STRATEGIC ANALYSIS

KNOWLEDGE DEVELOPMENT AND HORIZON SCANNING FOR STRATEGIC LONGTERM PLANNING IN CYBER SECURITY

Johannes GÖLLNER, M.Sc.
Federal Ministry of Defence and Sports, National Defence Academy, Vienna, Austria
Joachim KLERX, PhD
AIT Austrian Institute of Technology GmbH, Innovation Systems Department
Klaus MAK, M.A.
Federal Ministry of Defence and Sports, National Defence Academy, Vienna, Austria

Abstract

Existing foresight studies produce expectations regarding mid-term and long-term expectations about the future. In particular, in the cyber domain, these expectations tend to change accidently, caused by disruptive events. For reliable long-term strategic planning it is necessary to understand the dynamics of these changes. Our horizon scanning method is developed to address social needs, as well as scientific capabilities and technical solutions and will produce reliable knowledge about analysing weak signals for threats, disruptive events and long-term trends.

Transparent, public knowledge about long-term trends is very important for the efficiency of each strategic long term planning activity in all supply chain networks and in relation to domain cyber space. In the last few decades, the ICT infrastructure did become ubiquitous for all supply chain networks, for all critical infrastructures and, in particular, for knowledge management in these domains. Each stakeholder has their own expectations about future trends and behaves in accordance with these expectations. Misleading expectations can cause flawed investments and political strategies.

This publication will present a method for semi-automatic knowledge creation and sharing to increase knowledge about future developments and future needs in the system. This knowledge can support long term capability planning, research agenda setting, innovation management and strategic long term planning in cyber security. However, it is in the core

of foresight not to predict the future of cyber security, but to build it. Thus, knowledge development and horizon scanning are support actions for strategic planning activities.

Keywords: Knowledge development, Z-Model, multi-layer multiple vector model, horizon scanning, foresight, strategic long term planning, research agenda setting, critical infrastructure, supply chain network protection, cyber security, documentation, information logistic, knowledge logistic, risk management, information-,scenario-, risk mapping, innovation management.

Introduction

It is a well-known fact that speed of innovation is high in the cyber domain. A main reason for this is that tools for manual, semi-automatic and automatic knowledge processing are developed and used in the cyber domain at a very early stage. Given the fact that knowledge is the most important success factor in the cyber domain, it is obvious that innovation speed is not only high, but is constantly increasing. Thus, knowledge development and horizon scanning are one of the most important strategic capabilities in domain Cyber Space.

ICT-networks, in particular with other supply chain networks [1] (basic networks, supply networks and administrative- as well as governmental networks), have a very strong vertical and horizontal interaction. Those interactions between ICT infrastructure supply chain networks are vulnerable to professional cyber-attacks.

It is very likely that future cyber-attacks, like actual advanced persistent threats (APTs), will be very well prepared, achieving sustainable disruption of global and continental supply chain networks from critical infrastructure sectors such as finance , energy , transport , health care and food production. APT attacks on the command & control systems of these economic sectors are expected to generate high economic damage. To keep pace with the high innovation rate in the cyber

1 Johannes Göllner, Andreas Peer, Manfred Gronalt, Gerald Quirchmayr. Risk analysis for supply chain networks. I3M: The 11th International Multidisciplinary Modelling & Simulation Multiconference- HMS-track: Intermodal transportation systems and services, September 10-12, 2014 University of Bordeaux, France; http://www.msc-les.org/conf/i3m2014/i3m2014_program.pdf .

domain and to address new unknown threats with preventive actions, new forms of knowledge development and knowledge management are vital. Therefore, continuous horizon scanning to support strategic and political decision making in the cyber domain is absolutely indispensable. Based on horizon scanning - and foresight results, it is possible to develop preventive strategic risk management for enterprises and public services to proactively protect the global supply chain networks from any future damage.

The CentDoc[2], (partly from the National Defence Academy (NDA)) is the operational unit for managing open source information for the Austrian Armed Forces (AAF). Since 1968, relevant documents for the AAF have been analysed, stored in databases and distributed to defined user groups. The main tasks are usually registration, screening, evaluation, content exploitation, terminology extraction, categorising, and creation of abstracts, profiling and indexing of a wide variety of sources. With the use and application of different tools in the field, as well as development and evaluation of new methods and knowledge management approaches, the CentDoc has gained maximum of efficiency in knowledge management for armed forces.

