. Second, specialized global future scenarios are developed; this process is described in Section 3.3. Finally, the scenarios and the identified technologies are brought together and an exemplary evaluation is shown in Section 3.4.

3.1. Identification of emerging security technologies

Emerging security technologies are those currently at the development level with a realistic application potential by 2020–2030. Furthermore, they are characterized by their relevance for security issues and an expected future demand which implies they will have a high impact on economic competitiveness and social welfare.

Within the ETCETERA project, various methods were used such as patent analysis, publication analysis and desk research that led to the identification of the technology areas of communication technology, energy technology, environmental security technology, human machine interface or sensor technology, and specific topics within these. Aspects like the time frame, security relevance (impact on future security issues, mainly driven by security demands), application potential, market potential, and ethical rating (e.g. privacy issues) were considered in the selection process that was accomplished by technology experts. The result of this task was a prioritized list of 30 emerging technologies which are described in one of the main project reports (Weppner et al., 2012). Nine of these technologies (homomorphic encryption, cognitive radio, indoor navigation, small-scale energy harvesting, smart textiles, and four different kinds of sensor technologies) were selected for further analysis in the scenario-based technology evaluation process (Savage et al., 2013).

In the following, three of the nine technologies are used to exemplify the evaluation process: homomorphic encryption, small-scale energy harvesting and indoor navigation. These technologies are suitable to show the diversity of possible barriers and drivers and the evaluation of their application potential with regard to the scenarios. Homomorphic encryption from the field of communication technology is an encryption technique that permits computation of encrypted data without decrypting it beforehand. This increases confidentiality and has application potentials in the context of cloud computing (see, for example, Ryan, 2013, pp. 2265). Small-scale energy harvesting from the field of energy technology captures and stores energy from external sources. It is embedded as a subsystem and produces power without interfering with the main system. The energy source is freely available in the environment and is captured passively by the energy harvesting system (see, for example, Lallart et al., 2010). Indoor navigation from the field of mobile platform technologies allows navigation in different kinds of facilities using several sensors and networks. Different further services like marketing services but also support for mass evacuations can be provided using this technology (see, for example, Miller, 2006).

3.2. Identification of the barriers to and drivers for emerging security technologies

This section describes how we identified the barriers to and drivers for these emerging security technologies in light of their degrees of implementation and the differing, specific challenges and societal demands associated with the technology areas.

In the first step, drivers for and barriers to each technology were identified in a workshop with more than 30 experts with different backgrounds from science and research, policy, industry and the police. Here we decided to use the world café concept (Brown, 2002; Brown and Isaacs, 2005), because this methodological approach is very suited to gathering and exchanging ideas, is open to new ideas and creates an inspiring atmosphere. The different (stakeholder) experts help to identify the risks and challenges perceived by different groups. The discussion was held at an abstract level, not considering the scenarios. As mentioned above, we emphasized technical and non-technical aspects with regard to the development and application potential of the selected emerging technologies. Because of the specific characteristics of civil security technologies, it is crucial to consider not only their technological feasibility, but also non-technological factors like societal needs, and legal and political frameworks. The identified drivers and barriers were classified by the following dimensions: as social, technological, economic, ecological, legal and political. For example, the societal perspective considers different social elements that can hinder or support the application and development of the technology. Aspects regarding the use, application framework and the value added of the technology for everyday life and its influence on fundamental rights are addressed, as are cultural factors, changes within the value system and the level of training. Furthermore, aspects were discussed like developments in fashion and trendiness, dealing with data overflow and trust in the interpretation of data and signals as well as privacy issues, the public's acceptance of technologies in daily routines and associated potential health risks. However, the technological perspective considers aspects which are directly or indirectly related to the technologies themselves. These include aspects concerning functions, applications, markets and, rival or disruptive technologies. General aspects are explained regarding the supply side, like stagnation of the technology development or its enhancement, quality, efficiency, and insufficient production. Finally, aspects specific to the research and development potential were discussed.

All three technologies address different technological fields associated with their own specific challenges and societal demands. Examples include the increased usage of IT, sustainability, new energy provision (smart grids), increased mobility, and new concepts for buildings and housing (smart buildings). These technologies have diverse characteristics. While homomorphic encryption is only a theoretical concept and proof of concept or practical implementation are still missing up to now, indoor navigation is being practised and many applications already exist. There are “just for fun” applications like location-based marketing, but also the first technologies for civil protection. Small-scale energy harvesting has sustainability and miniaturization as its main driving forces. To illustrate this step, it is insightful to take a closer look at some barriers and drivers of the three selected technologies (for detailed explanations, see Bierwisch et al., 2013): For homomorphic encryption, cloud computing serves as a driver. Cloud computing is the technical frame within which homomorphic encryption is implemented to secure the stored cloud data. The widespread acceptance of cloud services influences the adoption of homomorphic encryption and it therefore has a mainly technical driver. On the other hand, as mentioned above, homomorphic encryption is still a theoretical concept. At present, its technological realization is a barrier that needs to be overcome, so practical implementation is mandatory for its applicability. For small-scale energy harvesting, efficiency and lower energy consumption are identified as drivers. Increased computing times as well as smaller and more effective energy storage are the economic drivers of more and new application potentials. This could also increase the demand from the user side. Waste disposal might evolve to become an ecological barrier, because there is a certain risk that devices containing small-scale energy harvesters will not be able to be disposed of in an environmentally-acceptable way. However, the spread of mobile devices, especially smart phones, and the mobile internet in general are technical drivers for the use of indoor navigation systems, because indoor navigation is also usable as an app. Tracking and privacy concerns are barriers in this context. This technology might raise privacy issues due to the possibility to track the movement of people within buildings and industrial espionage concerns (e.g. stealing maps of competing companies). Also, data security regulations might be a legal barrier to the usage of indoor navigation.

