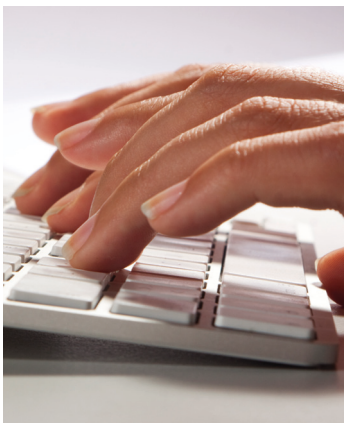
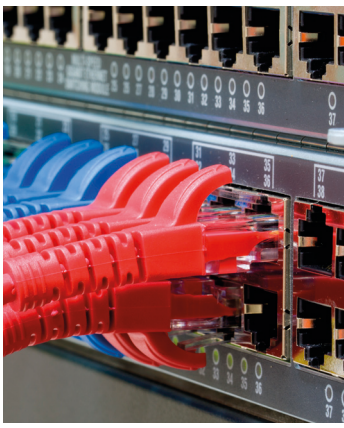
Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace



OSCE Organization for Security and Co-operation in Europe

ISBN 978-92-9235-022-2

Design: HiSolutions AG
Layout: OTHERVIEW, Watrowicz & Watrowicz GbR
Print: Ueberreuter Print GmbH
Image source: fotolia.com / Kanea, B., Wylezich, wellphoto, panomacc

The project received financial support from the United States Delegation to the OSCE.

Action against Terrorism Unit
Transnational Threats Department
OSCE Secretariat
Wallnerstrasse 6
A.1010 Vienna, Austria
Tel: +43 1 514 360, atu@osce.org

Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace

OSCE Organization for Security and Co-operation in Europe

Table of Contents

Foreword

I am pleased to present the Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. This guidebook has been developed by a number of experts from the public and private sector of OSCE participating States as well as the European Union and the North Atlantic Treaty Organization.

The importance of energy security and energy infrastructure security cannot be overstated. It is among the most serious security, economic and environmental challenges of both today, and the future. In recent years, protecting critical energy infrastructure from terrorists has received increasing attention from the international community. Since critical energy infrastructure contains the fuel that keeps the global economy moving and our societies working, our dependency on such infrastructure makes it an ideal target for terrorists. The disruption or destruction of this infrastructure would have a serious impact on the security, safety, economic well-being and health of individuals and the world as a whole.

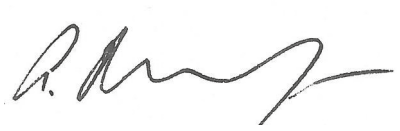
Protecting critical energy infrastructure from terrorist attacks is an issue particularly salient for the Organization for Security and Co-operation in Europe (OSCE), whose 57 participating States, as well as 11 Partners for Co-operation, include some of the largest producers and consumers of energy as well as many strategic transit countries. OSCE participating States adopted in November 2007 a Ministerial Council Decision on Protecting Critical Energy Infrastructure from Terrorist Attack [MC.DEC/6/07], whereby they committed to co-operate and better co-ordinate and to consider all necessary measures at the national level in order to ensure adequate critical energy infrastructure protection from terrorist attacks.

In implementation of Ministerial Decision MC.DEC/6/7 the Action against Terrorism Unit of the OSCE Transnational Threats Department (TNTD/ATU) organized a Public-Private Expert Workshop on Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks, in Vienna on 11-12 February 2010.

The Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) project was initiated by TNTD/ATU in order to promote implementation of this decision through the publication of this Good Practices Guide.

The intent of the publication is to raise awareness of the risk of cyber-related terrorist threat to NNCEI, particularly to industrial control systems and cyber-related infrastructure, among all stakeholders and to promote the implementation of good practices for protecting this infrastructure. This Guide identifies key policy issues and challenges and collects selected good practices as possible solutions. The Guide is to serve as a reference document containing key information for government policy makers, state authorities in charge of critical (energy) infrastructure protection, owners and operators of non-nuclear energy infrastructure, and other stakeholders in OSCE participating States and Partners for Co-operation.

This publication intends to provide a framework that encourages the formulation and implementation of appropriate policies and institutional management of cyber security related to NNCEI, based on a co-operative, integrated (all-hazard) and risk-based approach, and with an emphasis on achieving incident response preparedness, overall infrastructure resilience and energy reliability. Issues include: risk assessment, physical security, cyber security, contingency planning, public-private partnerships, community engagement (including the special contributions of women community members), and international/cross-border co-operation.



Alexey Lyzhenkov

Co-ordinator of Activities to Address
Transnational Threats

Acknowledgements

The Action against Terrorism Unit of the OSCE Transnational Threats Department (TNTD/ATU) and its Head on Anti-terrorism Issues, Thomas Wuchte, would like to express its gratitude for the following OSCE participating States, experts and staff members for their contribution to this Guide:

OSCE participating States contributing to the Guide:

Belarus, Croatia, France, Germany, Hungary, Lithuania, the Netherlands, Romania, Slovakia, Slovenia, Sweden, Switzerland, Tajikistan, Turkey, USA

The European Union and the North Atlantic Treaty Organization for their support

Members of the Stakeholder Consultative Group contributing to the Guide:

Mario d'Agostini, Federal Office for National Economic Supply (FONES); Head of secretariat division Electricity and Drinkable Water; Swiss national representative in Industrial Resources and Communication Services Group [IRCSG, Industry] within Partnership for peace, EAPC (NATO); Chairman of AHWG Energy CIP

Brad Davidson, International Affairs Analyst, Office of Infrastructure Protection, U.S. Department of Homeland Security

