COMPREHENSIVE SECURITY RESEARCH TO CONTRIBUTE TO CRITICAL INFRASTRUCTURE PROTECTION

CONTRIBUTIONS TO SECURITY GOVERNANCE IN DISASTER RISK REDUCTION

Rosemarie Stangl[1], Alexander Siedschlag[2], Diana Silvestru[2], Florian Fritz[2], Andrea Jerković[2]

ABSTRACT

Critical infrastructure protection (CIP) has become a major issue in civil security, emergency management and natural hazard management. The all-hazard approach has gained ground on the international scale, and the "comprehensive approach" in security policies and security research has been advanced in order to meet current and future threats based on better integrated information, assessment, policies and capabilities. This paper aims to showcase this "comprehensive approach", highlighting its character and cross-links to CI and natural hazard and disaster management. The paper also contributes to a broader perspective on CIP by addressing current European political concepts and socio-cultural conditions, as well as possible future EU roles. A focus is put on international critical infrastructure (CI) risks, and results from an Integrated Risk Taxonomy are presented. The paper concludes with proposing socio-cultural aspects for future research topics related to CI risks and security governance.

Keywords: security research, comprehensive approach, critical infrastructure protection, integrated risk governance, emergency management

INTRODUCTION

Security research is still on its way to establish itself as an overarching academic discipline. It developed from research funding programmes, including the security theme of the 7th EU Framework Programme (FP7) as well as national initiatives such as the Austrian KIRAS programme and national security research programmes in other European countries. Those programmes share a civilian focus (including dual-use aspects). Both on the European and national level civil security is strongly associated with protection of the citizens, and comprehensive critical infrastructure protection, addressing all relevant hazards and threats (such as natural hazards, terrorism, infectious diseases, criminality, technological/industrial accidents etc.) and their interconnectedness. Security is generally understood to comprise a society's efforts to maintain and improve its commonly acquired material and immaterial values, including prevention and reduction of hazards and prompt and efficient relief actions in case of emergencies or events. The aim of security research is to prevent and manage primary physical and material damage such as disruption and breakdowns from flooding, eruptions, fires, emissions, from physical or from cyber-attack, and also the prevention and handling of secondary damage such as social, psychological or economic damage. This requires integrating research from social sciences and humanities with technological, natural science and/or engineering.

[1] DI Dr. Rosemarie Stangl, Corresponding author: CEUSS | Center for European Security Studies, Sigmund Freud University Vienna, Schnirchgasse 9a, A-1030 Vienna. (e-mail: rosemarie.stangl@sfu.ac.at).

[2] Prof. Dr. Alexander Siedschlag; Bakk.phil. Diana Silvestru; Mag. Florian Fritz; MMag. Andrea Jerković, MPA: CEUSS | Center for European Security Studies, Sigmund Freud University Vienna.

Therefore, there is no single technical or technological approach to security, and neither to security research (Geiger 2009: 6, 19). Consequently, recent European concepts have put a comprehensive approach at the centre. Noticeable efforts have been undertaken by the EU to pursue a more integrated und multi-dimensional course of action.

This paper is based on results from a recently concluded Austrian pioneer project (SFI @SFU) funded by the national security research programme KIRAS. The project aimed to establish and improve national comprehensive security research at academic institutional level, and to contribute to the advancement of the KIRAS-programme. Special focus was put on the consolidation of the human, social and cultural scientific aspects and components of security research in common security research conception and practice, in particular for CI vulnerability determination and protection, and crisis and disaster management. Additionally, this paper reports first results from the FP7-project FOCUS on "Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles" that among other "big themes" explores future challenges to EU security roles in natural hazard management and critical infrastructure protection, and how planning of future security research could best take this into account in order to support those EU roles.

After explaining the applied methods, the concept of the comprehensive approach is elucidated. Subsequently, current international political and experts discussions on the CI concept are highlighted Following on from this, European CI protection strategies and programmes are critically summarized, focusing on Germany, the UK and Austria. The next chapter presents results from secondary analysis of case studies on social effects of CI breakdown and is complemented with results from an Integrated Risk Taxonomy elaborated from current risk profile documents. The paper concludes with identifying future security research requirements and potential contributions to further refining the comprehensive approach on the conceptual and the practical level.

METHODS

To identify weak spots in critical infrastructure protection and related disaster management, the SFI@SFU-project chose a multi-dimensional and multi-methodological approach:

1) To improve public discussion and to raise awareness of social security risks, research dialogues between public authorities, stakeholders, critical infrastructure operators and the scientific community were initiated and workshops were organised on a national basis.
2) The expert dialogues were supported by structured expert inquiries, questionnaires and Delphi polls.
3) International scientific and political security related conferences were attended and strategically analysed in terms of future international security and research requests.