The aim of this step was to collect a wide range of the possible barriers to and drivers for emerging security technologies from different perspectives (e.g. policy, society, research and industry). The discussion of drivers and barriers allowed the participants a detailed study of the selected technologies and promoted the exchange among the individual experts.

3.3. The global scenarios—constructing a framework for the technology evaluation

Scenarios are used as a framework for the evaluation process. Their main objective is to simulate possible futures where security technologies could be used with special regard to the security-specific aspects described in Section 2.2.

Due to the range of different technology areas, their technological degree of implementation and distribution and their interplay with political, societal and economic systems, we decided to choose a global perspective for the scenarios in order to have a holistic framework that encompasses technological and non-technological aspects. However, due to the project framework, there is a strong focus on the European perspective.

The first step in the scenario process was to identify relevant aspects, called key factors, from different influential areas. Therefore, more than 100 future studies, reports and scientific literature on the technologies were analysed. The intention was to give a comprehensive picture of the state of the art and take diverse aspects into account. Finally, the following dimensions were used to derive factors and different future projections.

- EU-(Security)-Policy: Here, harmonization, the integration of further states and policy focus (human, national or defence orientation) are addressed.
- R&D, innovation characteristics, trends and drivers in technology: Public and private funding within the EU's R&D infrastructure are considered here as well as the resource consumption patterns. Commercialization strategies (for example, a security label) and the design and orientation of innovation activities (resilience or threat driven) are compared. Further, the need for human resources and their qualification is regarded as well as the potential orientation towards user needs in technology development.
- Society: This dimension addresses the social value system and the understanding of security. Cultural influences, the relevance of various societal aspects such as active ageing or the attitude towards technology (hype or scrutinizing) also play a role.
- Economy: The fragmentation level, characteristics of the security industry (dominated by small firms or big players, degree of fragmentation) and the security economy (focused on full control or risk acceptance) are discussed. The role of IPR (role of patents, standards and open knowledge) and production and consumption behaviour (sustainable or not) is also considered.
- Global stability and policy: This dimension deals with shifting global powers and global stability as well as the handling of global emergencies and disaster management. Further considerations concern the global economic framework (competing political systems or strong resilience orientation).

17 key factors were derived from these dimensions in a first workshop with 20 experts from industry, academia, society and policy. These factors are relevant aspects or variables which shape the future at the global level. The following criteria were taken into account for selecting key factors: relevance for the future 2020–2030, relevance for security, relevance for the selected technologies, relevance for the European Union, relevance for society and relevance for public and private institutions. When elaborating future scenarios, it is important to work out different possible future developments of each key factor (Gausemeier and Stollt, 2008, p.49f.). Hence a list was compiled including the key factors and the description of different possible future projections. For each factor, more than one alternative assumption was developed that was characterized by the following aspects: they have to cover the same aspects, differ from each other, should be possible or probable and can be positive or negative. For example, the key factor 'design and orientation of R&D in Europe' has two future projections. The first alternative describes the research and innovation landscape as resilience-driven which is characterized by a good balance between applied and basic security research. There is a shift of orientation in security research, not to prevent risks but to accept them and propose how to deal with them and the share of civil security in R&D is larger than the military share. The second alternative is a threat-driven research and innovation landscape. Such a landscape is characterized, for example, by more applied security research and insufficient basic research, decreased dual use of research results and the securitization of life. These alternative projections of the key factor describe different future developments and influence the scenario path then elaborated.

The objective of the next step was to clarify the influence of the global factors on each other and identify the most influential interrelations between factors that may be combined within one scenario. These interrelations were described textually, but also on a scale from 0 (no direct influence) to 3 (strong direct influence).The most influential key factors were derived based on this analysis. For example, shifting global powers and balances are the most influential, followed by the global economic set-up. These have an impact on politics and economic structures as well as society and are therefore the most important aspects for designing the scenario stories.

The consistency of the scenarios was then analysed. The selected factors and future projections are inserted into a consistency matrix and the future projections of the different factors are compared regarding their consistency on a scale from completely inconsistent to highly consistent (Gausemeier et al., 1996). A consistency matrix was constructed and bundles of future projections were taken as a starting point for the scenario descriptions in the form of short stories. The purpose was to find four scenarios with a relatively high consistency using different future projections that are constructed differently in relation to each other. In addition to high consistency, the scenarios tell a distinct, but convincing, logical and plausible story. Fig. 2 shows a section of the key factor list and an example of this short scenario story.

The scenarios describe relevant aspects for global scenarios like the economic and political situation, the influence on the research and innovation landscape as well as the linkages with civil society. The different paths result from the combination of future projections which lead to consistent stories. A particular effort was made to find an appropriate title that summarizes the content and tendency of each scenario. Fig. 3 illustrates the elaborated scenarios and the specific characteristics of each. Furthermore, the four different scenarios are positioned along the two most relevant dimensions: the global political and economic situation, characterized by the two extremes of stability and instability; and the framework conditions at the European Union level that range from weak to strong.

3.4. Scenario-based technology evaluation—combination of the two building blocks

In the technology evaluation phase, the emerging security technologies are considered within the four scenarios. These scenarios are used as alternative frames to evaluate the development and application potential of the selected security technologies. The main point is to test the robustness of the selected technologies within the different scenarios considering their individual composition and finally to make adjustments by applying specific measures and actions to be prepared for the future. Therefore, as mentioned above, we conducted a workshop with more than 30 experts from different organizations (e.g. politics, industry, research).

The three exemplary technologies from Section 3.1 as well as their drivers and barriers were evaluated in the context of the different scenarios (see Fig. 4). In the following, the evaluation procedure is illustrated based on the example of homomorphic encryption. (See Figs. 1– 3.)

