This paper is part of the Proceedings of the 10th International Conference on Risk Analysis (RISK 2016)
www.witconferences.com

Awareness of the vulnerability of critical infrastructures to IEMI threats: lessons from Austria

B. Jager, A. Preinerstorfer & G. Neubauer
Department of Digital Safety and Security,
AIT Austrian Institute of Technology GmbH, Austria

Abstract

In recent years, the relevance of electromagnetic threats has increased steadily. In the meanwhile, electromagnetic attacks have been included as one of the novel dangers to critical infrastructures of European societies and beyond. Facing this challenge, the European Commission funded several projects addressing this issue. As one result, the FP7 project HIPOW aims at the development of a holistic regime for critical infrastructure protection against threats posed by electromagnetic radiation in Europe. An examination of policies at different institutional stages issuing the protection against IEMI threats serves as a starting point for evaluating the current protection framework. HIPOW will raise awareness about general vulnerabilities and shortfalls in the design of real-life European critical infrastructure. By making recommendations to policy makers and organisations operating critical infrastructures, HIPOW contributes to the harmonisation of emerging protection frameworks against IEMI threats across Europe. This implies the establishment of a network for operating and supervising protection and preparedness activities to face IEMI threats. Prospective findings will reflect how current protection concepts address identified threats posed by IEMI threats, how overarching strategies are shaping the protection framework and how these strategies may enhance resilience of societies. For that purpose, initiatives intending to increase security will be analysed with regard to their significance for the European security approach.
Keywords: critical infrastructure protection, European critical infrastructures, European security policies, human induced hazards, IEMI, vulnerability.

WIT Transactions on The Built Environment, Vol 160, © 2016 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SUSI16061

1 Introduction

Societal and economic performance specification in high industrialized regions, as in Central Europe, is characterized by its more or less complex electrical and electronic systems needed to meet the requirements of modern urbanity. Habits of today's societies are claiming on a permanent availability of communication and information exchange, electricity, food, water, healthcare infrastructures. Conveniences of on-demand-services are featured by an inter-connectivity of systems and their increasing remote or centralised controllability. Thus, the structure of contemporary societies is strongly dependent from smooth operation of infrastructure assets. In that course, the relevance of such support systems, actually dedicated to facilitate today's way of life, is shifting into the spotlight of the consideration. Infrastructure assets, which are essential for the functioning of modern societies, are in the centre of the current discussion. Those systems are covered by the term "Critical Infrastructure" (CI), which are defined as "[i]nfrastructures or parts of them, which play a crucial role for the maintenance of a vital societal functioning and whereas disturbance or destroying have serious consequences for the health, security, economy and social wellbeing of the population or the effectivity in governing of the government" [1]. An essential characteristic of such CIs is that their operational capability is decisive for the maintenance of the systems in highly advanced societies. Above all, policies on Critical Infrastructure Protection (CIP) does not refer to any specific cause for disruption or destruction, thus includes serious interferences as a consequence of natural disasters, industrial accidents or malicious damage in the sphere of crime and terrorism as well. Blackouts in North-America and Europe during the last two years put evidence on the vulnerability of energy infrastructures and consequently the need to find effective measures to prevent/or to mitigate the consequences derived from a major supply disruption [2]. Europe's critical infrastructures are highly connected and highly interdependent. Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction. Non-state actors as well as state actors pose a serious threat to the security of society by interfering central supply systems. The consequences of an attack to the industrial control systems of critical infrastructure could vary widely. Such incidents are conceivable due to cascading effects as depicted in Figure 1.

The effects of an Intentional Electromagnetic Interference (IEMI) attack can be described by a multi-level and branched functional chain starting with the local distortion of a subsystem. The malfunction might be propagated over the whole system having crucial consequences for the population, industry or affected states [3]. Most CIs are depending on electrical/electronic systems in order to guarantee their frictionless operation. These systems are potentially vulnerable to IEMI attacks and so the United States Department of Homeland Security addressed this topic in a report [4] demonstrating the potential damage caused by electromagnetic weapons.