From these a series of experts' requests to future research topics and orientation was collected and a criteria catalogue was deduced. Further SFI@SFU-project related studies included:

- integration and systematization of most recent risk assessments and assessment of subjective protection requirements for critical infrastructures;
- deduction of socio-political effects from critical infrastructure break down;
- deduction of indicators for subjective criticality assessment from individual risk perception and attitudes;
- catalogue of interfaces between technical and social science aspects in security research;
- comparison of international emergency management policies (co-ordination, competences and emergency organizations).

The studies were based on 1) secondary analyses, 2) desktop research and 3) literature reviews and comprised the 4) analyses of political strategic documents with focus on security and disaster management. The following chapters address selected results from these studies and highlight current political and experts discussions on the critical infrastructure concept, on specific risk views and on protection strategies and programmes.

THE COMPREHENSIVE APPROACH

Comprehensiveness basically means to address the range of threats and challenges by the full menu of instruments in order to contribute to overall stability and security. "Comprehensive approach" refers to both an operational approach and theoretical concept summarizing efforts that, by coordination of different actors and strategies, try to achieve political targets in the increasingly complex environment of international crisis management. Originally the term was used by NATO but, with the emergence of "security research", has undergone significant extension of scope. The EU, referring to "comprehensive approach" as a concept pertaining to international crisis management (denoting a harmonized deployment of resources, capabilities and capacities throughout all the crisis management cycle phases from primary prevention to reconstruction) in the first place, later started to apply the term to the field of civil security and civil security research, primarily to describe methodological requirements for research projects to meet. However, civil protection, crisis management and appropriate allocation of financial and other resources, as well as saving human lives from anthropogenic and from natural disasters play an increasing role in contemporary concepts of comprehensive security, abroad and domestically.

Analyses attempting to synoptically summarize the concept are rare and are limited to the area of international civil-military crisis management. Given the KIRAS-programme's objective to implement a comprehensive approach and given the SFI@SFU-project´s objective to develop an institute for "comprehensive security research", raised the need to analyse the concept in a differentiated and cross-cutting manner. To this end, evidence for 40 different semantic manifestations of the term as such has been gathered so far (as March 2011), exploiting the relevant national and international policy and research-related documents.

The more the term "comprehensive approach" expanded across sectors, the more its contents became more blurred and more intuitive. The quantitative analysis undertaken has provided a valuable foundation for further elaboration of the term as an analytical concept within security research. A generic set of core definitions could be established by SFI@SFU and FOCUS analyses of national, European, and international strategic documents (sorted by decreasing relevance):

- systemic approach to assessment and decision making;
- bundling of different efforts on national and international level;
- coordination (as opposed to integration or standardization);
- burden-sharing of all actors involved;
- „interventionist approach": the integration of the people and actors directly concerned into the problem-solving process of security problems is not a priority.

Interestingly, the exchange of information, acceptance and a common operational picture do not play a role in the majority of incidences, as does the original semantic context of the term: civil-military coordination (which by now has significantly transcended). Austrian approaches, especially in the context of KIRAS, emphasize the dimensions of information exchange and common operational picture in the framework of a "comprehensive approach". They could become an international role model. In order to truly enact a "comprehensive approach" to the state of the art, the practical use for concrete security tasks and for education and training should rely on well-defined interfaces and the required institutional adaptations. Also, a differentiated display contributes to the clarification of the concept which hitherto has been seen rather as a terminological blur. This is important for the scholarly as well as the practical objectives of national and European security research.

INFRASTRUCTURES, SECTORS AND CRITICALITY

The concept of critical infrastructures (CI) and CI sectors is not self-evident. Rather, the sector designation is a permanent process of awareness rising on the political level, characterized by spatial and temporal variation and influenced by various national trends, by the political situation and current crises and disasters. Involving increasing accuracy and detailed perspectives, the process is dependent on public and trans-boundary discussion and views, but also on subjective/political perception, region-specific priorities and economic values (see also Metzger, 2004).

Internationally, the trend towards more coordination and convergence on core sets and indicators of criticality becomes apparent. A SFI@SFU-study focussing on sector specification showed, that predominant consensual sectors are physical-technical infrastructures such as energy infrastructures, ICT (information and communication technologies), water and transport infrastructures. Conversely, socio-cultural sectors (including administration, authorities and government units, security and emergency services, scientific, cultural and commercial facilities, media, but also the chemical and CBRNE-(chemical, biological, radiological and nuclear explosives)-related industry currently are rather heterogeneous in designation. Deviation in criticality assessment generally results from diverging national situations and (legislative and cultural) preconditions: Are there culturally valuable goods? Are there hazardous chemical and industrial goods? Are there security facilities? In case of positive answers to such questions, these sectors usually are assessed to be critical and risk prone both in definition and in the political perception and discourse.