In the example, the focus is on the drivers and barriers of the technological dimension, the market dimension and the political and legal dimension. The driver of cloud computing can be seen as a technological pre-condition and is therefore supported by a framework whose characteristics include stable conditions for R&D activities, financing and funding as well as society's trust in technology, especially in the “Technology rules the world” and the “2nd Woodstock” scenarios. The suspicious attitude towards technologies in society tends to decrease technology acceptance in “The broken pitcher” scenario. Regarding the realization and implementation of homomorphic encryption, there is still work to be done to achieve its practical realization. In the “Buddenbrooks global” scenario, the demand for security technologies is generally high and a high technology penetration of everyday life is common. But there is also more emphasis on applied research activities, and the investment in basic research is reduced. Therefore, the implementation of this technology and its innovation success may be hindered in this framework.

With regard to the market dimension, the strategic use of patents is identified as a major barrier. This patent behaviour might lead to a blockade of technical fields because key technologies are protected and not freely accessible for other developments. A consequence might be that only a few providers exist, leading to a high level of dependency and rising prices on the market. The economic barrier of the strategic use of patents might be a strategy for enterprises to strengthen their competitiveness, especially in the “Buddenbrooks global” scenario, because of the fragmented strong European market and the market-driven R&D structure focused on applied research. Furthermore, the mismatch between privacy technologies and governmental forensics is a barrier to industry on a political and legal level. Legal regulations and interventions by state actors clash with technical aspects and data security. On the one

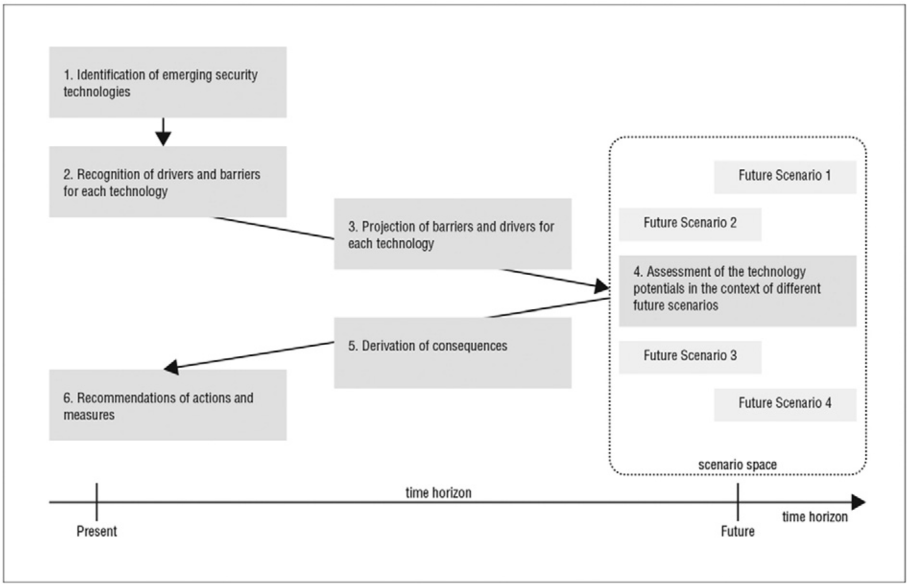
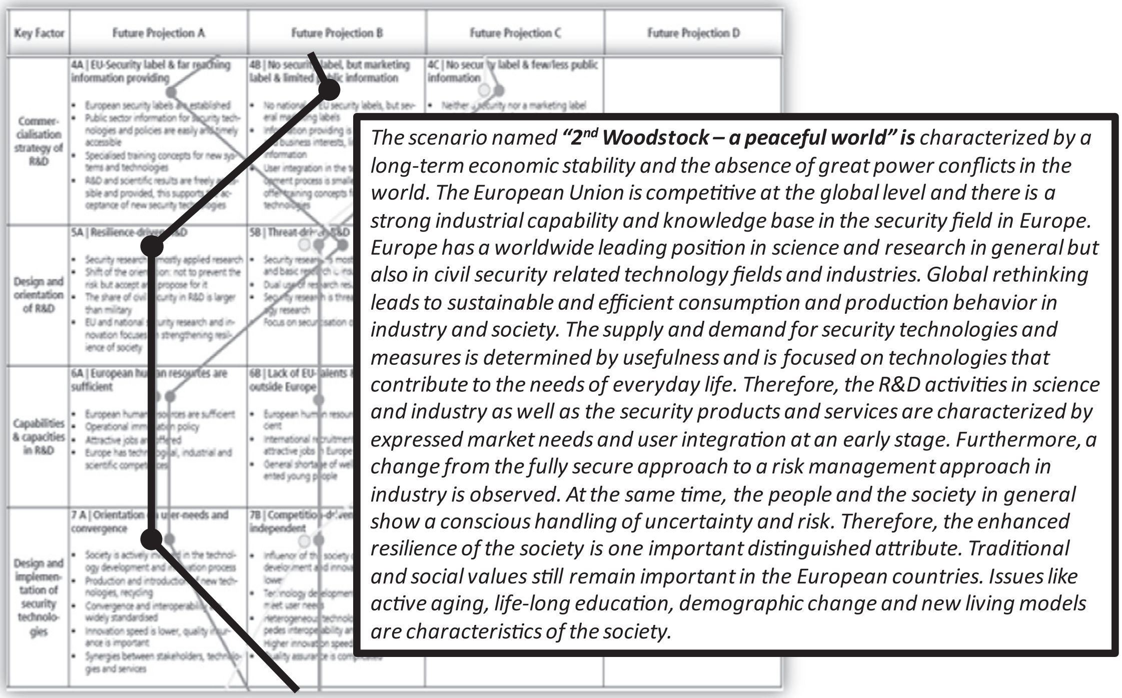