Vytautas Butrimas, Chief MoND Adviser for Cyber Security, Ministry of National Defense, Republic of Lithuania

Sharri R. Clark, Foreign Affairs Officer, Bureau of Counterterrorism, U.S. Department of State

William Flynn, Deputy Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security

Petra Hochmannova, Head of CSIRT.SK, DataCentrum - Ministry of Finance of the Slovak Republic

José Antonio Hoyos-Pérez, Policy Officer, Critical Energy Infrastructure Protection, European Commission, Directorate-General for Energy

Daniel Ionita, CERT-RO Romania

Marybeth Kelliher, Foreign Affairs Officer, Bureau of Counterterrorism, U.S. Department of State

Danka Kubikova, Senior State Advisor Ministry of Economy of the Slovak Republic Slovak Republic

Jan Lukacin, ABB, s.r.o. Sales Manager, Slovak Republic

Richard Prosen, Foreign Affairs Officer, Bureau of European Affairs, U.S. Department of State

Paul Reither, OMV AG, Head of Group Security and Resilience

The Project Consultants:

Heiko Borchert, Managing Director, Sandfire AG, Switzerland

Enno Ewers, Managing Consultant System Security, HiSolutions AG, Germany

Carolin Grimm, Consultant Corporate Security Management, HiSolutions AG, Germany

Mathias Köppe, Consultant Corporate Security Management, HiSolutions AG, Germany

Robin Kroha, Director Corporate Security Management, HiSolutions AG, Germany

Alexander Papitsch, Senior Consultant System Security, HiSolutions AG, Germany

Ina Reiffersberger, Consultant Corporate Security Management, HiSolutions AG, Germany

Gordon Schwarzer, Managing Consultant Corporate Security Management, HiSolutions AG, Germany

OSCE staff

Anton Dengg, Adviser on Anti-terrorism Issues, TNTD/ATU, editor of this publication

Selin Freidl, Project Assistant, TNTD/ATU

Mehdi Knani, Assistant Programme Officer, TNTD/ATU

Alexander Malyshau, Senior Information Management Assistant, Co-ordination Cell, TNTD

Nemanja Malisevic, Cyber Security Officer, Co-ordination Cell, TNTD

Reinhard Uhrig, Deputy Head and Programme Co-ordinator, TNTD/ATU

Laszlo Szücs, Programme Officer, TNTD/ATU, editor of this publication

Richard Wheeler, Senior Programme Officer, Energy Security, Office of the Co-ordinator of OSCE Economic and Environmental Activities

The Action against Terrorism Unit of the OSCE Transnational Threats Department (TNTD/ATU) would also like to express its gratitude and appreciation to the Government of the United States of America for its financial contribution to the project.

1.
Executive Summary

OSCE Organization for Security and Co-operation in Europe

1. Executive Summary

National and business infrastructure have always been viewed by adversaries as potential targets. In the ancient world[1], supply lines to cities and countries, and sometimes the stored supplies themselves, were subject to attack or military supply lines were assaulted to weaken an army. In the past, such attacks focused on supplies such as food and water or military targets, but industrialization has created a new target: the energy supply.

In today's highly industrialized world, few things can function without energy. Life as we know it would no longer be possible if there was no energy industry or if a power outage occurred over a long period. Our potential enemies are also aware of this.

For this reason, countries and energy sectors must take responsibility for implementing measures to guarantee that energy, including electricity, is available at all times. The participating States of the Organization for the Security and Co-operation in Europe (OSCE) are no exception. The OSCE is uniquely placed as a pan-European and trans-Atlantic body of highly industrialized and developed participating States with Partners for Co-operation from North Africa to Australia to address energy infrastructure security, particularly threats from terrorist attacks and those emanating from cyberspace.

This guide describes the significance of non-nuclear critical energy infrastructure (NNCEI) for countries and energy consumers and identifies threats to that infrastructure, focusing on cyber-related terrorist attacks. It is not intended to be a comprehensive threat analysis or to explain all protection measures in detail. Nor does it discuss whether and to what extent a particular country or operator of non-nuclear critical energy infrastructure is actually vulnerable to these threats, as this can only be determined on an individual basis. Rather, the guide will highlight methodological issues that need to be taken into account for the protection of non-nuclear critical energy infrastructure and offer suggestions for good practices to mitigate potential vulnerabilities.

Although the aim of the good practices presented here is to assist countries with identifying and countering threats to cyber-related terrorist attacks, these measures may be adapted, extended and/or applied to other threats and other sectors. This possibility is taken into account throughout the guide.

A detailed discussion of these threats and recommendations for greater preparation and resilience follows. Based on our findings, recommended good practices for all countries and companies operating non-nuclear critical energy infrastructure include:

1. Raising awareness of the significance of non-nuclear critical energy infrastructure and the extent to which it is threatened by cyber-related terrorist attacks, as well as other types of potential threats;

2. Promoting national and international co-operation between public agencies and owners and operators of non-nuclear critical energy infrastructure to face the threat of cyber attacks;

3. Facilitating information exchange between public agencies and the operators of non-nuclear critical energy infrastructure regarding ways of dealing with the threat of cyber attacks; and

4. Using existing national and international forums and, if appropriate, creating standardized national and international forums and frameworks for addressing cyber-related terrorist attacks on non-nuclear critical energy infrastructure to consider co-ordinated measures, such as raising awareness, outreach and partnering with industry, and where appropriate, implementing adequate regulations.

The OSCE has a special role in this, as it can act as an intermediary between international organizations such as the European Union (EU) and North Atlantic Treaty Organization (NATO), participating States, and the owners and operators of non-nuclear critical energy infrastructure.