During the designation process of the past years a further trend became evident: originally, physical infrastructures, addressing assets and systems in terms of technical structures (such as communication networks, information technologies, supply chains) and traditional sectors (e.g. transport and energy), were classified to be particularly critical (Gordon and Dion, 2008: 3-4). Less conventional infrastructure sectors such as food and health sector, government units, emergency services, cultural assets and media structures were only recently appreciated to be of critical significance for society. Not only the disruption of physical-technical but also of socio-cultural ("soft") infrastructures is increasingly acknowledged to potentially cause substantial consequences to a nation and its societal functioning.

The International Risk Governance Council (IRGC, 2007) provides a dimension-based perspective and sets infrastructure criticality at three variables: the geographic dimension of disruption and breakdown (local to international), the magnitude (low to massive) and the time factor (short term to long term). Metzger (2004: 73-80) distinguishes 1) symbolic criticality (the cross-linking is rather critical than infrastructure itself) from 2) systemic criticality. However, he cross-links criticality with interaction and inter-dependencies between infrastructures (e.g. energy – transport – information networks). Additionally, criticality is strongly affected by political perception: individual cognition, the illustration of threats and other factors such as a bias caused by membership to a political faction are crucial for the political discussion of threats and their prioritization.

The assessment of infrastructure criticality, its components and potential disruption are crucial for infrastructure and security management. But objective quantification and determination of criticality are doubtful. Hence, qualitative knowledge of physical risks and social vulnerabilities is essential to determine indicators and factors such as risk perception, individual cognition, political discourses, loss of trust, and public reaction to disastrous events and counter-/ mitigating measures. Most recent trends to assess infrastructure criticality involve multi-perspective analyses and assessment procedures decoupled from existing analysis tools and subject-specific bias, and move beyond the deficiencies of conventional single-perspective approaches. This complies with the demand for objectivity and attempts to adequately capture the complexity of technical and societal systems by integrating society-related indicators and parameters.

Critical infrastructure and supply chain protection have centred on aspects like the massive impacts of disruptions and failures on society (such as loss of lives, public disturbances, and economic damages). Public-private partnerships and international cooperation are recognized as a prerequisite to realize the protection of both critical infrastructures and supply chains. The need for general risk assessments, awareness building, and closing of gaps on the levels of organizations, technology,

political strategies, and countermeasures has been highlighted. However, future development of threats, technological and structural risks, relating to changes in technology, political, economic and social affairs as well as changes in values, ideologies, and beliefs are often not considered – providing an important challenge for future research.

CRITICAL INFRASTRUCTURE PROTECTION – EUROPEAN AND SELECTED NATIONAL POLITICAL CONCEPTS (EPCIP, APCIP, GERMANY AND UK)

The *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection* (EU, 2008) provides commonly adopted definitions of *"critical infrastructure"* and *"European critical infrastructure"*. Basically, owners, operators and respective member states hold the responsibility for CIP. The EU encourages the member states to set up national programmes for designation and qualitative and quantitative aspects, to accomplish sector identification and dependency studies and to elaborate a common terminology, general criteria, guidelines and procedures as a first step. Further steps include identification of deficiencies, suggestions for measures and financing, the implementation of minimum protection standards and their surveillance.

The EU-Directive 2008/114/EC introduces a practice to identify and designate European critical infrastructures (ECI), committing each member state to designating potential ECI according to the EU-definition and according to cross-sectoral criteria (casualties, economic and public effects) and sector specific criteria (taking into account individual sector characteristics). Further criteria to be considered, as addressed in the *European Programme of Critical Infrastructure Protection* (EPCIP) (European Commission, 2006: 7), are geographic scope of impact (when disrupted or destroyed), severity and consequences (public, economic, environmental, political and psychological effects, public health consequences) or geographic and sector specific dependencies.

The EPCIP points out the all-hazard approach (prioritizing terrorism) and the principles of subsidiarity, complementarity, confidentiality, stakeholder cooperation, proportionality and sector-by-sector approach. The framework comprises the identification and designation of CI, an action plan, the establishment of a *Critical Infrastructures Warning Information Network* (CIWIN) and a CIP *Contact and Expert Group*; further the support of the member states, a contingency planning and the external dimension. The objectives to guarantee European-wide adequate and equal protection levels, minimal single points of failure and rapid and tested recovery processes were defined earlier on (Commission of the European Communities, 2005: 3-13).

Together with the member states, the EC will develop guidelines and thresholds for criteria application. As a first step the directive addressed the energy and transport sectors differentiating subsectors for each (electricity, oil, gas respectively road, rail, air, inland waterways transport, ocean and short sea shipping, and ports).

To implement the EU-Directive 2008/114/EC, Austria developed the *Austrian Programme for Critical Infrastructure Protection* (APCIP) according to the EU-characteristics (BKA and BMI, 2008). Strategically, APCIP strives for the identification of Austrian critical infrastructures (ACI), their protection by prevention and rehabilitation measures and vulnerability reduction towards natural hazards, technical and human failure, terrorism and organised crime (all hazard approach, MASTERPLAN, 2008). Classification criteria for sector designation include 1) number of affected citizens with respect to health and social impacts; 2) economic impacts; 3) environmental impacts; 4) psychological impacts; 5) spatial dimension; 6) period of impact; 7) lack in substitution and alternatives; and 8) interdependencies.