1. Identification of emerging security technologies
2. Recognition of drivers and barriers for each technology
3. Projection of barriers and drivers for each technology
4. Assessment of the technology potentials in the context of different future scenarios
5. Derivation of consequences
6. Recommendations of actions and measures
Future Scenario 1
Future Scenario 2
Future Scenario 3
Future Scenario 4
scenario space
time horizon
Present
Future
time horizon

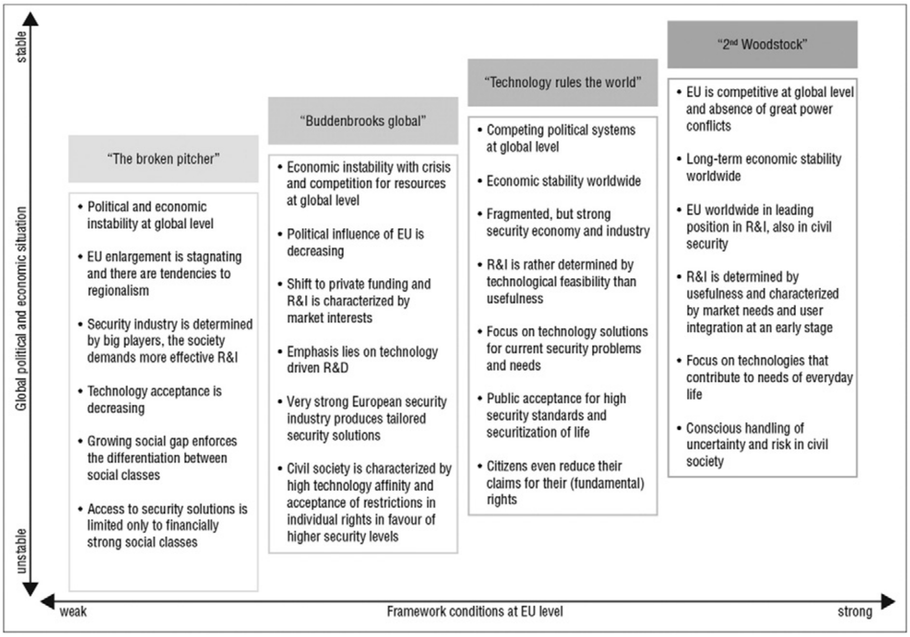
Fig. 1. Process description (own illustration, inspired by Reibnitz (1991, pp. 14)).


Key Factor
Future Projection A
Future Projection B
Future Projection C
Future Projection D
Commer-cialisation strategy of R&D
4A | EU-Security label & far reaching information providing
4B | No security label, but marketing label & limited public information
4C | No security label & few/less public information
Design and orientation of R&D
5A | Resilience-driven R&D
5B | Threat-driven R&D
Capabilities & capacities in R&D
6A | European human resources are sufficient
6B | Lack of EU-talents | outside Europe
Design and implemen-tation of security technolo-gies
7 A | Orientation on user-needs and convergence
7B | Competition-driven independent

The scenario named ***"2nd Woodstock – a peaceful world" is*** *characterized by a long-term economic stability and the absence of great power conflicts in the world. The European Union is competitive at the global level and there is a strong industrial capability and knowledge base in the security field in Europe. Europe has a worldwide leading position in science and research in general but also in civil security related technology fields and industries. Global rethinking leads to sustainable and efficient consumption and production behavior in industry and society. The supply and demand for security technologies and measures is determined by usefulness and is focused on technologies that contribute to the needs of everyday life. Therefore, the R&D activities in science and industry as well as the security products and services are characterized by expressed market needs and user integration at an early stage. Furthermore, a change from the fully secure approach to a risk management approach in industry is observed. At the same time, the people and the society in general show a conscious handling of uncertainty and risk. Therefore, the enhanced resilience of the society is one important distinguished attribute. Traditional and social values still remain important in the European countries. Issues like active aging, life-long education, demographic change and new living models are characteristics of the society.*

Fig. 2. Section of key factor list, future projections and "2nd Woodstock—a peaceful world" scenario path (own illustration).

hand, the demand for privacy technology is supported due to the high demand for security. On the other hand, states can reduce this demand through legal measures that may be supported by the dominance of the national orientation of European security policy as well as the dominance of national legal frameworks as in the "Buddenbrooks global" scenario. One example of such legal measures are the backdoors integrated in security methods for governmental actors. In addition, the different legal frameworks of EU member states might be seen as a barrier to homomorphic


stable
Global political and economic situation
unstable
weak
Framework conditions at EU level
strong

"The broken pitcher"

- Political and economic instability at global level
- EU enlargement is stagnating and there are tendencies to regionalism
- Security industry is determined by big players, the society demands more effective R&I
- Technology acceptance is decreasing
- Growing social gap enforces the differentiation between social classes
- Access to security solutions is limited only to financially strong social classes

"Buddenbrooks global"

- Economic instability with crisis and competition for resources at global level
- Political influence of EU is decreasing
- Shift to private funding and R&I is characterized by market interests
- Emphasis lies on technology driven R&D
- Very strong European security industry produces tailored security solutions
- Civil society is characterized by high technology affinity and acceptance of restrictions in individual rights in favour of higher security levels

"Technology rules the world"

- Competing political systems at global level
- Economic stability worldwide
- Fragmented, but strong security economy and industry
- R&I is rather determined by technological feasibility than usefulness
- Focus on technology solutions for current security problems and needs
- Public acceptance for high security standards and securitization of life
- Citizens even reduce their claims for their (fundamental) rights

"2nd Woodstock"

- EU is competitive at global level and absence of great power conflicts
- Long-term economic stability worldwide
- EU worldwide in leading position in R&I, also in civil security
- R&I is determined by usefulness and characterized by market needs and user integration at an early stage
- Focus on technologies that contribute to needs of everyday life
- Conscious handling of uncertainty and risk in civil society

Fig. 3. Characterization of the four scenarios (own illustration).