In cooperation with the Austrian Institute of Technology, new methods are developed at the CentDoc to address future cyber challenges. Strategic foresight and adaptive innovation management can contribute to increasing the capability of security organisations to keep pace with the high speed of innovation processes in the cyber domain or even to win the innovation race at some point in the future. According to research results from IINNOSEC[3] and ETTIS[4], this includes:

2 CentDoc: **Department of Central Documentation and Information Service of the** National Defence Academy at the Austrian Ministry of Defence and Sports;

3 The INNOSEC Project is supported and promoted within the security research programme of the European Commission (FP7-SEC-2012-285663). Parts of the article were taken from the deliverables which are referenced in the respective sections. We would like to thank all authors of the INNOSEC project for contributing to this article.

4 The ETTIS Project is supported and promoted within the security research programme of the European Commission (FP7-SEC-2011.6.3-1). Parts of the article were taken from the deliverables which are referenced in the respective sections. We would like to thank all authors of these deliverables for implicitly contributing to this article; however, the authors of this article take full responsibility for this publication.

1. **Processes of ideation: horizon scanning, searching, monitoring and** identification of topics, weak signals, idea generation; and idea management;
2. **Processes of selecting and designing: including evaluation and selection of new** and state of the art ideas, solutions and technologies, identification of capability gaps and new research topics
3. **Processes of implementation: with research about adoption, adaption,** innovation and implementation of new ideas and solutions
4. **Learning loop** *and feedback*: including knowledge management and risk management[5]

This paper presents a framework for horizon scanning in the cyber domain, with initial results from cyber horizon scanning and the future outlook, including a process model for an horizon scanning centre.

Knowledge development for foresight

Knowledge development for foresight is a collection of iterative processes. The quality on each level has consequences for the quality of the next level. If data acquisition and information retrieval are not precise, the quality of the next level is lower than necessary. Thus, quality checks are necessary on every level.

The following graph shows the development of knowledge in a horizon scanning centre (HSC) as a collection of processes of knowledge accumulation with quality assurance and risk assessors-evaluation (Z model). The knowledge development starts with information logistics processes for data acquisition and information retrieval. This usually includes big data capabilities for automatic weak signal mining.

In the second step, the quality of the information is enriched by human analytics and crowd intelligence.

5 Joachim Klerx, Andreas Kasztler and Jillian Yeow, "Strategic foresight and innovation management in security research", upcoming in 2015.

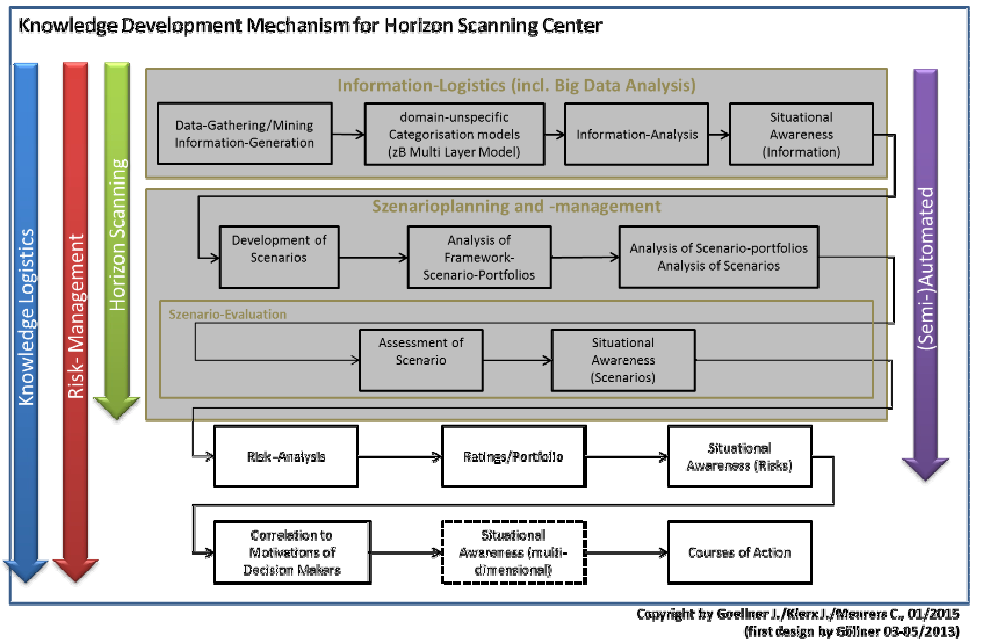

Figure 1. Knowledge logistics in a Horizon Scanning Centre[6]

The enrichment process uses general and domain specific classifications to create an initial collection of scenarios for situational awareness, based on available information. Plausible and resilient scenarios are created by using background information and additional knowledge from experts. This leads to a situational awareness picture, based on existing knowledge. Finally, the risk analysis leads to a multidimensional picture of risks and opportunities for the future. This serves as strategic knowledge for long term planning and decision making in adaptive innovation management.