In accordance with the European Programme the APCIP-MASTERPLAN delineated eleven sectors (see Tab. 1). Nuclear industry and space facilities are considered to have no significance for Austria, but additional focus is put on constitutional facilities, maintenance of public welfare and distribution systems, emergency services and relief units. Sector designation is not finalised yet, hence different

sources slightly vary in sector information and are based on different (European) sources. Tab. 1 presents a comparative overview of the preliminary deduced sectors, illustrating deviations in designation and description and demonstrating that sector designation is a continuous political awareness process as previously mentioned. A final list of the Austrian CI-sectors is announced for past risk and criticality analyses. Regional and local deviation in prioritization and, hence, deviating sector emphasis on national and federal level is expected.

Tab. 1 Comparison of preliminary deviated Austrian critical infrastructure (ACI) sectors

	APCIP-MASTERPLAN (2008: 5)	**EPCIP-sectors as basis for APCIP-sector designation (in MASTERPLAN 2008: 5)**	**KIRAS-Research Programme (BMVIT 2008: 6)**	**EU-Communication COM(2004) 702 as basis for KIRAS-sectors (Commission of the European Communities 2004: 4)**
Physical-technical sectors	Energy	Energy	Energy	Energy installations and networks
		Nuclear Industries		
	ICT	ICT	Communications and Information	Communications and Information Technologies
	Transport	Transport	Traffic and Transport	Transport
	Water	Water	Water	Water
	Chemical Industry	Chemical Industry	Production, Storage and Transport of Dangerous Goods	Production, Storage and Transport of Dangerous Goods
Socio-cultural ("soft") sectors	Food	Food	Food	Food
	Public Health	Public Health	Health Care	Health Care
	Finance	Finance		Finance
		Space Facilities		
	Research Facilities	Research Facilities	Scientific Infrastructure	
	Constitutional Facilities		Public Authorities, Administration and Judiciary	Government
	Maintenance of Public Welfare and Distribution Systems			
	Emergency Services and Relief Units			

Germany is mentioned here as an example for offensive and pioneer CI policies: it has been actively pursuing strategic arrangements for CIP since 2005. The German government developed a *Basic Protection Concept* with recommendations for operators (BMI, 2005a), a *National Plan for Critical Infrastructure Protection* (BMI, 2005b) and the *National Strategy for Critical Infrastructure* (BMI, 2009). It further provided an *Implementation Plan for Critical Infrastructure Protection* (BMI, 2007) and *Guidelines for Operators and Authorities* (BMI, 2008). However, in the United Kingdom, resilience and continuity programmes for CIP are relatively novel (Cabinet Office, 2010a and 2010b) and predominantly refer to natural hazards. This is due to the rather recent establishment and specific mission of the *Natural Hazards Team* in the *Civil Contingency Secretariat* in 2009, a subsequent response to the floods of 2007. The previously set up *Centre for the Protection of National Infrastructure* (CPNI) provided security and protection advice and support to reduce vulnerability to national threats, but the relation to natural hazards was introduced only later. Though information on climate change and related risks is available, the general understanding and awareness of future weather-related extreme events are rather low. The lack in systematic and shared comprehension of a vulnerability scaling for each sector was acknowledged, and the protection framework was perceived to be patchy and inconsistent (ICE, 2009). For a long period, ad hoc responses to specific events were a common practice but are now being changed to measures centred on foresight and anticipation. The British *Critical Infrastructure Resilience Programme* (see Houses of Parliament, 2010) aims to

prepare and initiate prevention and protection activities focussing on preparedness for natural hazards, on response and on recovery. According to Cabinet Office (2010b: 7), key components have to be identified to increase resilience and robustness, and even "hard core" measures such as relocation as a long-term option have to be taken into account.

In conclusion of this chapter, the authors would like to come back to the European level: In its communication on the *EU Internal Security Strategy* the European Commission (2010a: 8-11) appeals for uniform risk analyses based on standardised criteria to establish a *Common Risk Management Framework* (CRMF), also including risk information and risk-based controls. Based on the *Security Strategy* and *the Communications on the Prevention of Natural and Man-made Disasters* (European Commission, 2009), the EC developed *Risk Assessment und Mapping Guidelines for Disaster Management* (European Commission, 2010b) to support the member states in their efforts and contributions for a *European Risk Atlas*, serving as a further basis for an adequate coherent all hazard risk policy due to be established by 2014.

SOCIO-POLITICAL EFFECTS AS RESULT OF CRITICAL INFRASTRUCTURE FAILURE

It is generally acknowledged that failure of CI, such as malfunctions and accidents in transportation, health service, emergency care or power supply, has an impact on the social components of a system. If an infrastructure-endangering event occurs, domino effects and/or cascading effects are very likely due to interference or outages of the critical infrastructure. Those effects have the potential to bring different sectors of society to standstill. In addition to direct harm to citizens and economic losses this often generates loss of confidence in the political system.