1 Michael J. Assante: „Infrastructure Protection in the Ancient World: What the Romans can tell us about their Aqueducts – What we may apply to our modern infrastructures", Proceedings of the 42nd Hawaii International Conference on System Sciences (2009), p. 4

2. Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure

OSCE Organization for Security and Co-operation in Europe

2. Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure

Just as there are differing definitions of terrorism, there are a number of definitions for "cyberterrorism". The real challenge for countries and companies is to identify the threats and recognize the attackers, as victims typically focus on the impact. With this in mind, it is not really surprising that attempts at defining the term have focused on the impact. Below are two definitions of cyberterrorism as examples:

"Cyberterrorism is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[2]

"Cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)."[3]

These definitions describe attacks on cyber infrastructure and attacks using cyber tools, although the term "cyberterrorism" has been used more broadly than the subject considered here. In the following sections, we define cyberterrorism as cyber-related terrorism and more specifically, for our purposes, as terrorist attacks on cyber infrastructure particularly on control systems for non-nuclear critical energy infrastructure. Ultimately, the focus is on the global and national significance of non-nuclear critical energy infrastructure, and general and specific cyber threats to it, including from terrorist attacks.

2.1 Critical Infrastructure

Infrastructure is vital to highly developed and productive modern societies, and the development of infrastructure is a key measure of economic competitiveness. Ensuring the competitiveness of countries in a globalized world is essential for wealth and progress, and critical infrastructure must be protected to maintain competitiveness.

Protecting critical infrastructure is a core task for national and corporate security and should always have a central place in a nation's security policy as the failure to protect it could have serious effects. "Critical infrastructure are organizations and facilities of great significance to the national community. Their breakdown or malfunction would cause long-term supply bottlenecks, serious disruption to public safety or other dramatic consequences."[4]

The EU defines critical infrastructure as "an asset, system or part thereof located in Member States which is 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."[5]

The United States (U.S.) Department of Homeland Security defines critical infrastructure as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction."[6]

2 Mehmet Nesip Ogun: Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research (2012), p. 209

3 Gabriel Weimann: Cyberterrorism: The Sum of All Fears?: Studies in Conflict & Terrorism, p. 130

4 Nationale Strategie zum Schutz Kritischer Infrastrukturen, p. 4, German Federal Ministry of the Interior, URL: http://www.bmi.bund.de/cae/servlet/content-blob/544770/publicationFile/27031/kritis.pdf (11/13/2012, author's translation)

5 Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (2008/114/EC)

6 National Infrastructure Protection Plan (NIPP), p. 109: U.S. Department of Homeland Security, URL: https://www.dhs.gov/national-infrastructure-protection-plan (11/13/2012)

All of the definitions are very similar at their core – they all refer to significant effects on public safety/security, economic prosperity, and societal well-being. Some important additional aspects of critical infrastructure are cross-sector dependencies and far-reaching effects. An outage in one critical infrastructure sector can impact other sectors. This is especially true for the energy sector because all other sectors need energy to operate. In addition, an incident in one geographical area can have regional or even international impacts. For example, the 2003 power outage in New York affected over 55 million people in the United States and Canada with consequences for other sectors including transportation and public health leading to several fatalities. Since all sectors require power to operate, a power outage will almost inevitably have consequences for other sectors. For example, gas stations are usually not equipped with substantial emergency supplies. A power outage could therefore lead to shortages or even a shutdown at a gas station. Moreover gas stations may not be able to provide fuel (sector: energy) for vehicles (sector: traffic and transportation) and emergency generators that are necessary to run other critical infrastructure. Without back-up, permanent, and/or alternative supplies, hospitals (sector: healthcare), banks (finance and insurance), and public institutions (sector: government and administration) may not be able to maintain their operations.

Cascade Effect

The term is used as a metaphor for processes that lead step-by-step from one stage to the next, like a waterfall [Italian: cascata].

The following sectors and industries are widely considered to be critical infrastructure:[7]

Sectors	Industries
Energy	• Electricity • Natural gas • Oil
Information and Communication Technology (ICT)	• Telecommunications (including satellites) • Broadcasting systems • Software, hardware and networks (including the Internet)
Traffic and transportation	• Shipping • Aviation • Rail transport • Road traffic • Logistics
Healthcare	• Healthcare • Medicines and vaccines • Laboratories
Water supply	• Dams • Storage • Treatment and distribution networks
Finance and insurance	• Banks • Stock exchanges • Insurance companies • Financial services
Government and administration	• Government • Parliament • Legal institutions • Emergency services
Nutrition and agriculture	• Food trade • Agriculture
Media and cultural assets	• Radio • Press • Symbolic buildings

Table 1: Critical Infrastructure Sectors[7]

7 National Infrastructure Protection Plan (NIPP), p. 109: U.S. Department of Homeland Security, URL: https://www.dhs.gov/national-infrastructure-protection-plan (11/13/2012)

It is essential to maintain equilibrium in critical infrastructure such as energy, which supports and sustains other critical infrastructure (e.g., equilibrium in the electricity grid is necessary at all times because disruptions can spread within seconds). A power outage often has serious consequences due to the cascade effect, inevitably affecting other sectors and their infrastructure. Transformer stations and high voltage power lines are often more critical than generating plants in this respect, since it is usually possible to compensate for the loss of a power station[8], whereas a grid outage or an outage in critical sections of the grid cannot be compensated for.