The different dimensions are based on unspecific classifications and domain specific classifications, as in the **multi-layer multiple vector model in figure 2.**

6 Second Design by Göllner, Klerx 07/2013 published in Klerx, Joachim Göllner, Johannes, Mak, Klaus, Horizon Scanning for emerging risks in supply chain systems, in: Wilby, Blachfellner, Hofkirchner, Book of Abstracts, **EMCSR-European Meetings on Cybernetics** and Systems Research, S.601-607, Wien, 2014; vorgestellt im Rahmen der Präsentation auf der EMCSR 2014.

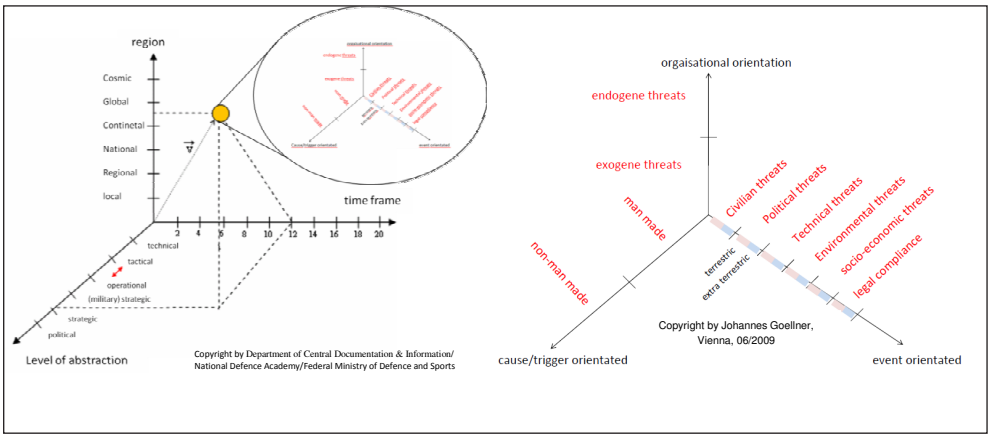

Figure 2. multi-layer multiple vector model-General and specific for threat analysis[7]

On the first level, all information is classified by the typical categories of the human mind (Kant), time, space and level of abstraction.

On the second level of this multi-layer classification model[8], the information is structured along the dimension "organisational orientation" with endogen and exogen threats, the dimension "cause/trigger oriented" with man-made and non-man made threats and the dimension "event oriented" with civilian threats, political threats, technical threats, environmental threats, socio-economic threats and legal compliance.

7 Presented at 7th Social Network Conference 2011 at the University of Greenwich, London, United Kingdom, 07/2011, (accepted peer-reviewed paper): Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria (Johannes GOLLNER, Christian MEURERS, Andreas PEER, Guenter POVODEN). The Multi Layer Model has been developed at the National Defence Academy of the Austrian MoD-internal research project „Scenarioplanning and knowledge management at the AAF" (2010 – 2012) through Johannes GÖLLNER, Klaus MAK, Christian MEURERS, Andreas PEER and Günther POVODEN.

8 Göllner, Johannes, Meurers, Christian, Peer, Andreas, Langer, Lucie, Kammerstetter, Markus: „Bedeutung des Risikomanagements für die Sicherheit von Smart Grids/Relevance of Risk Management for the Security of Smart Grids „ in Göllner, Johannes, Mak, Klaus, Meurers, Christian (Hrsg.): Viribus Unitis, Wissensmanagement - Ausgewählte Schriften, Militärwissenschaftliches Journal der Landesverteidigungsakademie, Band 16/2014, HDruckZ, Wien, 2014, p.179ff und Symposium Energieinnovation 2014, Technische Universität Graz, 2014,http://portal.tugraz.at/portal/page/portal/Files/i4340/eninnov2014/files/lf/LF_Meurers.pdf

Depending on the different sorts of scenario planning methods, different sorts of quality checks are included. For plausible and resilient scenarios, the scenario creation process is divided into three sections:

- the actual production process
- an ongoing quality assurance and
- a plausibility check.