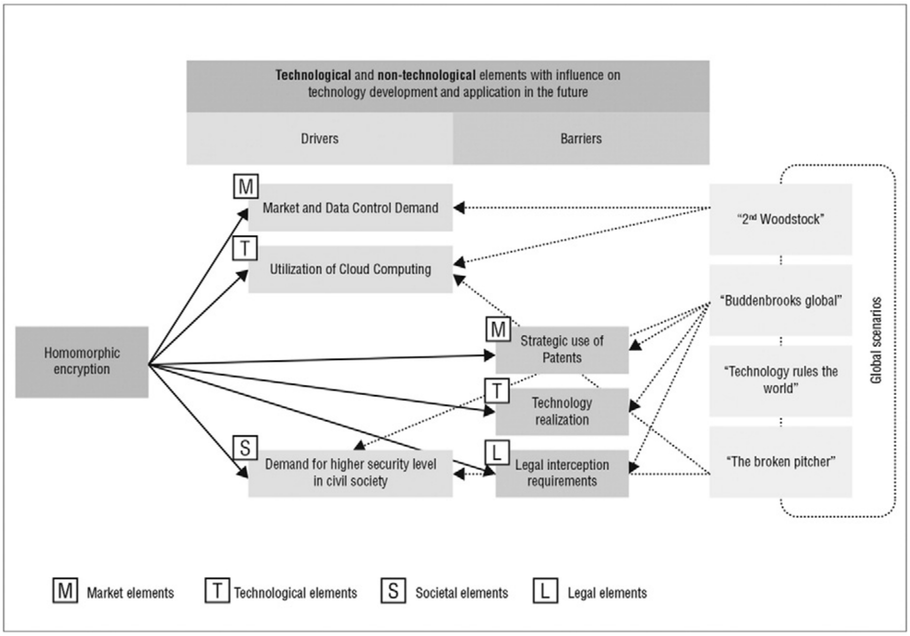

Technological and non-technological elements with influence on technology development and application in the future
Drivers
Barriers
Homomorphic encryption
M Market and Data Control Demand
T Utilization of Cloud Computing
M Strategic use of Patents
T Technology realization
S Demand for higher security level in civil society
L Legal interception requirements
"2nd Woodstock"
"Buddenbrooks global"
"Technology rules the world"
"The broken pitcher"
Global scenarios
M Market elements
T Technological elements
S Societal elements
L Legal elements

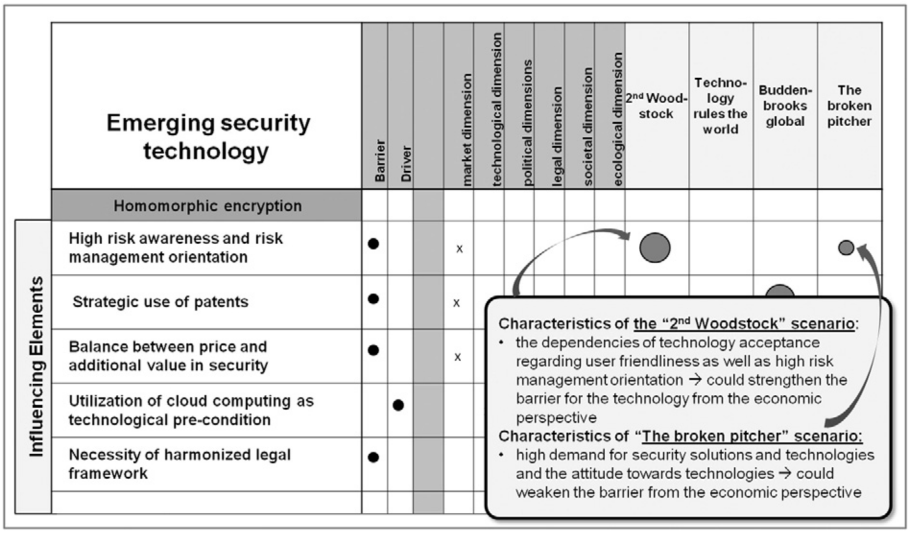
Fig. 4. Scenario-based technology evaluation—example for homomorphic encryption (own illustration).

encryption technology. The legal framework increases the complexity of practical implementation due to the national applicable law and individual adaptation so that additional agreements are necessary. Because of the different levels of integration on the European level and lack of harmonization on a legal level in "The broken pitcher" scenario, the required harmonized legal framework to support the development and application of the technology is not given.

Fig. 5 illustrates the elaborated barriers to and drivers for homomorphic encryption and their developments in the individual scenarios. Depending on the framework conditions, the barriers and drivers of each technology can be strengthened or diminished.

This work was carried out for all nine emerging security technologies (Bierwisch et al., 2013). We came to the conclusion that specific global developments of the influencing factors can strengthen or deactivate the barriers to and drivers for the technologies. Fig. 6 shows the overall assessment of the development and application potential of the three selected emerging security technologies within the scenarios.

The last step of the project was to derive actions and recommendations and to transfer these findings into a socio-economic model to assess the emerging security technologies in a more quantitative way (for a detailed description, see Bierwisch et al., 2013, forthcoming; Burbiel and Schietke, 2013).