Within the EU, for example, oil infrastructure are considered less critical than electricity and gas infrastructure. Oil is critical for transportation, but the market is globalized and oil is relatively flexibly distributed within the EU. EU member states also have significant reserves of oil. Each member state is required by law to hold oil reserves sufficient to satisfy domestic demand for at least 90 days.[9] The U.S. Strategic Petroleum Reserve currently comprises 694.9[10] million barrels of oil, enough for 36 days.[11]

2.2 Non-Nuclear Critical Energy Infrastructure

According to the International Energy Agency (IEA) the following energy resources contributed to the global production of energy in 2010:[12]

Fuel[13]	Absolute in Mtoe[14]	Share in %
Coal	3,475.77	27.3
Crude oil	4,159.37	32.7
Oil products	-51.93	-0.4
Natural gas	2,727.61	21.4
Nuclear	718.96	5.7
Hydro	295.62	2.3
Biofuels and waste	1,278.03	10.0
Others	113.71	0.9
Total	12,717.16	100

Table 2: Global Energy Production in 2010[15]

Non-nuclear energy resources account for 94.3 percent of global production. This makes such infrastructure an appealing, although not uniformly vulnerable, target for all sorts of deliberate disruptions and attacks.

Non-Nuclear Critical Energy Infrastructure (NNCEI) includes the exploration, production, storage, refining, processing and distribution of fossil fuels and supporting infrastructure systems such as electricity, as well as the extraction and processing of new energy sources.

8 For example, this can be done at the national level by importing electricity.

9 IEA, URL: http://www.iea.org/publications/feeepublications/publication/EPPD_Bochure_English_2012_02.pdf (Status: 03/20/2013)

10 Cf. Strategic Petroleum Reserve Inventory, URL: http://www.spr.doe.gov/dir/dir.html (12/07/2012)

11 Assuming an average daily use of 19.15 million barrels; see URL: https://www.cia.gov/library/publications/the-world-factbook/fields/2174.html (13/02/2013)

12 International Energy Agency, Key World Energy Statistics 2012; there are no newer comparable figures on international level available

13 For further explanations see: International Energy Agency, Key World Energy Statistics 2012, p. 17

14 1 million tons of oil equivalent (Mtoe) = 11.630 gigawatt hours (GWh).

15 International Energy Agency, Key World Energy Statistics 2012.

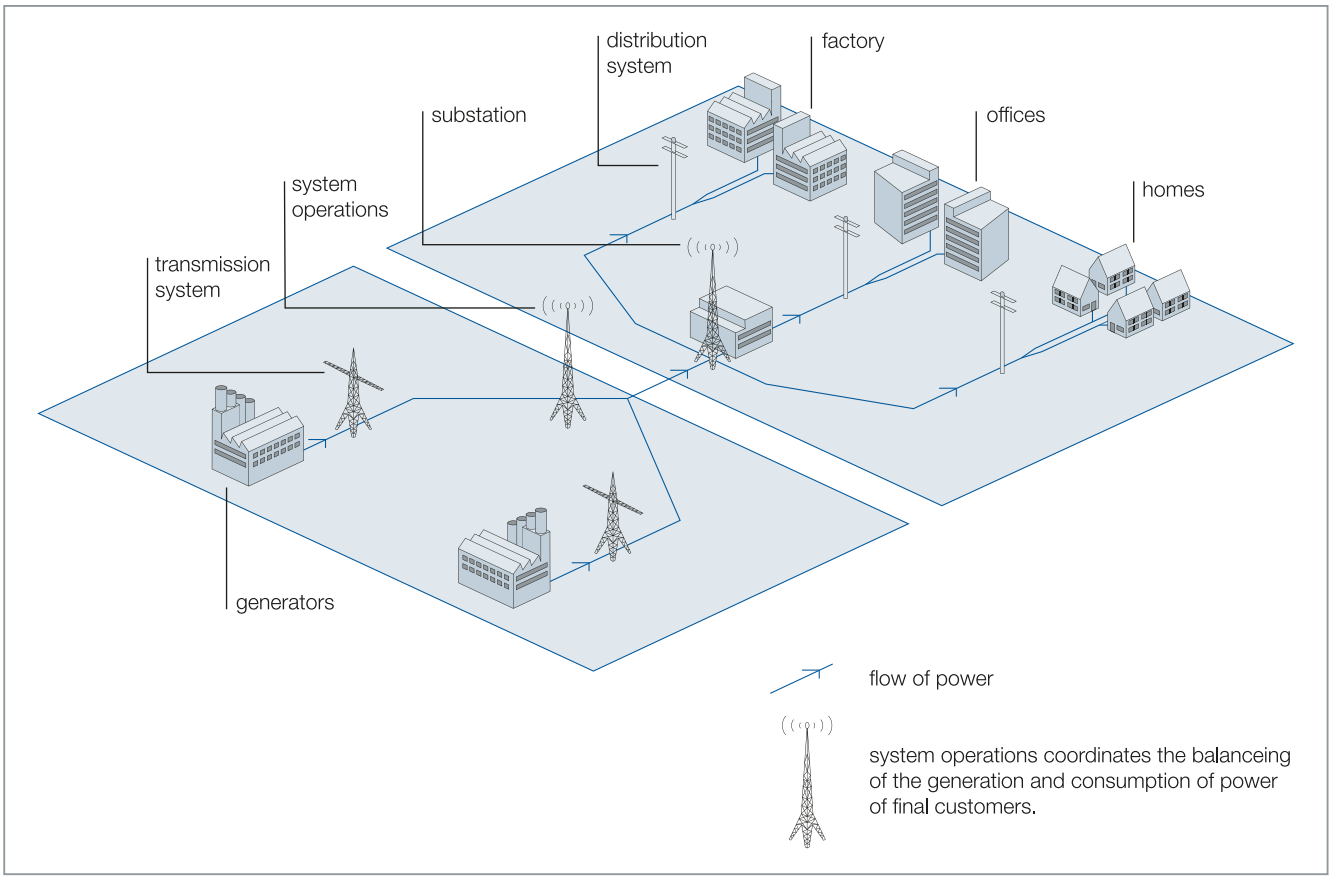


Figure 1: Functions of the Electricity Industry

The complete non-nuclear critical energy infrastructure supply chain includes the exploration of energy-bearing raw materials, energy production, transmission and distribution, storage and final energy consumption[16].[17] In addition, the supply chain also includes the trade of various energy sources and energy itself, as as well as the personnel and organizations who manage supply chain and business activities.

