INFORMATION & SECURITY
An International Journal

Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Procon Ltd.

Volume 29, 2013

Content *I&S*

Volume 29, Number 1

Methods & Techniques in Scenario-based Foresight

Threats, Scenarios, Roles

Volume 29, Number 2

Scenarios and Security Research Planning

The Way Ahead

I&S Monitor

Information & Security: An International Journal

Munné, vol.29, 2013, 147-160 http://dx.doi.org/10.11610/isij.2911

FUTURE SECURITY TRENDS AND THEIR IMPACT FROM AN INDUSTRY POINT OF VIEW

Ricard MUNNÉ

Abstract: Impacts from future security trends on industry have been derived from the work performed in the scenario foresight for alternative futures, and for embedded scenarios of security research in the FOCUS project.[1,2] For each FOCUS theme,[3] and for each scenario found in project reports, changes from the current situation have been analyzed and their impacts for different industries and activity sectors have been assessed. Trends have been grouped by industry/activity in each theme and those with significant ground in each scenario have been selected. According to scenario analysis, public services, ICT and technology, and critical infrastructure sectors are those which are more impacted by detected security trends from the scenarios analyzed. Specifically ICT has some cross cutting trends impacting in more than one theme, like information integration; intelligent knowledge based monitoring of new social media and other open information sources, information management and common situational pictures. Natural disasters, global environmental change and comprehensive approach are the most impacted FOCUS themes by future industry security trends. The analysis presented here may be useful for the assessment in the development of new research tracks or new products in the industry.

Keywords: foresight, security, industry, impact, critical infrastructure, comprehensive approach, EU framework, global actor, natural disasters, supply chain

Introduction

FOCUS[1,2] is an EU co-funded project with the goal of providing a contribution to European security research to effectively cope with future EU roles responding to tomorrow's challenges resulting from the globalization of risks, threats and vulnerabilities. FOCUS methodology does this through the elaboration of multiple scenarios in the form of alternative futures that are plausibility-probed and not just threat scenarios. FOCUS applies an "embedded scenario" integrating method (see Figure 1), delineating options for future tracks and broadened concepts of security research within context scenarios for EU roles to respond to transversal challenges (whose

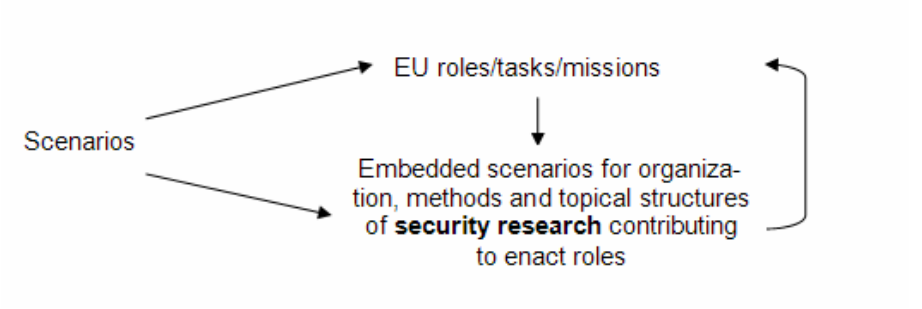

Figure 1: Logic of the FOCUS embedded scenario method.

causes are exogenous, but whose consequences will be experienced within the EU). This is performed along five big themes.

Future trends' impacts on industry have been assessed from the results from each one of the five thematic areas in which the project has split the research work, i.e. from FOCUS results found in the scenarios of alternative futures and from embedded scenarios of alternative futures of security research.

The method used for extracting the industry impacts consisted in analyzing each scenario and detecting changes from the current situation for industries or activity sectors described in the scenarios. First, we assessed changes found in different scenarios from the same theme, looking for consistency of impact. In a second round we selected those industry impacts that are the basis for a given scenario. Detected impacts may have influence over several industries affected by future security trends caused by political, economic or even natural events, proposed by scenarios defined for each of the five FOCUS themes.

The analysis presented here may be useful for assessments in planning for the development of new research tracks or new products in the industry.