The process begins by describing the system and system boundaries, as well as main drivers, system parameters and variables. After the system definition, the dynamic part of the system is subsequently analysed. The results from this analysis and evaluation are included in different subsystems as part of the modelling aspect. Each modelling step is supported by simulation (if possible) and plausibility checks. With checks for diversity and homogeneity, a resilient set of scenarios can be generated.

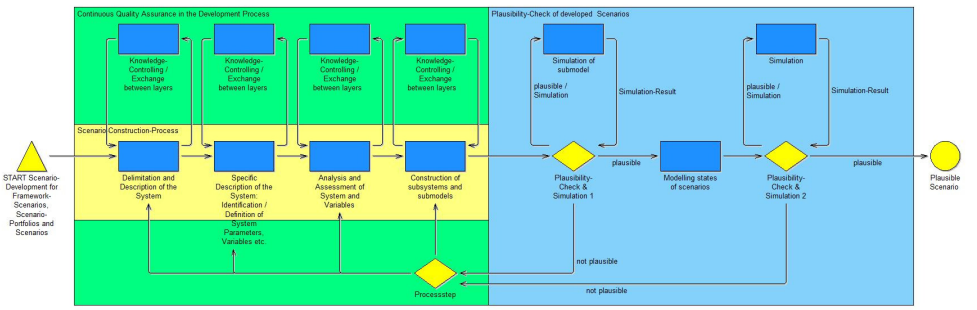

Figure 3. Quality Management Process for Designing of plausible and resilient Scenarios[9]

At the end of the process, plausible and robust framework scenarios, scenarios portfolios and individual scenarios are processed according to the Z-model. However, in particular for the cyber domain, system dynamics are only partly useful, as simulation environments for innovations are not reliable. Therefore, a different strategy for scenario generation is necessary.

9 Source: Göllner, Johannes, Meurers, Christian, Peer, Andreas (National Defence Academy) und Povoden, Günter (NBC-Defence School), result of the Austrian MoD-internal knowledge management/research project „Scenario planning and knowledge management at the Austrian Armed Forces, 2010-2012.

Given the fact that horizon scanning for weak signals will come up with weak signals for trends, threats, opportunities, disruptive events and wild cards, this can be used as a starting point for scenario formulation. The following chapter will present some preliminary results of horizon scanning activities in cyber security.

Results of horizon scanning in cyber security[10]

The main goal of the weak signal mining activity is to identify possible future threats, based on discussions on internet. However, the interpretation of which signal might be a future threat depends very much on human interpretation. Therefore, a two-step strategy was applied. In the first step, a community was identified; in which members of the community publish content about future threats on the internet. In the second step, the content was clustered to find out about the main topics of possible future threats and an in depth analysis of these topics was conducted to get hints about possible weak signals for future threats. Based on a dataset of about 160,000 links to sites containing the phrase "future threats", discussion topic where clustered and identified, with regard to their potential for a weak signal.

In communication theory, a signal is a sign with a specific meaning to the receiver of this signal. If the communication is built up with a carrier signal of white noise, then a signal with a specific meaning has to be different from the white noise. As a core concept in signal processing, the signal is the peak that transfers the information from the sender to the receiver. Consequently, a weak signal is a signal which is statistically not very different to the carrier signal.

In text mining, the basic corpus, or more precisely, the word frequency matrix of the basic corpus, is used as a kind of white noise for the analytical process. The TIA algorithm identifies weak signals, based on changes in the word frequency matrix, which are used as indicators for semantic weak signals. These signals can either indicate a threat or an opportunity. It can give hints to resulting future

10 Based on results from the ETTIS Project (FP7-SEC-2011.6.3-1). D4.2, D4.4, D4.5, D5.3, D5.4, D6.3.

social needs, or can be a wild card. As the following graphic symbolises, it is a good process in semantic analysis to check first, whether there is a potential for a threat or opportunity, then check, whether there are hints at social needs in the topic and, finally, check whether there is a potential for a wild card.