➥ Figure 1: Functions of the Electricity Industry[18]

- Energy is produced by transforming an energy source into electrical power. Energy sources include products containing carbon[19] and solar, wind and hydroelectric energy.
- Transmission and distribution can be divided into two phases. In phase one, the energy source is transported (e.g., by pipelines, ships and trucks); in the second, the electrical power itself is transported.
- Energy storage, like transmission and distribution, can also be divided into two phases. The first phase comprises storing the energy source;[20] the second is the storage of electrical power.
- Part of the energy generated is utilized in the non-nuclear critical energy infrastructure supply chain (e.g., for power generation). A much greater part, however, is used by the final consumer (companies, private households, etc.).
- Energy sources and power are usually traded on trading platforms, which are necessary for international energy trade. All of these trading platforms depend on information technology. Trading platforms play an important role to set energy prices by matching demand and supply. This means that prices fluctuate.

16 Final energy consumption does not include the energy required for energy production, transmission and distribution. International Energy Agency, Energy Statistics Manual 2012, p. 27

17 Examples of legal definitions of these parts of the supply chain: Directive 2009/72/EC (7/13/2009) and directive 2009/73/EC (7/13/2009), Article 2 in both cases.

18 Examples of legal definitions of these parts of the supply chain: Directive 2009/72/EC (7/13/2009) and directive 2009/73/EC (7/13/2009), Article 2 in both cases.

19 Fossil fuels and others such as agricultural, industrial and household waste

20 Fossil fuels and others such as agricultural, industrial and household waste

- Administration is required to ensure that the whole supply chain functions. It includes management boards, HR departments, and service and maintenance.

Final energy consumers are the consumers of the energy generated, excluding those consumers who utilize energy in order to generate energy.[21] For example, today's final energy consumers can also generate and store energy through photovoltaic installations and accumulators. New forms of decentralized energy storage capacity include innovations like the batteries of electric cars. This blending of the roles of final energy consumer and producer poses a new challenge for energy companies when it comes to guaranteeing the security and reliability of the relevant infrastructure elements. The global figure for the final consumption of primary energy[22] in 2010 was 8,676.63 Mtoe,[23] equivalent to approximately 2/3 of energy generated.

Two factors are of significance to final energy consumers:

- 1. Energy costs
- 2. Energy availability[24]

Energy costs vary from one final consumer to another. The significance of this lies in the proportion of energy costs in the costs of production of goods or services, as well as in relation to the population's living standards. The proportion in energy-intensive industry is higher than in the service sector. In Germany, for example, the proportion ranges from 0.2 percent in the service segments of manufacturing industries to almost 10 percent in the chemical industry and metal production and processing.[25] If primary energy consumption is applied to the population of a country, consumption per capita ranges from 142 kg ROE in Eritrea to 16,844.1 kg ROE in Iceland.[26]

As noted earlier, a nation's economic performance depends on the availability of energy.[27] This is related on one hand to the fact that energy contributes directly to economic development and national employment. On the other hand, reliable supplies and competitive energy prices are advantageous for a country's economy and viability as an industrial location, particularly for energy-intensive industries. As a consequence, security of supply[28] is increasingly becoming a criterion when companies select locations for investment – and being an attractive industrial location can promote a country's growth and wealth.

Government and industry stakeholders focus on energy's economic contribution to a country's wealth and growth and security of supply as well.

Energy's economic[29] contribution varies from country to country. The energy industry in Austria, for example, employed 28,300 staff in approximately 1,570 companies and generated €5.3 billion[30].[31] In Germany, on the other hand, the energy supply sector generated €408.5 billion[32] in 2010 with 221,264 employees in 1,722 companies.[33]

Although a country's energy consumption and its economic performance are often shown as related, this is an outdated view because developments in energy efficiency mean that national energy consumption no longer increases in line with economic performance[34].[35] Other factors that contribute to this effect include structural change (towards less energy-intensive production or a larger service sector), relocating energy production components abroad,[36]and changes in population growth. In extreme cases, economic performance can increase while energy consumption declines.

Non-nuclear critical energy infrastructure is particularly important for a country's supply security, because it is in the energy sector, along with the telecommunications sector, in which an outage can lead to cascade and/or

21 For example, coal-fired power stations require a great deal of energy to generate electricity. This kind of energy use is not considered final energy consumption.

22 Total Primary Energy Supply (TPES), International Energy Agency, Key World Energy Statistics 2012, p. 63

23 International Energy Agency, Key World Energy Statistics 2012

24 ifo Schnelldienst 07/2011, p. 10ff

25 German Federal Statistical Office, Energieverbrauch des Verarbeitenden Gewerbes nach ausgewählten Wirtschaftszweigen 2010.

26 German Federal Statistical Office, Basisdaten Primärenergieverbrauch 2009/2010.

27 For example, ifo Schnelldienst 07/2011, p. 10ff

28 Security of supply is an important concept. From a national and from a corporate perspective, the concept describes the need to guarantee the uninterrupted flow of resources to manufacture whatever products are necessary. Energy costs also play a very important role, as can be seen in current European debates about subsidies for renewables and the oil and shale gas bonanza in the United States. This important topic is not covered extensively but is mentioned in this guide.