Future Security Trends with Impacts on Industry Derived from Comprehensive Approach Analysis[4,5]

The comprehensive approach is an integrative approach to security, and then it basically addresses issues on information analysis and development of comprehensive capabilities. Impacts on industry are basically towards ICT based technologies (integrative, analyzers and knowledge systems) to extract, integrate, analyze and describe security related issues according to future EU agreed policies.

Information Integration

The growth of multimedia data and the expanding number of data sources is increasing the amount of data available which carry the potential to raise security, welfare, trust and create new economic opportunities. According to Neelie Kroes, Vice-President of the European Commission responsible for the *Digital Agenda for Europe*, "Data is the new gold."

This trend has three basic ramifications:

- *Standardization of information models and communication networks:* This will facilitate the exchange of information across multiple organizations and within the same organization, providing better managerial information, improving operational coordination and strategic planning and decision making.
- *System integration*: One step beyond integrating mixed civil-military systems that will allow to develop capabilities in the form of partnership between EU bodies and private actors, for example, merging national computer emergency response teams (CERTS) into a supranational EU team.
- *Methodologies for integrating data from various heterogeneous external sources*: In this field "Semantic data integration" and "Big data" are two different approaches known today. This type of information integration could be the basis for the development of a pan-European security information architecture that could cover all aspects of a comprehensive approach and be the basis for a command and control system.

Impacts: ICT industry, governmental organizations (civil and military), non-governmental organizations.

Information Management and Common Situational Pictures

This trend includes information exchange between different actors as well as the ability to capture information from other automated sources that help to complete the situational picture, feeding national and EU operational and strategic decision making.

It requires the availability of assets, as satellite based surveillance and communications, as well as cyber security capabilities, that may be shared by civilian and military actors and evolve from public-private cooperation.

Impacts: ICT industry, security industry, governmental organizations.

Intelligent, Knowledge Based Monitoring of New Social Media and Other Open Information Sources

The massive access of people to internet and the evolution of social networks are producing an increasing amount of data. It has been acknowledged that structural information ("who is connected with whom") and information payload are valuable resources for risk prevention and trend analysis in order to make more forward-looking decisions.

As of today, the situation regarding the monitoring and control by authorities of those social networks is quite precarious, especially during political and emergency crises.

Extracting relevant information and knowledge from the information available in those networks presents two main challenges:

- Relevance: How to identify relevant information from noise?
- Completeness: How to reach a level of certainty that all relevant information got extracted?

Intelligent, knowledge based monitoring of new social media and other open information sources can provide opportunities to monitor, for example, terrorist, first responder and victim activities by location and to identify trends. The information extracted can be used to feed common situational pictures as described in the previous trend.

Extracting useful information is required to analyze trends, anticipate events or quickly respond to incidents.

More advanced methods, tools and shared protocols for "big data" are urgently needed. In particular, a more robust infrastructure for capturing, storing, processing, and visualizing very large social media datasets is required. This matter also carries implications for fundamental citizens' rights, freedom of expression and data privacy issues.

Also the use and presence in social networks by emergency organizations is still emerging, so there is a big potential for development of crisis communication and management. Emergency services should review their current social media presences, and develop more comprehensive, flexible strategies for using social media in times of crisis. Crucially, this also involves further staff training in using social media effectively.

Impacts: ICT industry, security industry, emergency services (governmental and non-governmental), governmental organizations.

Security Economics System

One of the trends derived from the scenarios produced is a security economics system. This trend is focused in avoiding possible vulnerabilities; on technology assessment; and on supply chain networks (including banking, financial and insurance networks). Based on scenario development and simulation, the main aim of the research is to develop marketable products, procedures and services for EU and state agencies as well as companies and businesses within the European Union.

Impacts: Technological industry, supply chains.

Public Health System

Another trend derived from the scenarios is based on the conviction that European Union's citizens health is the most valuable asset of the EU and its economy. The system includes all existing and individual health care systems of the respective Member States. The main objective is to develop common standards in fields such as public health structures and processes, budgeting infrastructure, facilities and capability development.

Impacts: Health industry.