Crises and disasters always take place in (social) contexts. Decades of investigations in the field of disaster research have shown that natural disasters (floods, hurricanes, tornadoes etc.) do not only affect society economically – for example through physical loss of structures, homes, plant closures etc. – but also have negative psycho-social consequences on the affected community. Recovery through an efficient organizational response reduces such negative effects.

Case studies (such as from Platz, 2006; Birkmann, 2010; Lorenz, 2010) – based on interviews with disaster victims, site investigations and questionnaire surveys – describe *inter alia* the various social affections and implications in the wake of CI failure. Several impacts identified through the SFI@SFU desktop research on hitherto available case studies are summarized in Tab. 2.

Tab. 2 Identified types of citizen affections and perceived social impacts in case of CI failure

Failure or breakdown of critical infrastructure	*Types of citizen affections and social impacts*
Power Supply	• Operating failures of electrical devices without emergency power supply (fridge, computer etc.); • Defrosted food as potential source of human disease; • Impossibility of buying and selling food and other goods as a consequence of the shortage of cash supply based on the failure of electronic payment systems. Disturbance of various services in the retail industry; • Disturbed consumer behaviour, e.g. demand for (cold) instant meals and ready-to-serve food; • Collapse of small healthcare providers like medical practices/pharmacies; • Disturbance of the water supply and sewage system; • Disturbance of the public and private transport sector through failure of lamps and street lighting; • Anxiety, fear, insecurity, uncertainty and even panic provoked by lasting blackouts of unknown cause • However, short-term blackouts induce pro-social, friendly attitudes, even enthusiasm and willingness to help those affected. • Disturbance of typical social routines, appearance of social conflicts; • Plundering, rapes, robberies, revolts; • Increase in personal communication and significance; • Consolidation of social relationships;
Water Supply	• Quality reduction of potable water due to excrements, bacteriological or chemical

	contamination or to pathogenic agents in the pipe network; • Particular exposure of vulnerable groups (children, elderly people, pregnant women or persons with immune deficiencies) to the occurrence of infectious diseases; • Impairment of hygienic measures like hand washing and sewage disposal; • Risk of flooding due to inundation of the sewage system.
Public Health	• Life-threatening risks for patients, homes for elderly and nursing homes; • Overcrowding of the temporary care facilities.
(Tele-)Communication	• Impairment to use telecommunication bypass strategies; • Communication difficulties among action units can affect the waiting periods for victims and slow down their rescue.
Transportation systems	• Risk of isolated victims due to the inaccessibility of blocked/damaged streets and bridges; • Difficulties in locating specific addresses of victims by action units due to loss of/ damage to the road signs.
Insurance industry	• Damage caused by natural disasters usually is not covered. Adjustments /upgrading of policies result in a drastic increase of the insurance charges to be supported by the affected.

The identified types of citizen affections and social impacts resulting from CI failure give a clear description on the multiple vulnerabilities of the social system and its indispensable connections with the various CI. It can be concluded that the complexity of the social consequences from CI failure increases with increasing citizens' dependence on CI. Furthermore, the crisis behaviour also depends on the predominant social patterns and legal frameworks, on the general perceived legitimacy of political, economic and social institutions and on the amount of risk tolerance of the population.

CRITICAL INFRASTRUCTURES UNDER RISK – APPROACH TO MERGE MULTI-LEVEL RISK PERSPECTIVES TO AN INTEGRATED RISK TAXONOMY

Based on the *"Risk assessment and mapping guidelines for disaster management"* (European Commission, 2010a), the EU member states aim for a coherent risk management policy for CI by assessing nationally relevant and/or identified risks. National and international organizations support this effort by suggesting more or less consistent methods (BMI, 2008; BBK, 2010; Harnser Group EC, 2010). Most of these concepts consider technically oriented, single-perspective based assessment instruments but lack in multi-perspective and integrated approaches To support to extend existing concepts by socio-political factors and competences as integral components the FOCUS project highlights the close relationship between critical infrastructures and supply chains: how supply chains depend on transport infrastructures, energy supply, and information and communication technology (ICT); and how their risks interconnect.

The SFI@SFU-project contributed to improving integrated approaches by providing socio-cultural perspectives: Based on a comprehensive review of international literature on risk profiles and political documents, an *Integrated Risk Taxonomy* was elaborated. The classification integrates and merges current multi-level risk perspectives and represents a rather novel approach. Literature differs with regard to main and consequential risks; hence it seemed appropriate to detail a more specific classification according to primary, sub- and secondary risks. The novelty of this systematization is emphasized by the integration of politically relevant social and economic (secondary) risks resulting *in* and/or *from* disruption of CI. The integration of political risk profiles with experts risk assessments is a case *sui generis* and represents a fundamental basis for integrated risk assessment, the development of future assessment, measuring and protection concepts.