29 Including nuclear. There are no figures without nuclear available.

30 Gross value of output

31 Kuratorium Sicheres Österreich (KSÖ), Cybersicherheit in Österreich, p. 29, URL: http://www.kuratorium-sicheres-oesterreich.at/uploads/tx_ksothema/Cyberrisikoanalyse.pdf (04/12/2013)

32 Gross value of output

33 German Federal Statistical Office, Fachserie 4, Reihe 6.1 Produzierendes Gewerbe, p. 16ff

34 The gross value of output is often taken as a parameter.

35 ifo Schnelldienst 07/2011, p. 12

36 Dependencies between countries also create import risk.

domino effects. Cascade effects occur when two sectors are dependent on each other to the extent that an outage in one sector creates effects in the other. This interdependency can also lead to domino effects, whereby an outage in one sector leads immediately or after a short delay to an outage in a sector dependent on it. Short delay times should be used to execute security measures (e.g., to activate business continuity or crisis management teams, to execute their plans, or to start an emergency power supply to protect their supply chain).[37]

Countries that are aware of these effects will, in the event of an outage in one critical infrastructure sector, always strive to extend crisis and disaster management to other (unaffected) sectors and to include them in their planning. When preparing for a possible crisis, efforts will be made to strengthen the resilience[38] of individual sectors to enable them to maintain their activities as long as possible even if outages occur in other sectors. Cross-sector measures in prevention and crisis management are therefore essential in order to compensate for the different levels of security precautions in individual critical infrastructure sectors.

Protecting non-nuclear critical energy infrastructure is not only a national concern; it is a global concern. Non-nuclear critical energy infrastructure outages impair the availability and security of the energy supply, may threaten the stability of regions and governments, and affect prices on international energy markets. Terrorist attacks, natural disasters and technical or organizational threats can result in expensive damage to equipment and economic effects, as well as harm to the population. Depending on the scale of the disruptions, a society's confidence in the energy supplier and in the public sector's capability to handle crises may be severely shaken.[39]

As noted earlier, an outage in the energy infrastructure in one country or region can also cause a cascade effect resulting in outages in other countries' infrastructure or even global malfunctions. Because of these cascade effects, non-nuclear critical energy infrastructure protection requires internationally co-ordinated prevention and crisis management measures. In some countries, national governments write dedicated sector-specific plans. For example, the United States has sector-specific plans for each sector, including the energy and communications sectors.[40]

2.3 Cyber-related Terrorist Threats to Non-Nuclear Critical Energy Infrastructure

Energy networks can be vulnerable to deliberate physical assault, as shown by numerous attacks by militant groups on above-ground oil and gas pipelines in places like Colombia, Iraq and Nigeria. Pipeline networks are often thousands of kilometers long, making them difficult to monitor. Thus, providing comprehensive physical protection for them is extremely challenging and costly.[41]

In recent years, the energy supply chain has been more automated and thus has become increasingly reliant on computerized control systems, enabling modern power infrastructure to function more smoothly and efficiently. However, this also increases grid vulnerability, as modern networks are increasingly interoperable and remote-controlled. Although the use of open software standards is a cost-efficient way of operating the networks, it makes the entire power grid much more vulnerable to cyber attacks because of the known or open source code that can be manipulated.[42]

Threats to non-nuclear critical energy infrastructure can be categorized in many ways, based on intent, human involvement, and other criteria.[43]

Open Software Standards

Open software standards are easily accessible and easy to use for all market participants and have the advantage that they can be developed independently. There is often a regulatory interest in defining particular openness requirements for new software development. Internet standards usually satisfy all openness requirements, as with SSL (a protocol for encrypting information over the

37 More on this in chapter 4.

38 Resilience is the term used to describe the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions (cf. U.S. Department of Homeland Security 2009, National Infrastructure Protection Plan, p. 111).

39 Why Is Critical Infrastructure Protection Important? U.S. Department of Homeland Security, URL: http://www.dhs.gov/critical-infrastructure-sectors (16/11/2012)

40 Energy Sector-Specific Plan, U.S. Department of Homeland Security, URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf (2010); and Communications Sector-Specific Plan, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf (2010)

41 Chapter 7 contains further documents that explain how other critical infrastructure sectors like traffic and transport, water supply and ICT manage this issue, since they face the same challenges.

42 Critical Energy Infrastructure Protection: The Case of the Trans-ASEAN Energy Network, URL: http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructure-protection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349 (11/20/2012)

43 In addition to this division, other possibilities exist, such as the BSI's division into natural and anthropogenic threats. Cf. URL: http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/threats/threats_node.html (02/13/2013)

Internet) or TCP/IP (network protocols). Open standards are cheaper to use, since there are no licensing fees. Programs can be enhanced and programming faults can be repaired independently of the manufacturer.

The cyber-related terrorist attacks on which this guide focuses are intentional, person-related threats. There are many other threats, hazards and challenges that could be leveraged by terrorists opportunistically taking advantage of the crises and chaos they create, which are not the focus of this guide. Some of these non-nuclear critical energy infrastructure-relevant threats and challenges are: threats arising from geological conditions or the environment (e.g., extreme weather conditions or natural disasters); threats related to health (e.g., pandemics); geostrategic threats (e.g., political instability or piracy); regulatory challenges (e.g., regulations and price-setting platforms); and organizational challenges (e.g., subcontracting/dependencies on other organizations and "concealed dependencies"[44] in supply chains).