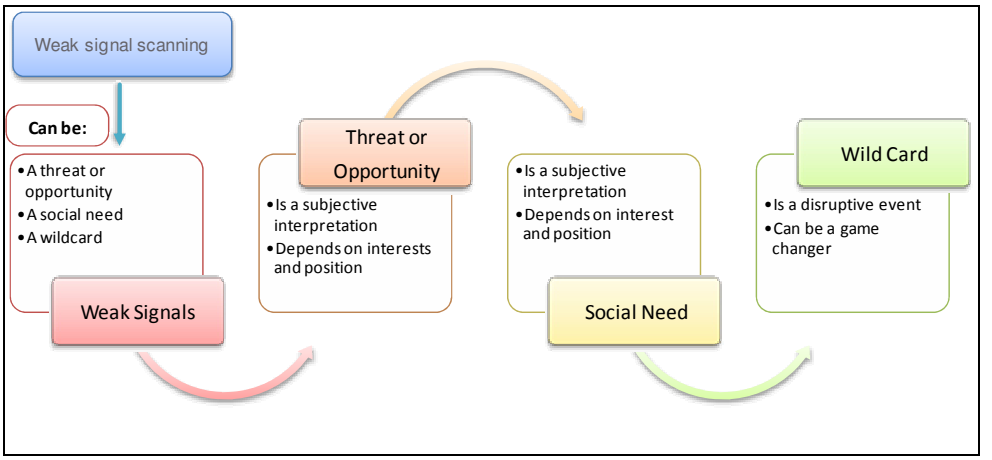

Figure 4. Analytical process in signal mining

The first scan produced the impressive conclusion that automatic weak signal detection works with the TIA. However, for threat identification and wild card detection, a semantic analysis with additional human judgement from experts was necessary.

Weak signals in the cyber domain

Weak signals are small and, therefore, often early signs of events which point to future threats, opportunities, needs or wild cards. In particular, the weak signals with a potential to be wild cards often point to future strategic discontinuity. Therefore, they have a high analytical value for strategic long term planning.

The following list of weak signals is a small selection of the weak signals, which were identified in the ETTIS weak signal mining with internet data.

ID	Selection **of identified weak signal**
1	Stuxnet as first SCADA attack software platform
2	Increasing amount of advanced persistent threats (APT)
3	Black Market prices explosion of Zero day exploits
4	New military cyber attack units
5	Better modular botnet development platforms
6	Trojan horse software service industry
7	Globalisation of information supply chains, strategic sourcing and cloud services
8	The Increasing Power of Transnational Corporations
9	Dark nets and cryptographic peer to peer nets for anonymous publishing and whistleblowing
10	Global black hacker industry and black markets
11	Increasing epistemic networks for knowledge exchange in organised cyber crime
12	Takeover of virtual currency supplier, by organised crime
13	A new power on the horizon - Global virtual communities
14	Geoshifts in Innovation
15	Increasing Mass Surveillance
16	Sensors and Tracking: Finding Anything, Anywhere, Anytime
17	A Droid for All Seasons: Robots Become More Versatile

Table 1. Selection of cyber weak signals

On the attacker side, the weak signals with ID 1, 2, 3, 4, 5 and 10 point to the direction that there is high speed professionalisation ongoing in the cyber-attack community. Future attacks, even from criminals, will be more like a targeted attack with sophisticated APTs, as the platform will distribute this expert knowledge to normal criminals.

On the attack target side, weak signal ID 4, 7, 8 point to the direction that there will be a strong increase in cyber capabilities of public services.

Threats and opportunities in the cyber domain

Threats can be a warning that one is going to hurt or punish someone; they can be a sign of something dangerous or unpleasant which may be, or is, about to happen, or they can be a source of danger[11]. In each meaning, the following 3 essential

11 http://www.thefreedictionary.com.

elements are part of a harmful event : a cause of this event (either accidently or by intention) and an effect of this event. Based on the wide geographic distribution of threat discussion on the internet, identified by TIA, it became obvious in the analytical work that a threat is a subjective interpretation of a specific event. If this event is harmful to a person or a group, this event is considered as a threat by all group members. This opinion is not necessary shared by other groups and all other human beings. In particular, there might be another group which takes advantage of this event. The group will not usually consider this event as a threat.