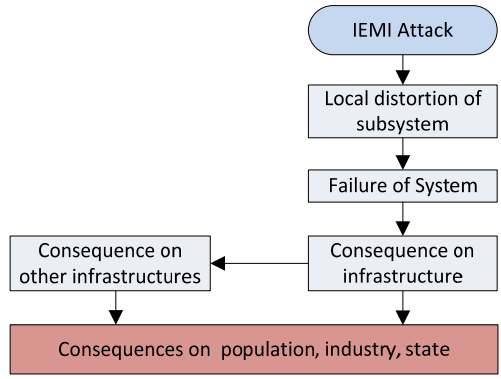

Figure 1: Cascading effects due to an IEMI attack [3].

The use of electromagnetic sources for criminal or other malicious purposes has increased steadily in the last decades. Since the nineteen nineties the use of so called electromagnetic weapons is not primarily limited to the military sector any more. According to the standard IEC 61000-2-13, the overarching term for these radio frequency weapons and the whole topic is as stated by URSI General Assembly, held in Toronto in 1999, IEMI. It is defined as: "*intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes*" [5]. There is a broad consensus in the open literature about the types of sources generating such effects to electric and electronic equipment. The man-made sources are classified into narrowband sources, broadband sources and communication jammers as described in many papers of the IEC SC 77C working group members, which are dealing with high power electromagnetics phenomena, e.g. [6, 7]. These sources differ in their radiated electromagnetic emissions in respect of parameters such as frequency, field strength, output power, pulse repetition rate, but will not be further addressed in this paper. The facts that electromagnetic radiation produced by IEMI sources is invisible and that these sources can be easily hidden in a truck or van makes them very interesting for criminals or persons with malicious intentions to perform their attacks. Moreover, detectors which are effective and cheap at once are not yet on the market and currently under development within different projects. Multiple authors indicate the challenge to trace the attackers, e.g. [8]. Possible targets are electronic components from critical infrastructures such as electronics from data centres or even airports [9]. Due to the fact, that patterns of damage are hardly quantifiable and competent authorities are amenable to secrecy obligation, research on the exposure of CIs to IEMI is challenged to avoid an isolated focus on certain vulnerabilities or specific threat scenarios. Requirements of a resilient community urge to widen the scope from concentrating on single protection approaches at the level of components and subsystems to the consideration of consequences on the society at large. Moreover, strategies for implementation of well-balanced and cost efficient

protection measures (including measures such as access restriction, surveillance, radiation detection, emergency planning etc.) are urgently required. In 2012 an EU FP7 project entitled "Protection of Critical Infrastructures against High Power Microwave Threats – HIPOW" [10] was initiated, aiming at the development of a holistic regime for the protection of European critical infrastructures against IEMI attacks. HIPOW will also raise awareness about general vulnerabilities and shortfalls in the design and operation of real life European Critical Infrastructures (ECI), and advise policy makers and critical infrastructure owners and operators how to improve the electromagnetic immunities of their systems. This includes the development of a network for operating and supervising protection and preparedness of threats arising from IEMI at the level of the European Union and its Member States. According to the scope of the HIPOW project, the focus mainly lies on regulation strategies which reflect on intentional threats arising from IEMI. In contrast to the frequently used all-hazard approach, intentional man-made threats to CI will be put in the centre, while damage caused by natural phenomena as well as unintentionally caused damage, e.g. industrial accident will not be considered in the current paper.