Technical failure, whether unintentional – possibly caused by human error[45] – or intentional, is another threat that can have consequences of considerable proportions. The inherent vulnerabilities and increasing complexities of technical components and systems continually create new risks. Examples of this include the crash of the entire European Commission's bank card system in Switzerland in 2000 due to a fault in the data center, and the 2003 power outage in the United States and Canada.

Technical malfunctions can have many causes. Yet in many cases, finding the cause is not cost-effective, cannot be performed within a reasonable period of time, or is not possible due to legal barriers. As a result, many measures concentrate on preventing or minimizing these threats rather than on the immediate impact and consequences of the threat. Technical threats can be complicated by organizational effects or the complexity of business processes, which can prevent or impede the discovery of human error/action or technical failure.

Even if technical failure is unintentional or accidental, terrorist attacks can exploit technical vulnerabilities with physical or cyber attacks. However, these types of attacks are considerably different in terms of planning and organizational complexity compared with other possible attack scenarios.

Ways of limiting these threats may include:[46]

a. Deploying different systems and separating the systems to prevent an outage in one system from damaging the whole system; avoiding single source dependencies

b. Including liability clauses for damage resulting from technical malfunctions in contracts to be able to claim compensation from the supplier if an outage does occur[47]

c. Continuously exchanging information with suppliers and others[48] about errors and vulnerabilities discovered, in order to remove or repair these problems as soon as possible.

Terrorism and other person-related threats can cause considerable financial, material and human losses. These threats can emanate from internal or external perpetrators. Internal perpetrators usually have more information than external perpetrators and statistically constitute the more serious threat; internal perpetrators are either accomplices or the main conspirators in the majority and most severe cases of loss.[49] This fact is of particular significance because companies have the best and simplest opportunities of reducing the threat by addressing such threats early. Examples of person-related threats include manipulation of products and theft of data with a range of motivations from sabotage to terrorism. Identifying internal perpetrators' motives can suggest ways of limiting damage. The following diagram shows the top 12 motives.

44 Concealed dependencies may occur if several suppliers are supplied from only one source. In this case, the company in fact has only one supplier, the original source, and if that fails, they are dependent on their suppliers' storage capacity.

45 Although the term "error" implies non-intentional activity, it is included here under intentional threats because in many countries negligence is a crime.

46 Individual measures are presented in more detail in chapters 4 and 5.

47 In this context it is important when selecting suppliers to ensure that the supplier is able to pay compensation. In other words, many small, financially insignificant companies should not even be considered as potential suppliers.

48 For example, associations, specialist media or national institutions such as CERTs

49 SiFo-Studie 2009/2010, p. 64ff

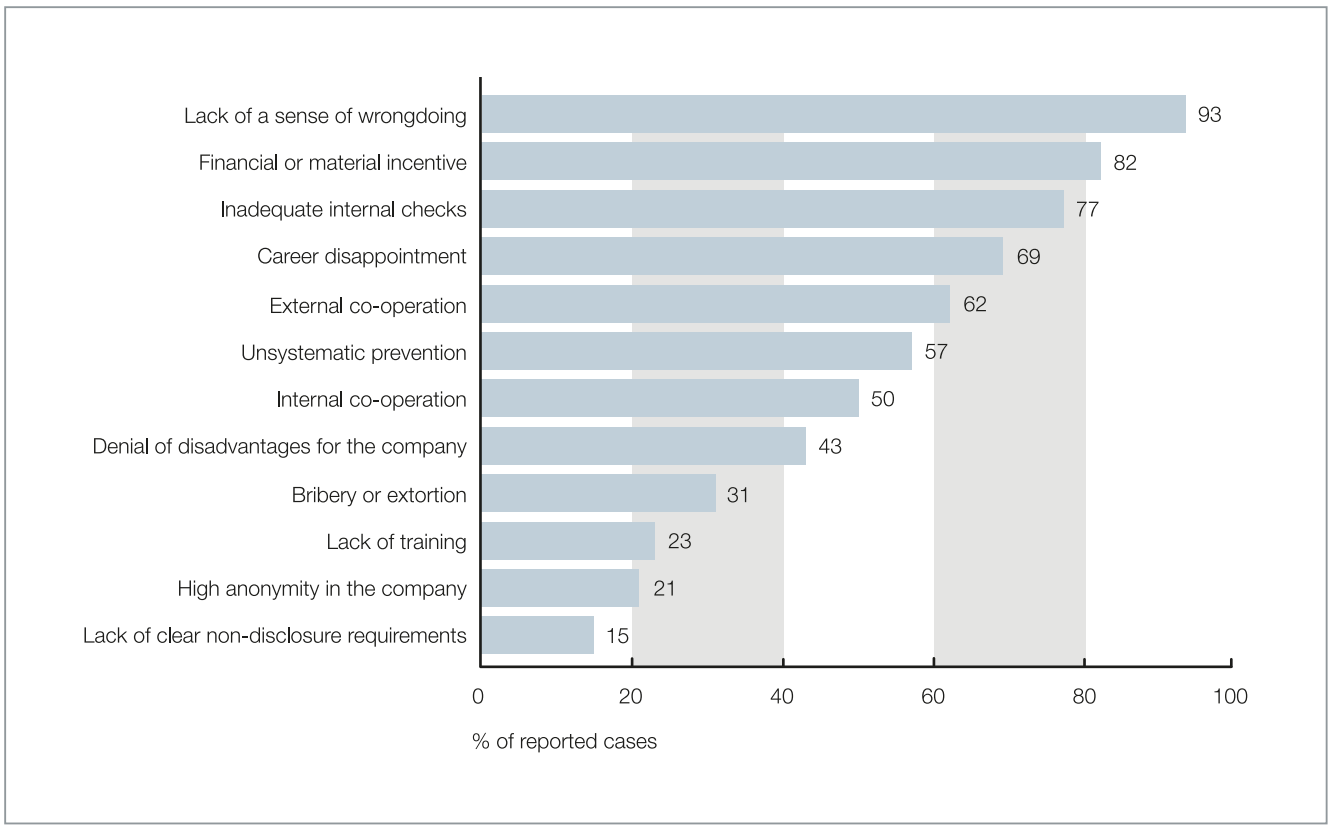


Figure 2: Internal Perpetrators' Motives[50]