The elaborated risk taxonomy is classified according to 5 common risk categories as illustrated in Figure 1 comprising a total of 22 primary risks computed from the analyses. In the light of the INTERPRAEVENT focus on protection of the environment from natural hazards the following paragraphs will highlight specific systematization details within the category *Natural Risks*.

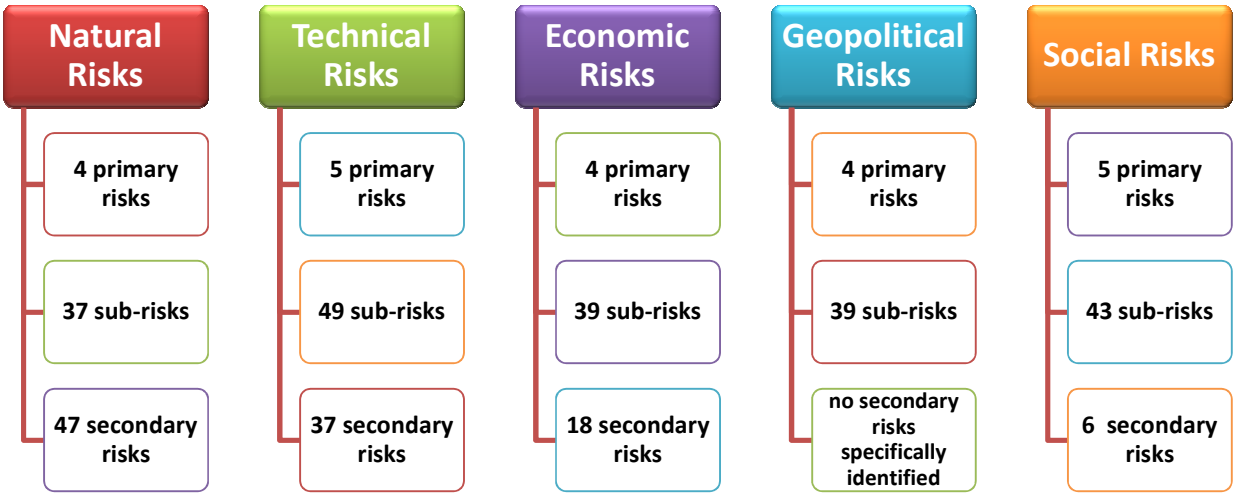

Fig. 1 Integrated Risk Taxonomy with respect to critical infrastructures: structural overview of risk categories and allocated primary risks, sub-risks and secondary risks as identified from currently available risk profiles

Amongst the category *Natural Risks* the systematization demonstrated *Natural Hazards and Disasters* to be generally acknowledged as major primary risk: 18 sub-risks such as flooding, volcanic eruptions, tsunamis, forest fires, droughts, cosmic threats etc. were identified in the analysed documents. Secondary risks, assessed to have - partially severe - socio-economic impacts, were named to be critical infrastructure damage or break down, disruption of water supply, shortage of water and resources, disruption of the supply chain and transport systems, hazards to livelihood, harvest losses, income losses, migration, infectious diseases, social stress, failure of social systems, conflicts, homelessness, social change and many more. According to most recent risk assessments, experts expect the sub-risks geomagnetic or sun storms and space weather, which are rather less known threats and have not appeared yet as alarming risks on the political agenda, to have striking impacts in particular to global ICT or energy infrastructures, and hence to society.

A further omnipresent and transversal primary risk both amongst experts and political actors *is Climate Change*. Sub-risks from *Climate Change* are seen in storm and flood increase, droughts, desertification, sea level rise, increase or shift of wildfires, increase of affected areas and others. As secondary risks disruption of water supply, shortage of resources, conflicts over resources, impacts on disaster management, interactions with social and environmental impacts or migration are repeatedly named in the documents. Beyond that it can be expected that all *Natural Hazard*-related secondary risks mentioned above might be attributed to climatic factors or climate change, too.

Interestingly, *Environment and Environmental Hazards* also identified to be primary risks amongst the category *Natural Risks,* partially coincide with *Technical Risks*: marine oil contamination, increased air pollution and ecological disasters are named to be sub-risks as are climatic disasters and epidemics. Secondary risks are more or less identical to the secondary risks from *Natural Hazards and Disasters*. A further primary *Natural Risk*, *Infectious Diseases,* with sub-risks such as pandemics, epidemics, pathogenics and others, is especially attributed to cause migration, social changes and long-term social consequence as secondary risks.

The risk profile analyses illustrated that failure to acknowledge inter-dependencies between technical CI and CI risks results in uncoordinated and fragmented protection concepts with respect to CI resilience enhancement. Whilst international debates centre on the handling of cascading effects and increasing network resilience, separation of responsibilities is still practiced nation-wide on political, ministerial and operational level, though can no longer be justified. A multi-sectoral approach and joint responsibilities could be a more adequate alternative to the currently rather fragmented operation.