Future Security Trends with Impacts on Industry Derived from Natural Disasters and Global Environment Change Analysis[6,7]

Global environment change and related natural disasters imply changes in the current production model, and in related critical infrastructures and in supply chains. Impacts on industry are basically towards all critical infrastructures, but specifically on energy generation and distribution. It will probably affect location of most manufacturing sites, resulting in the centralization in safer places.

In this theme, additionally to the impacts detailed below, the following impacts from other themes already detailed have been also detected:

- Information integration (from comprehensive approach)

Accommodation of Critical Infrastructures and Manufacturing Areas

In general, a highly centralized energy system leads to single events affecting large parts of it. Then, due to the increase of extreme weather events, induced by climate change, such as storms, will result in losses in wind power plants, and especially, the electrical grid that due to its centralized character is prone to this type of damage. Therefore EU will have to increase backup capacities in the form of additional power plants, redundant electrical lines, etc. In the long run, it will follow a decentralization policy in order to increase resilience to natural and man-made disasters.

While fostering local energy production, EU will support a redundant European energy grid, enabling energy trade when necessary. At the same time, regulations at the energy market ensure that trade is made less attractive and thus limited to a minimum.

High dependency on electricity and information networks increases vulnerability of critical infrastructures.

Globalization has caused significant relocation of manufacturing capacity from Europe to Far-East and China. Production assets reside on regions that are more prone to extreme events. On the other words, risks are arising. Some production sites will be moved to areas less affected by climate change-induced hazards wherever possible, leading to a high degree of centralization. Required critical infrastructures will be provided to these safer manufacturing areas.

Impacts: Utility companies, transport infrastructure operators, global trade, large corporations with manufacturing facilities in risky areas.

Impacts on Energy Industry

The ever increasing price of fossil fuels opens a huge market for renewable energy and energy saving technologies.

Nuclear—once a technology promising big returns to investors—will turn out to create ever increasing costs due to rapidly rising expenses for safety and security measures derived from accidents, including severe disasters. The costs will reach sums which may no longer be externalized.

Apart from the necessary development of new technologies in renewable energy production, especially reduction of energy input and emissions during production, the European electrical grid needs a thorough redesign. This is backed up by development of energy saving technologies and education for less energy consuming lifestyles in particular.

However, overall energy consumption will be increasing. EU will take actions against these problems by increasing the use of renewable energy systems. The use of renewable energy sources will be massively supported, on the one hand by generous funding schemes, and by adding formerly externalized costs from conventional energy production to its price on the other hand.

Supporting of renewable energies opens markets and provides possibilities for technological leadership. These technologies may be exported to developing countries.

Furthermore, funding of adequate methods of carbon capture and storage (re-forestation) as well as introducing carbon taxation would likely be acceptable and sustainable possibilities.

Increase of temperatures due to climate change will foster permafrost thawing, resulting in high investments for the upkeep of oil and gas pipelines. While a switch to tanker-based transport of oil and Liquefied Natural Gas (LNG) may increase security of supply, local energy generation based on renewable sources will guarantee independence on political developments outside the EU.

Impacts: Energy production and distribution industries.

Deployment of Remote Sensor Networks for Natural Events

Development of advanced technologies for disaster forecast systems for natural disasters will be funded by industrial research since it will help the reduction of overall costs. These new systems will put more emphasis on drivers of natural disasters and on long-term forecasts on planetary boundaries.

Extensive use of sensor systems' response to external events (natural or man-made):

- Natural disasters usually grow up very rapidly. Need of a precise sensor network connected to a quick reaction information and countermeasures system.
- GEC (Global Environmental Change) is a long cycle phenomenon which needs extensive use of sensors plus a coordinated network for exchanging and processing huge amounts of data over long periods for working out the correct conclusions at planet level.

Impacts: Technological industry, emergency services, critical infrastructure operators.

Restrictions to Mobility

Due to climate change, the increase of epidemics will lead to the intensification of border controls, effectively simplifying disease control. Thus, transmission of diseases through human travel will play a minor role within the EU borders, while outside, in the "rest of the world," epidemics will spread fast, fostered by inadequate treatment and bad living conditions. A major danger will arise from shifting habitats, resulting in the spreading of vector transmitted diseases to Europe, which were formerly mainly known in North Africa. While proper treatments will be easily available in Europe, sufficient capacities in health care will need to be considered.