Influencing Elements

Emerging security technology	Barrier	Driver		market dimension	technological dimension	political dimensions	legal dimension	societal dimension	ecological dimension	2nd Wood-stock	Techno-logy rules the world	Budden-brooks global	The broken pitcher
Homomorphic encryption													
High risk awareness and risk management orientation	●			x						●			●
Strategic use of patents	●			x								●	
Balance between price and additional value in security	●			x									
Utilization of cloud computing as technological pre-condition		●											
Necessity of harmonized legal framework	●												

Characteristics of the "2nd Woodstock" scenario:
- the dependencies of technology acceptance regarding user friendliness as well as high risk management orientation → could strengthen the barrier for the technology from the economic perspective

Characteristics of "The broken pitcher" scenario:
- high demand for security solutions and technologies and the attitude towards technologies → could weaken the barrier from the economic perspective

Fig. 5. Relationship between scenarios and driving and hindering forces—example for homomorphic encryption (own illustration).

4. Results & discussion

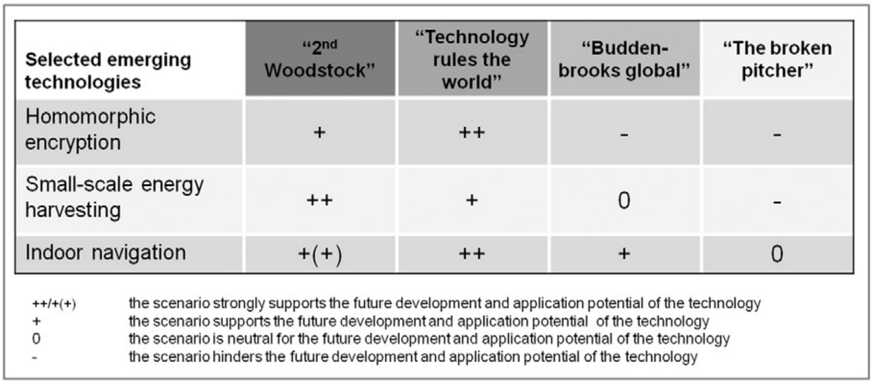
In the following, the results from Section 3 are briefly described and discussed in a broader context. The case study shows that qualitative narrative scenarios in combination with an analysis of market studies and scientific publications are suitable for technology evaluation in general. These studies focused on future market developments, like the diffusion of mobile devices related to indoor navigation technology, and future potentials for use. The application and development potentials of emerging and future security technologies were evaluated and barriers and drivers were derived and reflected upon in the context of the main influencing factors of the technology development. We were able to show which factors have a direct or indirect influence on the technology development and, at the same time, if these factors can be addressed directly with measures by actors from politics, industry and research, or if they are out of their sphere of influence. The actors involved may have direct influence, for example, on increasing a product's acceptance by launching a marketing campaign after testing its usability. Or, as a second example, if disposal is seen as challenging or problematic, it can be included in the technology development process at a very early stage by integrating cooperation partners with the necessary competencies. In Section 2.2, we defined the requirements when evaluating emerging security technologies. Within the scenario development process, many issues are addressed that might arise during technology development, even aspects like the social value system. The legal framework, especially at the EU level, was also considered. Market structure and its organization, the inner European level of harmonization and the R&D landscape were all part of the evaluation. We also addressed potential users and institutional boundaries. As Section 3.4 shows, the non-technical factors and their future projections make a significant contribution to identifying the drivers and barriers of the different emerging security technologies. Thus, we believe global scenarios are an appropriate method that takes into account the requirement to promote social acceptance and acceptability by integrating the relevant concepts in the development of new technologies.

The specific objective of this method, to identify and integrate technical and non-technical drivers and barriers for emerging security technologies at an early stage of technology development by using global scenarios, is partially achieved. Besides the results described above, global scenarios also display other strengths and weaknesses. It is possible to consider various aspects ranging from the social value system to shifting global powers. But societal requirements are diverse and heterogeneous both within and between member states. We tried to address this problem by varying the societal aspects and constructing different future projections. Regarding the global scenarios, the lack of quantification and the qualitative focus might lead to bias. Overlooking important aspects of the regarded context is also problematic but might be solved by conducting workshops with experts from different fields and organizations. It is essential to ensure a balanced relationship of factors and to cover them as dimensions of the problem. If the global scenarios are too wide-ranging and general, it becomes very difficult to set the technology in relation to them and to derive the influences on the regarded drivers and barriers. If drivers and barriers are not on the same level of abstraction, it is difficult to compare them. There is more work to be done on integrating all the relevant assessment dimensions and the characteristics of the scenarios in a socio-economic model. This is a way to add quantitative value to the methodological approach.

Within the scope of research programmes or projects, any indications of technical and non-technical barriers and drivers can be addressed in advance and gain attention as fundamental requirement in an early stage of the technology development process. So the results of the method introduced here serve as decision support and can help to develop recommendations for a European research agenda for emerging security technologies.

5. Conclusion

This paper addressed whether and how societal requirements and other influencing factors can be integrated at an early stage of technology development. An evaluation framework for emerging security technologies was developed using a method based on global scenarios. The study showed that global scenarios are an appropriate tool to assess emerging technologies regarding their future application and development potentials and taking technical and non-technical drivers and barriers into account. If social needs and concerns have to be considered, it is essential that they are mapped in the key factors when developing the scenarios as well as all the other related aspects that characterize the regarded field of interest.



Selected emerging technologies	“2nd Woodstock”	“Technology rules the world”	“Budden-brooks global”	“The broken pitcher”
Homomorphic encryption	+	++	-	-
Small-scale energy harvesting	++	+	0	-
Indoor navigation	+(+)	++	+	0

++/+(+) the scenario strongly supports the future development and application potential of the technology
+ the scenario supports the future development and application potential of the technology
0 the scenario is neutral for the future development and application potential of the technology
- the scenario hinders the future development and application potential of the technology

Fig. 6. Overall assessment of emerging security technologies within the scenarios.

Furthermore, scenarios are suitable to trace the links or dependencies between factors for the involved audiences, stakeholders, and actors responsible for the further technology development process in order to be able to exploit the future application and market potential of the technology.