2 Method

In order to promote holistic protection regimes for critical infrastructures, our contribution is intended to stimulate further standardisation activities in the area of threats to critical infrastructures posed by IEMI. Therefore, a two-phase approach is pursued in the frame of this work. While in phase one, information on CI protection will be gathered exclusively by desk research, in the second phase, data obtained by desk research will be compared with statements from representatives of competent authorities as well as CI providers by means of interviews. As a starting point, current protection strategies and programs of the European Union concerning the vulnerability of critical infrastructures are analysed. In particular, provisions on the protection of critical infrastructures against threats from several hazards, drafted by the European Union, will be examined, e.g. the protection strategies of the European Commission. Due to the fact, that national policy makers are in charge of capabilities, required for the functioning of the societal system, the investigation is also concentrated on protection approaches at national level. As an example for the transfer of a European protection strategy into national framework, the implementation in Austria will be evaluated with regard to threats arising from IEMI. A comparison of existing approaches will allow conclusions about the current level of protection against imminent risks, such as IEMI within European Communities.

Following the overarching strategy prepared by the European Union, respectively the European Commission, one implementation approach of national protection concepts – taking Austria as an example will be presented. Initially, links to communities' protection concepts, will be identified by discussing advantages of the Austrian practice. Thus, requirements for further standardization activities will be deduced and entered into drafting a holistic framework for the protection of CI against several threats including IEMI. In that

course, interviews will be conducted with representatives of the responsible ministries in Austria, namely the Federal Ministry of the Interior and the Federal Agency for State Protection and Counter Terrorism, which is also located at the Federal Ministry of the Interior. On the basis of interviews with experts, information will be obtained about (i) the current protection approach at national level, (ii) the distribution of responsibilities in managing CIP and its basis (mandate for operating as competent entity), (iii) the implementation process and its challenges at national level as well as protection concepts in the area of IEMI threats. Main findings from the national use case will be consulted to deduce recommendations, which are transferable at the level of European Communities.

3 Results

The European Community is pursuing a common threat scenario, which affects Member States more or less to the same extent. In order to ensure the guiding principles of the European Community, the priority of freedom, security and justice [11], the European Union (EU) has established protection concepts dealing with these threats on different institutional stages. Furthermore, multilateralism, cooperation beyond borders and security, as well as the strengthening of the capacity of neighbouring regions were mentioned for building up better security. By launching many programs and funding special issued projects, the European Union is promoting the contribution of the member states in enhancing the security of the European citizens and improving the resilience of the European society. Terrorism, the proliferation of weapons of mass destruction, regional conflicts, state failure and organized crime, as well as their linkage, were identified as new threats to Europe [12] and led, inter alia to the drafting of the European Security Strategy (ESS). On a very generic level, the ESS, the Common Foreign and Security Policy (CFSP), and the Common Security and Defence Policy (CSDP) serve as underlying policies that encourage security of citizens [13]. Thereby, the ESS constitutes a conceptual framework for the CFSP and the CSDP, by providing essential provisions for analysing and defining the EU's security environment, identifying key security challenges and deriving political implications for the EU [13]. CFSP was established by the Maastricht Treaty in 1993 and provides the foundation for a common defence strategy. The objectives of the CFSP are set out in Article 24 of the Treaty on the EU and are to be attained through specific legal instruments, such as joint actions and common policies adopted unanimously by the Council. Encouraged by the Lisbon Treaty, the CFSP is able to determine a long-term focus for EU's external actions. Furthermore, the effectiveness of the Common Foreign and Security Policy will be increased by entrusting the high representatives of Foreign Affairs and Security Policy with the mandate to implement strategies and decisions taken by the European Council and the Council in matters related to the CFSP. The Common Security and Defence Policy (CSDP), previously known as the European Security and Defence Policy (ESDP), includes the gradual framing of a common defence policy which might in time lead to a common defence. It intends to allow the Union to develop its civilian and military capacities for crisis