Impacts: Multinational corporations.

Supply of Raw Materials

Reducing complexity and physical length of supply chains (less transport of raw materials). Since exploration and exploitation are conducted mainly outside the EU, good contacts to the elite in raw material rich regions are essential, which would oth-

erwise render supply unreliable. Reducing this dependency through recycling technologies and a lifestyle demanding fewer raw materials will play a very important role in the EU. Recycling technologies reduce dependency on imports and counteract increasing prices for certain raw materials such as copper or rare earths.

Impacts: Supply chains and recycling industry.

Future security trends with impacts on industry derived from critical infrastructures & supply chain protection analysis [8,9]

Resilience of critical infrastructure and supply chains is basic to provide a stable framework to societies for their development. Critical infrastructures are facing several threats in the future, and industry impacts presented here are those that will provide more stability. Regarding supply chains there are chances for organized crime to take control of them under some conditions and in some regions.

In this theme, additionally to the impacts detailed below, the following impacts from other themes already detailed have been also detected:

- Information integration (from comprehensive approach)

Resilience of Supply Chains and Critical Infrastructure

Critical infrastructure and supply chain networks depend on information and communication (ICT) networks and related services. One basic trend is that resilience of critical infrastructure and supply chain networks is increasingly neglected.

Development of ICT network resilience will also require reinforced resilience in other primary and secondary networks or infrastructures such as energy supply. Policies will be set up to enhance resilience of supply chains as well as infrastructures. Smart grids will be developed that will allow for better and more resilient energy management and distribution networks.

Impacts: Supply chain and critical infrastructures.

Better Critical Infrastructures Decision Support Systems

A minimum standard of critical infrastructures information management will be stipulated in order to ensure that in case of emergency, appropriate actions can be taken efficiently and effectively. On the other hand, semantic interpretability of data without relying on exact specifications will have the advantage of attaining a certain level of format independence, yet at the cost of increased uncertainty.

Based on the integration of relevant collected information from different sources and levels, this information will be provided to owners and operators of critical infrastructure in order to take appropriate management decisions to ensure operability.

Impacts: Critical infrastructures.

Chances for Organized Crime in Supply Chains

As a result of weak European leadership, increasing financial constraint may reduce the resources available to public authorities to combat internal security threats. Differences within Europe can cause weak spots that organized criminals can use for illegal immigration, smuggling and counterfeit of commodities that will find their routes to Europe more efficient and used more than ever before. Consumers and retailers will participate unintentionally in criminal market operations.

Impacts: Supply chain.

Future Security Trends with Impacts on Industry Derived from EU as a Global Actor Based on the Wider Petersberg Tasks Analysis[10,11]

Impacts for this theme are common with those found for the comprehensive approach and in lesser extent to some of those found in other themes. As far as EU will need to play some roles regarding this issue, some basic need for information integration from all kind of sources will be needed to fulfil it.

No specific impacts have been detected for this theme, but the following impacts from other themes already detailed have been detected too:

- Intelligent, knowledge based monitoring of new social media and other open information sources (from comprehensive approach)
- Information management and common situational pictures (from comprehensive approach)
- Security economics system (from comprehensive approach)
- Deployment of remote sensor networks for natural events (from natural disasters and global environment change).

Future Security Trends with Impacts on Industry Derived from EU Internal Framework Analysis[12,13]

Many of the identified impacts are common with those found in the comprehensive approach and in lesser extent to some of those found in other themes. As far as EU will evolve towards an integrated entity, more focus to the surveillance of external borders from an integrative approach will be possibly needed.

In this theme, additionally to the impacts detailed below, the following impacts from other themes already detailed have been detected too:

- Intelligent, knowledge based monitoring of new social media and other open information sources (from comprehensive approach). However in this theme it has a multipurpose approach. The use of such technology includes education and training of decision-makers and first responders, as well as online collaboration for emergent groups, for example digital volunteers for new social media monitoring in crises and emergencies.
- Deployment of remote sensor networks for natural events (from natural disasters and global environment change).