The interaction of future security technologies with social, ethical, behavioural, economic and ecological aspects will become more and more important in planning processes like research programmes. With regard to the increasing relevance of societal aspects in various contexts, this is a suitable method for their early integration. Integrating societal aspects is very useful, especially in the realm of security technologies used to satisfy security needs.

Acknowledgements

The research leading to the presented results received funding from the European Union's Seventh Framework Programme under grant agreement no. 261512. Within the ETCETERA project (Evaluation of critical and emerging technologies for the elaboration of a security research agenda), the authors were responsible for carrying out an in-depth analysis of selected future technologies in the area of civil security using the scenario method as well as deriving indicators for the economic model based on the scenarios.

References

Bierwisch, A., Seitz, R., Grandt, S., 2012. The innovation system of security: a new quality in the relationship between political, economic and social actors. In: Fraunhofer ISI (Ed.), Innovation System Revisited. Experiences from 40 years of Fraunhofer ISI research, Fraunhofer Verlag, Stuttgart, pp. 129–152.

Bierwisch, A., Grandt, S., Kayser, V., 2013. Report on Development and Application of an Economic Model concerning High Risk/High Payoff: Socio-economic Model for the Assessment of Emerging Security Technologies. Deliverable 6.2, ETCETERA Project—Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda (October, http://www.etcetera-project.eu/deliverables/index.html, accessed 17-03-2015).

Bierwisch, A., Kayser, V., Grandt, S., Shala, E., Dönitz, E., 2015. Future Security Scenarios 2030—Assessment of Civil Emerging Security Technologies. Fraunhofer ISI, Karlsruhe (forthcoming).

BMWi, 2010. Zukunftsmarkt Zivile Sicherheit. Industriepolitische Konzeption des Bundesministeriums für Wirtschaft und Technologie. Bundesministerium für Wirtschaft und Technologie, Berlin (Online: http://www.bmwi.de/BMWi/Navigation/Service/publikationen,did = 369604.html, accessed 18-04-2012).

Brown, J., 2002. A Resource Guide for Hosting Conversations that Matter at the World Café. Whole Systems Associates.

Brown, J., Isaacs, D., 2005. The World Café: Shaping our Futures through Conversations that Matter. Berrett-Koehler, San Francisco.

Burbiel, J., Schietke, R., 2013. Recommendations for an Emerging Security Technology Research Agenda (ESTRA). Deliverable D6.1, ETCETERA Project—Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda (http://www.etcetera-project.eu/deliverables/index.html, accessed 17-03-2015).

Burt, G., 2007. Why are we surprised at surprises? Integrating disruption theory and system analysis with the scenario methodology to help identify disruptions and discontinuities. Technol. Forecast. Soc. Chang. 74 (6), 731–749.

Buzan, B., Weaver, O., 2009. Macrosecuritisation and security constellations: reconsidering scale in securitization theory. Rev. Int. Stud. 35, 253–276.

Cavoukian, A., 2009. Privacy by Design. 1. Information & Privacy Commissioner (available at http://www.ipc.on.ca/images/Resources/privacybydesign.pdf).

Christou, G., Croft, S., Ceccorulli, M., Lucarelli, S., 2010. European Union security governance: putting the 'security' back in. Eur. Sec. 19, 341–359.

Cuhls, K., 2008. Methoden der Technikvorausschau—eine internationale Übersicht. Fraunhofer IRB Verlag, Stuttgart.

Daase, C., 2011. Der Wandel der Sicherheitskultur—Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In: Zoche, P., Kaufmann, S., Haverkamp, R. (Eds.), Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. transcript Verlag, Bielefeld, pp. 139–158.

Davis, F., 1985. A Technology Acceptance Model for Empirically Testing New End-User Information Systems—Theory and Results. Massachusetts Institute of Technology.

Davis, F., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 13 (3), 319–339.

Di Stefano, G., Gambardella, A., Verona, G., 2012. Technology push and demand pull perspectives in innovation studies: current findings and future research restrictions. Res. Policy 41, 1283–1295.

Dosi, G., Freeman, C., Nelson, R., Silverberg, G., Soete, L., 1988. Technological Change and Economic Theory. Pinter Publishers, London.

Edquist, C., 2005. Systems of innovation. Perspectives and challenges. In: Fagerberg, J., Mowery, D.C., Nelson, R.R. (Eds.), The Oxford Handbook of Innovation. Oxford University Press, Oxford, New York, pp. 181–208.

European Commission, 2010a. The EU Internal Security Strategy in Action: Five Steps Towards More Secure Europe. European Commission, Brussels (COM(2010) 673 final).

European Commission, 2010b. An integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage. European Commission, Brussels (COM(2010) 614 final).

European Commission, 2012a. Security Industrial Policy—Action Plan for an Innovative and Competitive Security Industry. European Commission, Brussels (COM(2012) 417 final).

European Commission, 2012b. Public Consultation on the preparation of a new Communication on an Industrial Policy for the Security Industry. European Commission, Brussels (http://ec.europa.eu/enterprise/policies/security/files/doc/public_consultation/background_document_en.pdf, assessed 17-03-2015).

European Commission, 2014. Horizon 2020—Work Programme 2014-2015, 14. Secure societies—Protecting freedom and security of Europe and its citizens. European Commission Decision, Brussel (C(2014)4995 of 22 July 2014).

Gausemeier, J., Stollt, G., 2008. Szenarien für die deutsche Werkzeugmaschinen-Industrie. In: Gausemeier, J., Kinkel, S. (Eds.), Strategische Technologieplanung mit Zukunftsszenarien. Methoden, Hilfsmittel, Beispiele, VDMA Verlag, Frankfurt a.M, pp. 49–82.