Typical future threats in the cyber domain are governmental cyber espionage and spying, economic cyber espionage, cyber warfare as part of hybrid operations, data leak, - loss, and - trading events on black markets, unexpected results from large scale data fusion, an increasing amount of insider attacks, cyber extortion (economical), terroristic sabotage (government and critical infrastructure), an increasing amount of commercial and political disinformation, cyber bullying / reputational damage and all sorts of cyber crime.

Nevertheless, threats and opportunities are always a subjective expression of values shared within the group. An opportunity might either be a favourable or advantageous circumstance, occasion or time, or a chance for progress or advancement. The advantage is usually related to a specific group. Thus this group will consider the favourable event as an opportunity.

Disruptive events and wild cards in the cyber domain

Wild Cards are high-impact events that seem too incredible to believe. Therefore, they tend to be overlooked in long term strategic planning. Often, this even leads to a decline in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, „wild cards" refer to low-probability, high-impact events, as introduced by John Petersen, author of 'Out of The Blue -

How to Anticipate Big Future Surprises'[12]. However, more important than probability is that these topics are not well known and not part of the mainstream discussion.

To create this difference, the word disruptive event is used for high impact issues, which are not in the mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However, for strategic long term planning and scenario development they are very important, as they increase the ability in scenario planning to adapt to surprises arising in turbulent chaotic environments. In trend analysis, they point to trend breaks and tipping points.

The following table shows a small selection of possible disruptive events in the cyber domain.

	Possible disruptive Event
Cyber war	Sophisticated SCADA attack platforms (cyber weapons)
	New advanced persistent threats (APT), like Ghostnet, reconnaissance for future cyber conflicts
	Black Market prices explosion of Zero day exploits, as signal for military armament
	Trained and well established military cyber attack units, as signal for military armament
Organised crime	Modular botnet development platforms, as signal for globalisation of organised crime
	Trojan horse software service industry as support for sophisticated cyber crime
	Global black hacker industry and black markets
	Epistemic networks for knowledge exchange in organised crime
	Virtual currencies and organised crime
	Criminal networks in the era of globalisation
Increasing risk	Globalisation of, ICT service sourcing and cloud services, "my data is nowhere industry"
	Global advertising networks and private data exchange without any legal restrictions
	Cyber espionage of non-state actors to get knowledge about nuclear bombs

12 Petersen, J. (2000) 'Out of The Blue - How to Anticipate Big Future Surprises' Madison Books.

Society	Dark nets and cryptographic peer to peer nets
	A new power on the horizon - Global virtual communities
	A society of surveillance
	The establishment of an international cyber army
	Public services, private provider in cyber services
	Geoshifts in cyber innovation, from industrialised countries to new economies
	Digital sensors and tracking: finding anything, anywhere, anytime
	Security: marrying technological and human approaches

Table 2. Selection of possible future disruptive events in the cyber domain

Capability Development and Research Portfolio

Suggestions for research and for new capabilities can be derived from weak signal analysis and disruptive events. Assuming that cyber defence systems (CDS) are a good approach to the increasing perfection of APT attacks, specific research needs can be derived.

Research has shown that companies consistently leverage their R&D spending and demonstrate strong alignment between innovation and corporate strategies (as well as being attentive to the market and their customers' needs)[13]. In adaptive management, company strategies are formulated with reference to actual future expectations. In addition to this, the strategy is changed according to new weak signals, new threats, opportunities and disruptive events.

The following mind map shows research topics (for public financed research), which might be useful for developing new CDS capabilities, assuming that APT attacks are becoming more sophisticated in the future and that companies underestimate the APT threat.

13 Jaruzelski B. and Dehoff K. (2008) "Beyond Borders: The global innovation 1000", Strategy and Business, No 53, Winter.