management and conflict prevention at an international level, thus it will maintain peace and ensure international security in compliance with the Charter of the United Nations. Relying on a joint action of the Council, the Treaty of Lisbon institutionalized the European Defence Agency, which is responsible for (i) improving the defence capacities of the Union particularly in the field of crisis management; (ii) strengthening the Union's industrial and technological armament capacities; (iii) promoting European cooperation in armament matters. As *preventive measures*, the policy papers "European Programme for Critical Infrastructure Protection (EPCIP)" and its national counterpart, the Austrian Programme for Critical Infrastructure Protection (APCIP) are concerned with the protection of critical infrastructures. As stated by [2], EPCIP was drafted to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the EU. Provisions made by EPCIP are considered as an ongoing process, elaborated by regular reviews. Beginning with an emphasis on terrorist attacks, nowadays European Program for Critical Infrastructure Protection (EPCIP) is pursuing an all-hazard approach including several types of threats as cause for a disruption or destruction of CI.

European Critical Infrastructure (ECI) is a commonly used term in the sphere of the European Commission and describes those "assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [14]. There is no unitary definition which infrastructures have to be considered as CI at the international, the European, the national or regional level. Austria does not consider the same branches as CI compared to those classified as CI at the level of the European Union. Heterogeneous designations are depending on the respective vulnerability of an infrastructure to specific threat scenarios in a certain spatial context. From an Austrian perspective Critical Infrastructures (CIs) are defined "assets of strategically important companies and institutions" [15]. As essential characteristics, CI are considered with regard to the impact in case of a failure of the system, the relevance as services of general interest, the redundancy of the system and the market share of the company or the institution. In respect of the heterogeneity of European Critical Infrastructures (ECIs), the European Commission [16] nominated eleven sectors as illustrated in Table 1.

Table 1: Overview on European CI sectors [17].

No.	**CI sectors**		
1.	Energy	2.	Health
3.	Nuclear industry	4.	Financial
5.	ICT	6.	Transport
7.	Water	8.	Chemical industry
9.	Food	10.	Space
11.	Research institutions		

The European Community, the governments of Member States and business representatives will assess the success by (i) conducting inventories on provisions for critical infrastructures in country-specific jurisdictions of Member States according to the priorities determined in EPCIP, (ii) observing collaborations between companies and government in order to share information and reduce the likelihood of incidents which are causing widespread or long-term disruption of CI, (iii) implementing of a common approach to ensure the security of critical infrastructures through cooperation of all public and private actors.

Stipulated by the European Program for Critical Infrastructure of the European Commission, Austria launched a national equivalent called Program for Critical Infrastructure Protection (APCIP) to implement the European approach to protect CIs. APCIP is pursuing to build awareness for current risks at different levels, to ensure the persistence of an attractively business location Austria and to provide equal level playing fields. APCIP is based on the principles of subsidiarity, complementarity, confidentiality, cooperation and proportionality. Within APCIP, the focus lies on reducing vulnerability of Austrian CIs.

The implementation of APCIP in strategically important companies and institutions is shared responsibility of the Federal Chancellery and the Federal Ministry of the Interior. The inter-ministerial task force for the CIP, which was established on the basis of the Council of Ministers Lecture in 2008, was converted into the "Advisory Board APCIP", which involves several ministerial departments to participate at the panel. In particular representatives of the Federal Ministry for Foreign Affairs, the Federal Ministry of Defence and Sport and the Federal Ministry of Transport, Innovation and Technology etc. are part of the working group. Furthermore, cooperation was established with some selected countries, partially bordering on Austria. Joint information workshops with stakeholders from different institutions and countries are held to exchange information and share lessons learned. Another step to strengthen the functional cooperation amongst the government, science and economy, the common information platform Critical Infrastructure Warning Information Network (CIWIN) serves as an interface for public authorities and strategic enterprises.

Considering that major parts of Critical Infrastructures (CIs) are privately owned, CI owners/operators are mainly responsible to implement protection of CIs. In order to ensure protection of CI against several threats, responsibilities in the area of CIP are shared between the state and economy. Due to the fact, that CIP in Austria is drawn on a voluntary agreement based on Public Private Partnership (PPP), authorities of the state are prompted to enter into dialogue with companies and establish close cooperation with CI owners/operators in order to ensure security of supply. Events, whereby the impact exceeds the capabilities of private operators, called for coordination by federal state agencies, e.g. in the case when relief units are deployed to mitigate the damage or impact on the society.