ICE (2009: 9) considers limited knowledge to be one of the greatest risks to critical infrastructures in terms of inadequate financing and funding of infrastructure maintenance. Also the Strategic Foresight Initiative (2011a, 2011b), rating aging or over-aged infrastructures and protective structures (such as dams, dykes, bridges etc.) to be major risks, recommends improved public communication. To support and to improve public knowledge of overall risks, publicly available information with respect to infrastructure location, risk character and nature, effects from failure etc. is essential. ICE (2009: 9) suggests using databases as information basis and for mapping.

In the United Kingdom, a *Centre for the Protection of National Infrastructure* (CPNI), and consequently, a *Natural Hazards Team* have been established for CIP and disaster management planning. These institutions have the mission to create, develop and operate cross-sector CIP and resilience programmes and projects (Cabinet Office, 2010a; ICE, 2009: 4-8). ICE's critics (2009: 4-8) still focus the separate bodies and suggest a high-level coordination authority, which the authors advocate as a qualified model to integrate information, communication and networking in terms of critical infrastructure-network-resilience. It is of critical significance to advance knowledge of (all) risks, information about the location and nature of infrastructures, and potential consequences of a breakdown etc. In accordance with suggestions from ICE (2009: 9) the SFI@SFU-project encourages to link existing databases and hazard maps such as the Austrian HORA (Natural Hazard Overview and Risk Assessment Austria) or hazard zone plans with infrastructure databases and to make them publicly available as open source "CIMs" (critical infrastructure maps) to owners, operators and citizens.

CONCLUSIONS AND FUTURE SECURITY RESEARCH NEEDS

Since the 1990s, several components of risk profiling and CIP have been changed and added, as for example, can be deduced from the *Austrian Strategy for National Crisis and Disaster Protection Management* (BMI, 2009), which is based on the *National Security and Defence Doctrine* from 2001. Shifts in political emphasis have been internationally observed, often in accordance with upcoming challenges from major events (such as the 9/11-terrorist attacks), but natural hazards have continued to be specifically pointed out as infrastructure risks of extensive concern. This is echoed by a report from the British *Institute of Civil Engineers* (ICE, 2009), concluding that natural hazards resulting from climate change (in particular flooding) can be foreseen to constitute the major threat to CI in the long run, surpassing terrorist threats. However, the *Strategic Foresight Initiative* (2011) of the *U.S. Federal Emergency Management Agency* (FEMA) emphasizes that climate change will also cause a shift in threats to previously unaffected areas, and, in combination with other drivers, such as aging infrastructures and urban population growth, will be particularly challenging for future emergency and disaster management.

These examples illustrate that CIP as an important mitigation instrument in disaster management should be based on continuous risk surveillance and on continuous assessment of research demands to effectively adapt measures and concepts. As pointed out in this paper, CIP is a continuing process in both politics and research. Following SFI@SFU final results and FOCUS first results, in line with the "comprehensive approach", future contributions to "*comprehensive critical infrastructure protection*" should in particular address social aspects of technical challenges, such as the following:

- interactions between anthropogenic systems/factors and natural hazards in the overarching context of nature sustainability;
- anthropogenic (or "man-made") natural disasters and multi-disciplinary scenarios of maximum credible natural events – contributing to identifying maximum possible damage from a combination of primary (e.g. destruction by shockwave), secondary (e.g. fires), and tertiary (e.g. supply chain damage, loss of production) effects for a given region, nation, or the EU as a whole;
- socio-technical analyses of cross-sectoral threats to critical infrastructures, including wider impact scenarios;

- cultural and awareness related aspects of communicating CI risks and security aspects to a wider public;
- awareness raising, risk perception, cognition of causes and coherence, and preventive measures;
- potential and limits of mainstreamed CI security standards, also considering social and cultural criteria;
- socio-political, socio-economic and politico-economic impacts of CI breakdown;
- infrastructure requirements from changing demographic and risk patterns;
- identification and elaboration of best-practice preparedness concepts, based on international experience legal framework requirements for the implementation of best practice CIP and crisis response planning scenarios.

Acknowledgements: The research leading to these results has received funding from: (a) the Austrian Ministry of Technology, Transport and Innovation (bmvit), in the context of the project SFI@SFU: "Development of an Austrian Centre for Comprehensive Security Research at Sigmund Freud Private University Vienna" (http://www.sfi-sfu.eu) in the Austrian national security research programme KIRAS (http://www.kiras.at); (b) the European Union Seventh Framework Programme (FP7/2007-2013: (http://cordis.europa.eu/fp7/security/home_en.html)) under grant agreement n° 261633, in the project FOCUS: "Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles" (http://www.focusproject.eu).

REFERENCES

BBK (2010). Methode für die Risikoanalyse im Bevölkerungsschutz. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Wissenschaftsforum Band 8: Bonn.