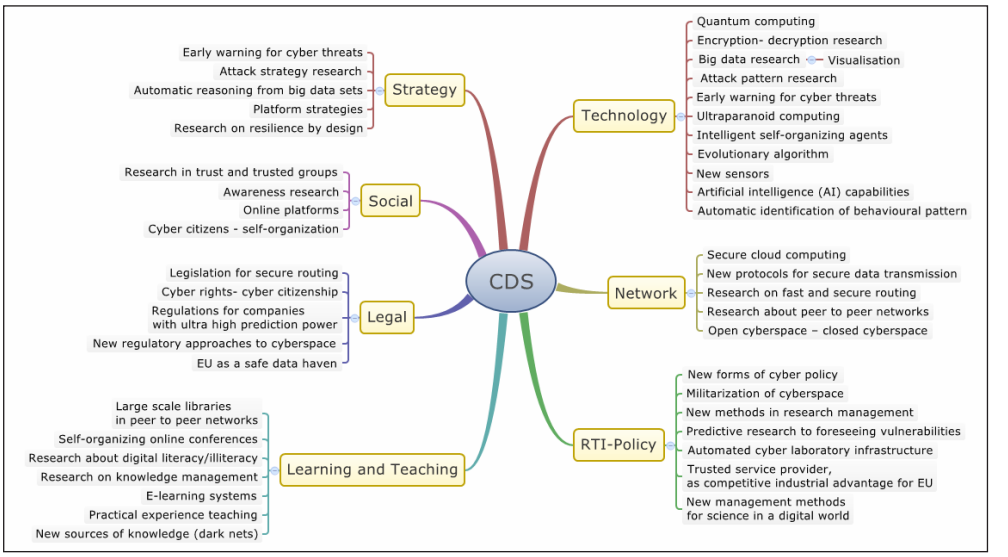

Figure 5. Selection of future research opportunities in the cyber domain[14]

"The capabilities and competencies that the security organisations possess are critical to their performance. However, we need to recognise that those capabilities may reside outside the organisation as well as within it. The ability to access capabilities that are external to the organisation (e.g. research labs, innovation brokers, academic institutions) is critical in many security organisations and this speaks for the importance of external environmental scanning; the capability to develop effective networking with external knowledge provides; and, the development of the absorptive capacity necessary to integrate external capabilities with internal competencies."[15]

Thus, the proposed research topics address the building of "public knowledge" to increase the ability of national companies to address APT attacks. Consequently, this increases the resilience against espionage with APTs and protects the competitive knowledge of national companies. However, public financed research is costly and should only be financed to address real social challenges.

14 ETTIS, D5.4, **results from Threat Identification Agent (TIA), developed by Joachim** Klerx.

15 Joachim Klerx, Andreas Kasztler and Jillian Yeow, "Strategic foresight and innovation management in security research", upcoming in 2015.

Adaptive Management with Risk Monitoring and Capability Planning

Adaptive management can reduce the risk of wrong investments in a fast changing environment. With reference to the last chapter, the investment in CDS research can be distributed over the next few years. An adaptive innovation strategy would make the investments in CDS dependent on the increase of APT attacks and impact of the financed research. However, this is just an example of how to use the results from semi-automatic horizon scanning.

In more general terms, for visualisation or representation of risks for the domain cyber space in correlation to the supply chain networks, , CentDoc has co-developed, as part of a research project[16] consortium, a concept for risk monitoring based on data, information and knowledge. This Risk Performance Monitoring System (RPMS) is founded in Knowledge Performance Monitoring System (KPMS)[17].

This RPMS can be used for strategic risk monitoring for companies and public services for monitoring cyber risks individually and in relation and interaction to global, continental, supra-national and national supply chain networks[18]. The RPMS represents the correlation between knowledge product and risk product or, in other words, correlation between knowledge mapping and risk mapping. The RPMS is a prerequisite for using the results from semi-automated horizon scanning and foresight for risk mapping, according to the monitoring concept, described in the Z-model.

16 financed by Austrian BMVIT/FFG KIRAS Project 840905-META RISK: Meta-Risk-Model for critical infrastructures (www.kiras.at). partly published in GÖLLNER, Johannes, BENESCH, Thomas, SCHAUER, et al. Framework for a Generic Meta Organisational Model. 14th FRAP - Finance, Risk and Accounting Management Perspectives Conference Oxford, U.K., 2014, paper Nr. 100.

17 Published in Woitsch R., Mak K., Göllner J., Grundlagen zum Wissensmanagement im ÖBH Teil 2: Wissensbilanz als Steuerungsinstrument im ÖBH: Ein Evaluierungs-Rahmenwerk aus der Sicht praktischer Anwendungen. National Defence Academy, Vienna. 2010, ISBN 978-3-902670-47-2.

18 EU FP 7-Project: FOCUS- Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles, Deliverable 5.2: EU 2035 roles related to critical infrastructure & supply chain protection. http://www.focusproject.eu/web/focus/wiki/-/wiki/THEMATIC_SCENARIO_SYLLABI/Scenarios+for+%22EU+2035%22+roles+%28futuristic+mission+scenarios%29+as+a+security+provider.