Furthermore, inter-departmental collaborations in the area of CIP exist with the National Crisis and Disaster Protection Management (SKKM), located at the

Federal Ministry of the Interior, security authorities, the Austrian Armed Forces as well as with emergency services and strategic economic partners. As an Austrian peculiarity, the Austrian Armed Forces can be requested for assisting public relief units or the security service of the company. Within the working program of the Federal Government 2013 -2018 quality criteria and training standards for private security services, risk managers and consultants have been defined. In order to encourage preparedness and rapid response in the case of an event, Federal Chancellery and the Federal Ministry of the Interior launched training exercises on the basis of common standards and results arising from training will be evaluated regularly by the Advisory Board APCIP. Based on training experiences, the Advisory Board is enabled to estimate, if and to what extent the performance of strategic institutions can become more resilient by granting a preferred supply with basic essentials, e.g. electrical power or natural gas.

Based on an individual investigation of country specific threats and critical infrastructure, APCIP [1] reflects on measures to implement EPCIP at the national level in Austria. The Action plan proposes the drawing up of a list with strategically important infrastructures in Austria, their prioritization, a definition of proper standards for the protection and security, the implementation of protection measures, the development and the establishment of cooperation regarding the information management as well as the evaluation of implemented measures. Classification criteria for the identification of relevant sectors include (i) number of affected citizens with respect to health and social impacts, (ii) economic impacts, (iii) environmental impacts, (iv) psychological impacts, (v) spatial dimension, (vi) duration of the impact, (vii) lack of substitutes and alternatives and (viii) interdependencies [18].

As illustrated in Table 2, as a part of part of the vulnerability analysis, twelve domains have been designated as CIs within the two main categories – physical and socio-cultural sectors.

Table 2: Overview on sectors determined as Austrian Critical Infrastructures [1].

Categories	**Sectors**
Physical (technical) sectors	Energy
	ICT
	Transport
	Water
	Chemical industry
Socio-cultural (“soft”) sectors	Food
	Public health
	Finance
	Research facilities
	Constitutional facilities
	Maintenance of public welfare and sectors distribution systems
	Emergency services and relief units

In contrast to European Critical Infrastructures (ECI), the list of Austrian Critical Infrastructures (ACI) also comprises constitutional institutions, sustainability of the social system, and maintenance of the distribution system and relief workers too. Furthermore, a different prioritization of branches amongst the spatial dimensions of the state exists (e.g. state-level, level of provinces, districts and municipalities). This approach considers that the different political levels hold various competences and know-how, which are suitable to manage issues more efficiently. Interrelationships between levels and actors with vague divisions of responsibilities present a challenge for analysing roles, actors and their sphere of influence [16]. The Austrian list of CIs covers in total 400 organisation according to OENACE (Austrian classification system of all economic activities according to Nomenclature of Economic Activities), including institutions and companies of public interest. At the moment, close cooperation with more than 80 percent of ACIs have been established. In the frame of APCIP, the Austrian Ministry of the Interior and the Federal Chancellery of Austria developed a self-assessment tool for CI operators/owners to evaluate their risk in operating complex assets. It is based on national and international standards such as ISO 27000 and the Austrian Manual for Information Security and seeks to build awareness in order to stimulate prevention measures, mitigation strategies as well as to utilize proper response mechanism in the case of a disruption or destruction. Evaluating vulnerabilities by itself aims at providing incentives for CI operators/owners to implement protection measures as best as possible. In particular, the evaluation tool renders assistance for the identification of operational IT-risks, advice to set up mitigation measures and to draft reactive measures, e.g. by tailored contingency plans. In the view of competent authorities in Austria, IEMI has been considered as one threat to critical infrastructures amongst others. As reflected by the questions in the self-assessment tool, a serious threat is assumed by attacks, which have not been further specified but may be of criminal or terrorist nature. In particular, the issue addresses whether and to what extent assets or components of them are vulnerable to threats posed by high power electromagnetics. In the case this question will be answered in affirmative, attention is drawn to appropriate redundancies of the service of the assets or their endangered components. Against the background, that the federal law provides the Criminal Code § 278b, applicable to the threat posed by organisation aiming at committing terrorists act [19], the common initiative of the Federal Ministry of the Interior and the Federal Chancellery is more focusing on prevention and mitigation.