Birkmann J., Bach C., Guhl S., Witting M., Welle T., Schmude M. (2010). State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall. Schriftreihe Sicherheit Nr. 2 Forschungsforum Öffentliche Sicherheit, Freie Universität Berlin: Berlin.

BKA, BMI (2008). Das österreichische Programm zum Schutz kritischer Infrastrukturen, Masterplan APCIP1. Vortrag an den Ministerrat. Online in Internet: URL: http://www.kiras.at/uploads/media/MRV_APCIP_48_17_2_4_2008_FINAL.pdf. Last accessed: 2011-07-11.

BMI (2005a). Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Bundesministerium des Inneren Referat P II 1: Berlin.

BMI (2005b). Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Bundesministerium des Inneren. Online in Internet: URL: http://www.bmi.bund.de/cln_156/SharedDocs/Standardartikel/DE/Themen/OeffentDienstVerwaltung/Informationsgesellschaft/NPSI.html. Last accessed: 2010-08-24.

BMI (2007). Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Bundesministerium des Inneren: Berlin.

BMI (2008). Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Bundesministerium des Innern Referat KM 4: Berlin.

BMI (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Bundesministerium des Inneren Referat KM4: Berlin.

BMVIT (2008). KIRAS Sicherheitsforschung. Österreichisches Förderungsprogramm für Sicherheitsforschung. Programmdokument für alle Programmlinien des Programmes KIRAS. Bundesministerium für Verkehr, Innovation und Technologie (BMVIT): Wien.

Cabinet Office (2010a). Sector Resilience Plan for Critical Infrastructure 2010. Natural Hazards Team Civil Contingencies Secretariat: London.

Cabinet Office (2010b). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Cabinet Office: London.

Commission of the European Communities (2005). COM(2005) 576 final. Green Paper on a European Programme for Critical Infrastructure Protection (presented by the Commission). Online in Internet: URL: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf. Last accessed: 2011-07-14.

EU (2008). COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union L 345/75. Online in Internet: URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. Last accessed: 2010-10-14.

European Commission (2006). COM(2006) 786 final. COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection. Online in Internet: URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf. Last accessed: 2011-10-14.

European Commission (2010a). COM(2010) 673 final. Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Online in Internet: URL: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf. Last accessed: 2011-08-09.

European Commission (2010b). SEC(2010) 1626 final. Commission Staff Working Paper. Risk Assessment and Mapping Guidelines for Disaster Management. Online in Internet: URL: http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/prevention/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf. Last accessed: 2011-08-09.

Geiger G. (2010). Sicherheit oder Sicherheitstechnologie? Der Beitrag der zivilen Forschung zur Sicherheit Europas. S14 Stiftung Wissenschaft und Politik S14. Deutsches Institut für Internationale Politik und Sicherheit: Berlin.

Gordon K., Dion M.(2008). Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security. OECD-Report. Organisation for Economic Co-operation and Development: Paris.

Harnser Group EC (2010). A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission: Norwich.

Houses of Parliament (2010). Resilience of UK Infrastructure. POSTNOTE Nr. 362. London: Parliamentary Office of Science and Technology: London.

ICE (2009). The State of the Nation. Defending Critical Infrastructures. Institution of Civil Engineers: London.

IRGC (2007). Policy brief. Managing and reducing social vulnerabilities from coupled critical infrastructures. International Risk Governance Council: Geneva.

Lorenz D.F. (2010). Kritische Infrastrukturen aus der Sicht der Bevölkerung. Schriftreihe Sicherheit Nr. 3 Forschungsforum Öffentliche Sicherheit, Freie Universität Berlin: Berlin.

MASTERPLAN (2008). Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP). Online in Internet: URL: http://www.kiras.at/fileadmin/dateien/allgemein/MRV%20APCIP%20Beilage%20Masterplan%20FINAL.pdf. Last accessed: 2010-11-17.

Metzger J. (2004). Das Konzept „Schutz kritischer Infrastrukturen“ hinterfragt. In: Wenger Andreas 2004: Bulletin 2004 zur schweizerischen Sicherheitspolitik. Forschungsstelle für Sicherheitspolitik: Zürich.

Platz U. (2006). Vulnerabilität von Logistikstrukturen im Lebensmittelhandel. Eine Studie zu den Logistikstrukturen des Lebensmittelhandels, möglichen Gefahrenquellen und den Auswirkungen verschiedener Gefahren bei einem Ereigniseintritt. Landwirtschaftsverlag Münster-Hiltrup. (Serie Band: Schriftenreihe des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft : Reihe A, Angewandte Wissenschaft; 512 / ISBN-ISSN-ISMN: 3-7843-0512-1).

Strategic Foresight Initiative (2011). „Getting Urgent About the Future“. Summary of Findings. Online in Internet: URL: http://www.fema.gov/pdf/about/programs/oppa/findings_051111.pdf. Last accessed: 2011-08-09.