Future Outlook

Given the limitations of single research actions, there is a need for institutionalisation of knowledge development and horizon scanning in a professional horizon scanning centre. Until now, virtually every country has administrative units that deal with strategic planning and the preparation of relevant knowledge for strategic long term planning. Given the new methods for knowledge management, automatic information retrieval, and information analytics, it would be a huge improvement in efficiency to use these methods for horizon scanning.

The search for new and relevant topics to support strategic long-term planning is not new. However, the approach using knowledge management and software support is different than the classical approach and has huge efficiency gains. In recent years, more and more horizon scanning centres are appearing worldwide. Some of them, like the RAHS in Singapore, are focused on automation. But the degree and approach is very different. Other countries, such as Brazil and Russia, announced that they are working on the development of HSC. However, it was not the goal of this publication to accommodate these centres.

Nevertheless, in the long run, it is necessary to include all the very different types of knowledge in the HSC to effectively support the long term planning process of adaptive innovation management.

The following figure shows a process model for a typical horizon scanning centre and how to integrate foresight knowledge in this continued scanning process.

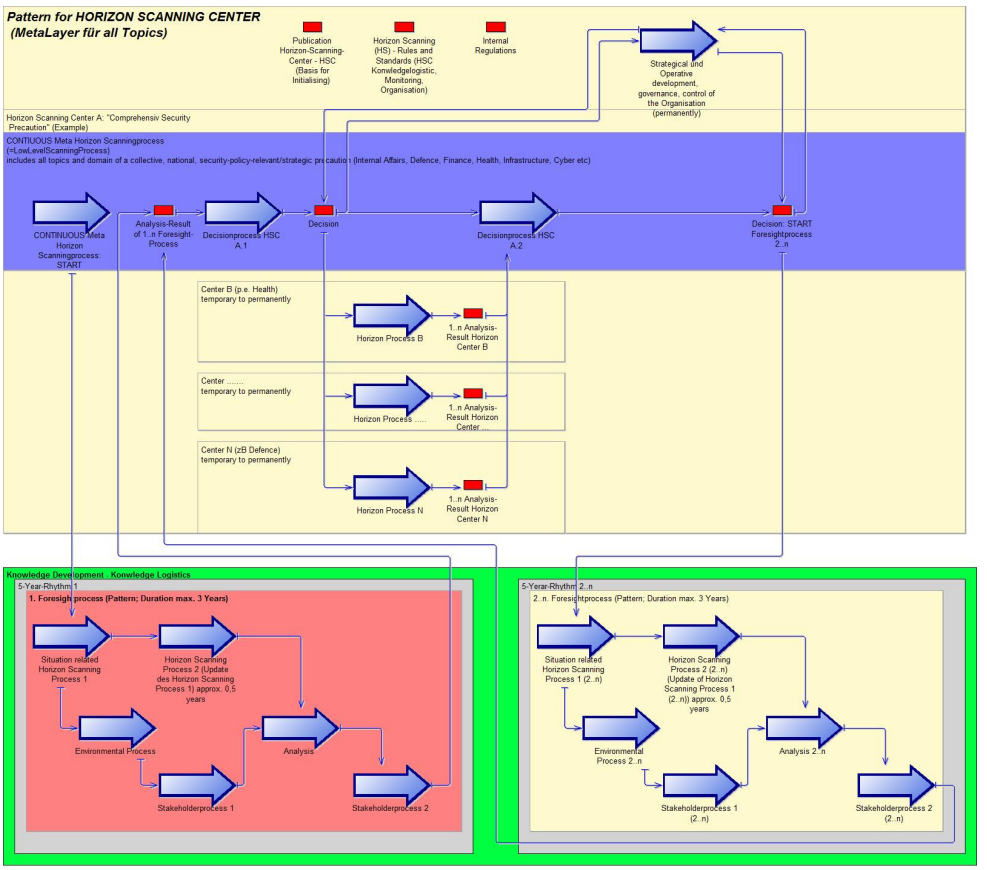

Figure 6. HSC Process Description for Integration external Foresight-Processes[19]

19 Source: Göllner, Johannes, Klerx, Joachim, Mak, Klaus, Meurers, Christian, 06.02.2015, based on the generic basic concept von Johannes Göllner, Joachim Klerx, Klaus Mak von 03/2012-04/2012 for EU-FP7 research proposal „SecScan".