Gausemeier, J., Fink, A., Schlake, O., 1996. Szenario-Management. Planen und Führen mit Szenarien. 2nd edition. Carl Hanser, München.

Georghiou, L., 1996. The UK technology foresight programme. Futures 28 (4), 359–377.

Godet, M., Chapuy, P., Comyn, G., 1994. Global scenarios: geopolitical and economic context to the year 2000. Futures 26 (3), 275–288.

Graf, H.G., 2000. Globale Szenarien: Megatrends im weltweiten Kräftespiel. Frankfurter Allgemeine Buch, Frankfurt am Main.

Hirsch, B., 2008. Gesellschaftliche Folgen staatlicher Überwachung. Datenschutz und Datensicherheit 2, 87–91.

Horton, A., 1999. A simple guide to successful foresight. Foresight 1 (1), 5–9.

Hough, P., 2004. Understanding Global Security. Routledge, London/New York.

Lallart, M., Priya, S., Bressers, S., Inman, D.J., 2010. Small-scale piezoelectric energy harvesting devices using low-energy-density sources. J. Korean Phys. Soc. 57 (4), 947–951.

Lin, C.A., 2003. An interactive communication technology adoption model. Commun. Theory 13 (4), 345–365.

Lowrance, William W., 2010. The relation of science and technology to human values. In: Hanks, Craig (Ed.), Technology and Values. Essential Readings, Malden/Oxford/West Sussex, pp. 38–49.

Lundvall, B.A., 1986. National System of Innovation: Towards a Theory of Innovation and Interactive Learning Anthem Press, London.

Martin, B.R., 1995. Foresight in science and technology. Tech. Anal. Strat. Manag. 7 (2), 139–168.

Martin, B.R., Johnston, R., 1999. Technology foresight for wiring up the national innovation system. Technol. Forecast. Soc. Chang. 60 (1), 37–54.

Miles, I., 2010. The development of technology foresight: a review. Technol. Forecast. Soc. Chang. 77 (8), 1448–1456.

Miller, L.E., 2006. Indoor Navigation for First Responders—A Feasibility Study. Wireless Communication Technologies Group, Advanced Networking Technologies Division, National Institute of Standards and Technology (February).

Mowery, D., Rosenberg, N., 1979. The influence of market demand upon innovation: a critical review of some recent empirical studies. Res. Policy 8 (2), 102–153.

Nagenborg, M., 2005. Das Private unter den Rahmenbedingungen der IuK-Technologie, Wiesbaden.

Nagenborg, M., 2009. Ethik als Partner in der Technikgestaltung. In: Maring, M. (Ed.), Verantwortung in Technik und Ökonomie. Universitätsverlag Karlsruhe, Karlsruhe, pp. 101–115.

Postma, T.J.B.M., Liebl, F., 2005. How to improve scenario analysis as a strategic management tool. Technol. Forecast. Soc. Chang. 72, 161–173.

Reibnitz, U., 1991. Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung. Gabler, Wiesbaden.

Ryan, M.D., 2013. Cloud computing security: the scientific challenge, and a survey of solutions. J. Syst. Softw. 86 (9), 2263–2268.

Salo, A., Cuhls, K., 2003. Technology foresight—past and future. J. Forecast. 22, 79–83.

Savage, S., Pohl, A., Levin, B., Khan, M., Noquet, D., Canet, G., Lotero, J.H., Pino, J.L., Revelin, S., Bonfanti, M., Ruhlig, K., Huppertz, G., 2013. Intermediate report on emerging technologies. Deliverable D5.1, ETCETERA Project—Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda (http://www.etcetera-project.eu/deliverables/index.html, accessed 17-03-2015).

Schomaker, P.J.H., 1995. Scenario planning: a tool for strategic thinking. Sloan Manag. Rev. 25–40 (Winter).

Streeten, P., 1980. Basic needs and human rights. World Dev. 8, 107–111.

von Hippel, E., 1976. The dominant role of users in the scientific instrument innovation process. Res. Policy 5 (3), 212–239.

von Schomberg, R. (Ed.), 2011. Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Publications Office of the European Union, Luxembourg.

Weppner, B., Huppertz, G., Pino, L., 2012. List of Emerging Technologies with Security Implications. Deliverable D4.1, ETCETERA Project—Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda (http://www.etcetera-project.eu/deliverables/index.html, accessed 17-03-2015).

Wilms, F.E.P., 2006. Szenarien sind Systeme. In: Wilms, F.E.P. (Ed.), Szenariotechnik, pp. 39–60, Fachhochschule Voralberg, Forschungszentrum Prozess- und Produkt-Engineering, Bern, Stuttgart, Wien.

Dr. Antje Bierwisch has been working as a senior researcher at Fraunhofer ISI in the Competence Center Foresight since August 2007. She did her bachelor and master studies in political science at the University of Erfurt, focusing on law, economics and the social sciences. Antje Bierwisch works on foresight and innovation concepts and methodologies (scenario method, roadmapping, patent and publication analyses), concerning different levels of innovation systems and with a focus on civil security. She coordinates national and European projects dealing with security technology assessment, the impact of societal needs and future opportunities for societal security.

Victoria Kayser (M.Sc.) has been working as a researcher at Fraunhofer ISI since April 2012. Her methodological background is in the field of bibliometrics, patent analysis and text mining, with a thematic focus on computer science. She obtained her Master of Science in Information Engineering and Management at the Karlsruhe Institute of Technology (KIT).

Erduana Shala (M.A.) has been working as a researcher at Fraunhofer ISI since November 2012. Besides her methodological focus on scenarios and foresight validation, her research interests are the philosophy of technology and science, technology and society (STS). She obtained her Master of Arts in European Studies at the Karlsruhe Institute of Technology (KIT).