4 Discussion and outlook

Experiences in the field of electromagnetic threats showed evidence that IEMI attacks are real and do occur, but due to classification and economic reasons most of the attacks are not documented. Methods for protecting infrastructures against electromagnetic attacks do exist which need a bunch of measures e.g. filtering and shielding. Therefore a strong recommendation for operators of

critical infrastructures is to investigate their vulnerability against these threats and to set countermeasures for protection. No matter if critical infrastructures are threaten by natural induced sources or human induced sources such as terrorism, initiatives aiming at the establishment of a comprehensive protection framework, need to consider the demands of CI operators/owners in order to establish a feasible protection strategy. Austria is pursuing a cooperation-based approach relying on the self-assessment of strategic companies and organisation. A close interlocking of different sub-systems of the state, involving actors at the state level, the economy, research and science, the media etc. becomes evident. This approach considers that the different actors hold various competences and know-how, which are suitable to manage issues more efficiently. As an Austrian peculiarity, its corporative background has proven itself as beneficial to proceed with challenges claiming on the solution on multiple levels. Responsible authorities are aware of the necessity to enter into dialogue with CI operators/owners proactively, because they, because they perceive themselves as service-provider in order to establish protection concepts that meet the requirements of addressees. Jointly, individual protection strategies can be developed tailored to the specifics of the respective CI operator/owner. Especially by introducing the self-assessment approach, where CI operators/owners are enabled to assess their vulnerability to certain threats by its own, capability will be conveyed, which may lead to a high sense of responsibility to implement protection. Pursuing collaboration at eye-level will naturally raise addressees' awareness and thus facilitate the implementation process. The consideration of federalism is vital for understanding the impact of the European Union on the jurisdiction of the Member States. With regard to the HIPOW approach to promote the establishment of a holistic protection framework at European level, such a cooperation/service-based approach seems to be beneficial to strengthen the resilience of the European Community. In the course of HIPOW a handbook will be developed covering recommendations to protect against IEMI and information to build awareness for these growing threat. This handbook will be provided on platforms like CIWIN to ensure the distribution to the critical infrastructure operators.

Acknowledgement

The FP7 Project HIPOW has received funding from the European Commission's Seventh Framework Programme (FP7/2012-2012) under Grant agreement no. 284802.

References

[1] Federal Chancellor of Austria, "MASTERPLAN Österreichisches Programm zum Schutz Kritischer Infrastruktur (Austrian Program for Critical Infrastructure Protection – APCIP)", Vienna, Austria, 2008.