Surveillance Technology for Border Control

Putting in place, at EU level, an integrated border management system to counter transnational threats. Focus on organized crime, cyber-threats, and illicit trafficking in material and weapons in the CBNR (chemical, biological, nuclear and radiological) sector.

Impacts: Security industry.

Analysis of detected industry impacts

For analyzing detected industry impacts of future security trends, every impact has been decomposed into each of its industry impacts, and assigned to each one of the corresponding FOCUS themes. In this way, an industry ranking has been obtained. It is presented in Table 1 below.

According to this ranking, the top industries with more impacts related to future security trends are:

Information and Communication Technologies: These results are basically due to the trends: *Information integration* (similar to the foreseen need of integrating information and systems to get a clear picture of various security related issues, instead of getting pieces of different information that are not interrelated); *Intelligent, knowledge based monitoring of new social media and other open information sources* (similar to the foreseen need to extract and feed valuable information from/to social networks in cases of emergencies and for crime prevention); *Information management and common situational pictures* (to provide environment information and present an approximate picture of real situations that facilitate the management of security related issues).

Governmental organizations: This so called industry is clearly the first one responsible for the provision of security in the EU countries, so many of the security trends are related to it as a provider of security or receiver of security related information.

Security industry: This is clearly related to the previous industry. The reason of this industry being in the third position is because security industry is the main provider of security solutions to Governments, and most of these solutions will be based in ICT to enhance and maximize potential safety in possible futures.

Table 1: Impacts by industry and theme.

FOCUS Theme / *Industry*	*Comprehensive approach (13)*	*Natural disasters & global environment change (14)*	*Critical infrastructures & supply chain protection (7)*	*EU as a global actor - Petersberg Tasks (12)*	*EU internal framework (8)*
ICT (8)	**3**	**1**	**1**	**2**	**1**
Governmental organizations (8)	**3**	**1**	**1**	**2**	**1**
Security industry (6)	**2**			**2**	**2**
Emergency services (6)	**1**	**1**		**2**	**2**
Technological (5)	**1**	**1**		**2**	**1**
Supply chain (5)	**1**	**1**	**2**	**1**	
Critical infrastructure operators (5)		**1**	**2**	**1**	**1**
NGOs (3)	**1**	**1**	**1**		
Large / multinational corporations (2)		**2**			
Health (1)	**1**				
Utilities (1)		**1**			
Transport infrastructure operators (1)		**1**			
Global trade (1)		**1**			
Energy (1)		**1**			
Recycling (1)		**1**			

A second view has been provided by grouping industries by sectors. The following match has been provided:

- *Public services*: Governmental organizations; Emergency services; NGOs
- *ICT & other technologies*: ICT; Technological
- *Infrastructures*: Supply chain; Critical infrastructure operators; Utilities; Transport infrastructure operators; Energy; Recycling
- *Globalization*: Large / multinational corporations; Global trade
- *Security*: Security industry
- *Health*: Health

This provides a sector ranking and a clear view of the impacts derived from each FOCUS theme, as can be appreciated in Table 2.

According to this ranking the sector with more impacts is the Public services sector. The reason is that it is broadly assumed that by 2035 it will be a basic security provider for the *comprehensive approach* and in *EU as global actor* themes.

The second sector in the ranking is *ICT & other technologies*, as a sector that will provide disruptive tools for the security in the *comprehensive approach* and in *EU as global actor* themes.

Table 2: Impacts by sector and theme

FOCUS Theme / *Sector*	*Comprehensive approach (13)*	*Natural disasters & global environment change (14)*	*Critical infrastructures & supply chain protection (7)*	*EU as a global actor - Petersberg Tasks (12)*	*EU internal framework (8)*
Public services (17)	**5**	**3**	**2**	**4**	**3**
ICT & other technologies (13)	**4**	**2**	**1**	**4**	**2**
Infrastructures (11)	**1**	**6**	**4**	**2**	**1**
Security (6)	**2**			**2**	**2**
Globalization (3)		**3**			
Health (1)	**1**				

In the third place in the ranking the *Infrastructures* sector is found, as it will be the most impacted by *Natural disasters*, and especially by emergencies caused by climate change. The sector will be also have main responsibility for security trends *impacting critical infrastructures*, therefore, the need of applying specific solutions for its security management.