[2] "Commission from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the fight against terrorism. COM(2004) 702 final", European Commission, 2004.
[3] G. Neubauer, F. Teichmann, C. Türk, T. Gruber, K. Lamedschwandner, A. Weinfurter, P. Böhm, S. Cecil und A. Preinerstorfer, "Schutz gegen elektromagnetische Bedrohungen", Truppendienst Bundesheer, Vienna, 2013.
[4] United States Departement of Homeland Security, "The Threat of Radio Frequency Weapons to Critical Infrastructure Facilities", TSWG & DETO Publication, 2005.
[5] International Electrotechnical Commission (IEC), *Electromagnetic Compatibility (EMC) – Part 2-13: Environment – High Power Electromagnetic (HPEM) Environments – Radiated and Conducted,* Geneva, Switzerland, 2005.
[6] E. Savage und W. Radasky, "Overview of the threat of IEMI (intentional electromagnetic interference)", in *IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Pittsburgh, 2012.
[7] D. Mansson, M. Backstrom and R. Thottappillil, "Intentional EMI against critical infrastructures, a discussion on mitigation philosophy", in *Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC)*, Beijing, 2010.
[8] C. Adami, C. Braun, P. Clemens, M. Joester, S. Ruge, M. Surhke, H. Schmidt and H. Taenzer, "HPM detector system with frequency identification", in *International Symposium on Electromagnetic Compatibility (EMC Europe)*, Gothenburg, 2014.
[9] A. Preinerstorfer, C. Adami, M. Joester, T. Pusch, M. Suhrke, R. Bumerl-Lexa, N. Kolosnev und G. Neubauer, "Investigation of the Impact of Various IEMI Sources to Electronic Passport Readers", in *Proceedings of th 9th Future Security Research Conference*, Berlin, 2014.
[10] Project Homepage, "HIPOW (Protection of Critical Infrastructures against High Power Microwave Threats)", 2015. [Online]. Available: www.hipow-project.eu/
[11] European Council, *The Stockholm Programme – An open and secure Europe serving and protecting citizens,* Official Journal C 115 of 4.5.2010, 2012.
[12] J. Solana, "European Security Strategy – A secure Europe in a better world", Brussels, Belgium, 2003.
[13] European Commission, "europa.eu", about CSDP – European Security Strategy. [online]. Available: http://eeas.europa.eu/csdp/about-csdp/european-security-strategy/index_en.htm. [Zugriff am 28 January 2014].
[14] Swedish Civil Contingencies Agencies (MSB), "Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure", 2014.
[15] Pschikal, Alexander (Federal Chancellery of Austria), "Schutz Kritischer Infrastrukturen", in *CSS Tagungsbericht Dritter D-A-CH Workshop*, Magglingen, Switzerland, 2013.

[16] European Commission, *Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism,* COM(2004) 702 final, 2004.
[17] "Commission staff working document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)," European Commission, Brussels, Belgium, 2012.
[18] "Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM(2006)786 final", Commission of the European Communities, Brussels, Belgium, 2006.
[19] Federal Law Gazette, *Formation of Terrorist Organisations,* Vienna, Austria: Article 278b of the Criminal Code, 2010.
[20] J. Dawson, I. Flintoft, P. Kortoci, L. Dawson, A. Marvin, M. Robinson, M. Stojilovic, M. Rubinstein, B. Menssen, H. Garbe, W. Hirschi and L. Rouiller, "A Cost-efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) attack", in *Proc. of the 2014 International Symposium on Electromagnetic Compatibility (EMC Europe 2014)*, Gothenburg, Sweden, 2014.
[21] O. D. Cardona, "The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management", in *Mapping Vulnerability: Disasters, Development and People*, London, UK, Earthscan Publishers, 2004.
[22] M. Wik, W. A. Radasky and R. L. Gardner, "Intentional Electromagnetic Interference (EMI). What is the threat and what can we do about it?", in *EMC 2000 WROCLAW 26–30 June 2000*, Wroclaw, Poland, 2000.
[23] H. Brauch, "Threats, Challenges, Vulnerabilities and Risks in Environmental and Human Security No.1/2005", SOURCE "Studiens of the University: Research, Counsel, Education", Bonn, Germany, 2005.
[24] J. Moteff, "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. CRS Report for Congress", Congressional Research Service – The Library of Congress, 2005.
[25] *Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. COM(2006) 787 final,* Brussels, Belgium: Commission of the European Communities, 2006.
[26] Commission of the European Communities, *Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection,* Brussels, Belgium: COM(2006) 787 final, 2006.