Regarding themes, those with most security trends impacts are *Comprehensive approach*, caused by an integrative vision of security; *Natural disasters & global environment change*, due to the foreseen impacts of climate change; *EU as a global actor - Petersberg Tasks* as one of the most broad themes with many similarities with comprehensive approach regarding security trends and associated impacts.

Conclusion

Even though the compilation of industry impacts cannot be considered complete and thorough, as it is based on the assessment of possible future scenarios of security, it clearly indicates what will be the most probable trends affecting industry sectors by 2035 due to likely future security scenarios.

Thus, the Public services sector in the most impacted sector, owing to its implication as a basic security provider for EU citizens. After that, ICT and technology sector is following, basically due to the fact that it will supply technology for most of the future security solutions to deal with security threats, primarily by its disruptive capacities (e.g., management of energy decentralized distribution girds) and because of its impact due to the pre-eminence in the management of security information (e.g., information management and common situational pictures). Also, the Critical Infrastructures sector is one of the most impacted sectors by future security threats, and therefore it needs new strategies and solutions to face with them.

Acknowledgement: The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261633. This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained therein. For more information visit the project website at www.focusproject.eu.

Notes:

[1] FOCUS: "Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles," www.focusproject.eu.

[2] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261633.

[3] FOCUS themes are: Comprehensive approach; Natural disasters & global environment change; Critical infrastructures & supply chain protection; EU as a global actor based on the wider Petersberg Tasks; EU internal framework.

[4] Center for European Security Studies Sigmund Freud Private University Vienna, FOCUS Deliverable 3.2, *Report on alternative future models of comprehensiveness* (December 2011).

[5] Danube University Krems, Austria, FOCUS Deliverable 3.3, *Syllabus of thematic embedded scenarios. Alternative futures of security research for a comprehensive approach* (March 2012).

[6] University of Natural Resources and Life Sciences Vienna, FOCUS Deliverable 4.2, *Literature and small-world study on future nature-related disasters* (May 2012).

[7] University of Natural Resources and Life Sciences Vienna, FOCUS Deliverable 4.3, *Syllabus of approximately 4 thematic embedded scenarios [for future security research in the Big Theme "Natural disasters & global environmental change"]* (September 2012).

[8] Ingeniería de Sistemas para la Defensa de España, S.A., FOCUS Deliverable 5.2, *Report on interdependence of infrastructures* (May 2012).

[9] Instituto Nacional de Técnica Aeroespacial (INTA), FOCUS Deliverable 5.3, *Syllabus of thematic embedded scenarios Alternative futures of security research for critical infrastructure & supply chain protection* (August 2012).

[10] Center for European Security Studies Sigmund Freud Private University Vienna, FOCUS Deliverable 6.2, *[EU role scenarios and resulting] Table of topics and necessary disciplines for a European research agenda [in the big theme: EU as a global actor based on the wider Petersberg tasks]* (June 2012).

[11] University of Haifa & Center for European Security Studies Sigmund Freud Private University Vienna, FOCUS Deliverable 6.3, *Syllabus of approximately 4 thematic embedded scenarios [in the Big Theme "EU as a global actor based on the wider Petersberg tasks"]* (September 2012).

[12] Center for European Security Studies Sigmund Freud Private University Vienna, FOCUS Deliverable 7.2, *Multi-disciplinary report on analyses of the Lisbon Treaty as organizing context for future EU roles* (June 2012).

[13] University of Haifa, FOCUS Deliverable 7.3, *Syllabus of approximately 4 thematic embedded scenarios [for future security research in the big theme "EU internal framework"]* (August 2012).

Ricard MUNNÉ is currently Project Manager, working in the Public Sector Unit in Atos Research and Innovation since 2011. Previously, he worked as Project Manager and Consultant in Public Sector projects, mainly in e-Government and e-Invoice areas. Ricard earned a degree in Telecommunications Technical Engineer from Escola Universitària d'Enginyeria Tècnica Telecomunicacions, La Salle Bonanova, Barcelona in 1989 and pursued a Master in Information Technology Management at Universitat Ramon Llull, Barcelona. *E-mail*: ricard.munne@atosresearch.eu