The following measures could be taken to reduce these factors, such as "inadequate internal checks," "unsystematic prevention," "lack of training," and "lack of clear non-disclosure requirements":[51]

a. Training, education, and awareness measures for staff and selected contract partners;

b. Holistic protection concepts (using encryption technology, classifying know-how, access controls, monitoring sensitive areas, etc.);

c. Issuing ethical guidelines and codes of conduct;

d. Applying the need-to-know principle[52]; and

e. Implementing a system for anonymous tip-offs to identify internal perpetrators.

Both internal and external perpetrators may be motivated to commit acts of terrorism. Background checks and strong operational procedures are essential to identifying and mitigating potential problems.

Although there has been some debate over how to delineate and define the various types of cybercrime and cyber-related terrorism, there is no disagreement that these threats are in the intentional category, since they involve various vulnerabilities being deliberately exploited by an individual or a group in order to cause damage. As technology continues to develop, the potential spectrum of possible vectors for criminal and terrorist cyber attacks is becoming wider.

On the basis of Article 2 through 9 of the 2001 Council of Europe Cybercrime Convention[53] (also known as the Budapest Convention), a very accessible typology covering various aspects of ICT systems security has been developed. The classification is very simple: it distinguishes between forms of technological abuse and crimes in relation to this technology. The UK Association of Chief Police Officers Good Practice Guide for Computer Based Evidence (2009) adopts a similar approach: "computers can be used in the commission of a crime [Type II]; they

50 SiFo-Studie 2009/2010, p. 71

51 Individual measures are presented in more detail in chapters 4 and 5. The extracts presented here are all taken from the SiFo-Studie 2009/2010, p. 76ff and Best Practice, T-System's client magazine, issue 04/2011.

52 Sensitive knowledge is only available to staff who require it for their work.

53 Council of Europe: Convention on Cybercrime (2001), URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (10/15/2012)

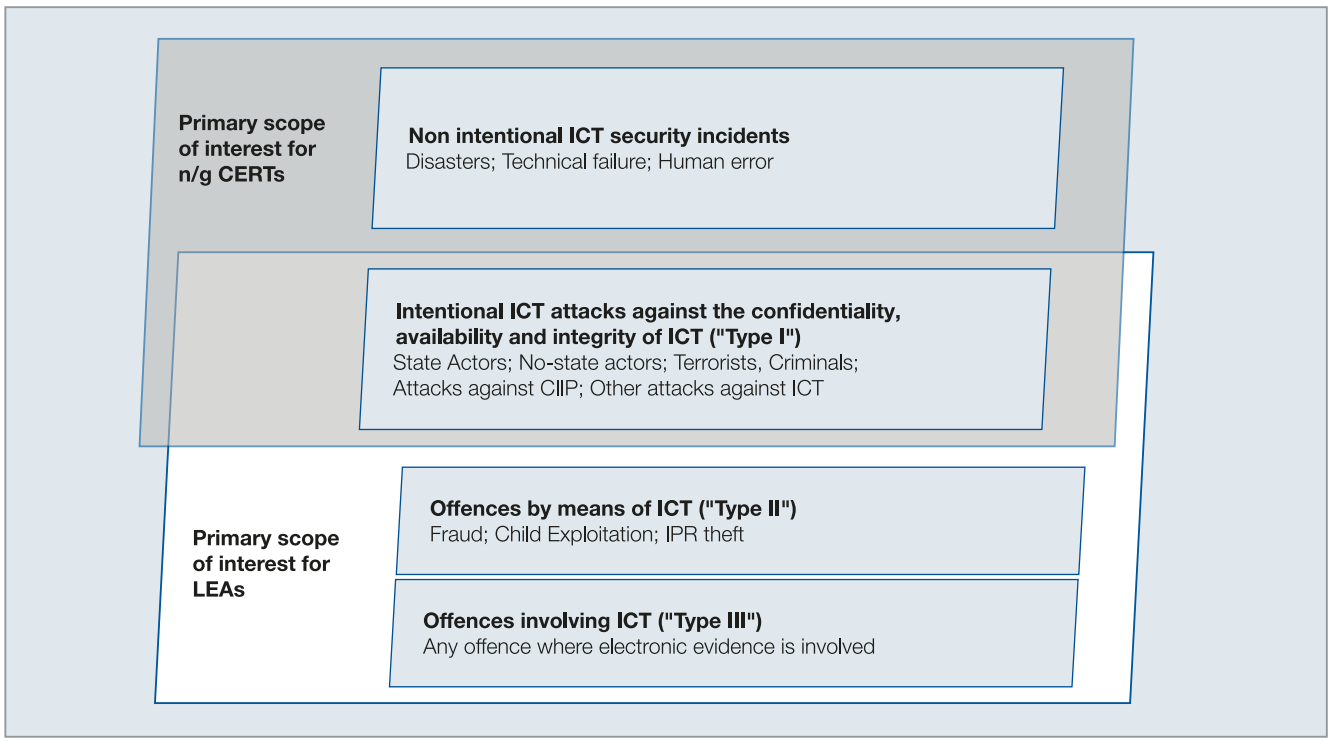


Figure 3: Characterization of Cybercrime and Cyber Security Incidents

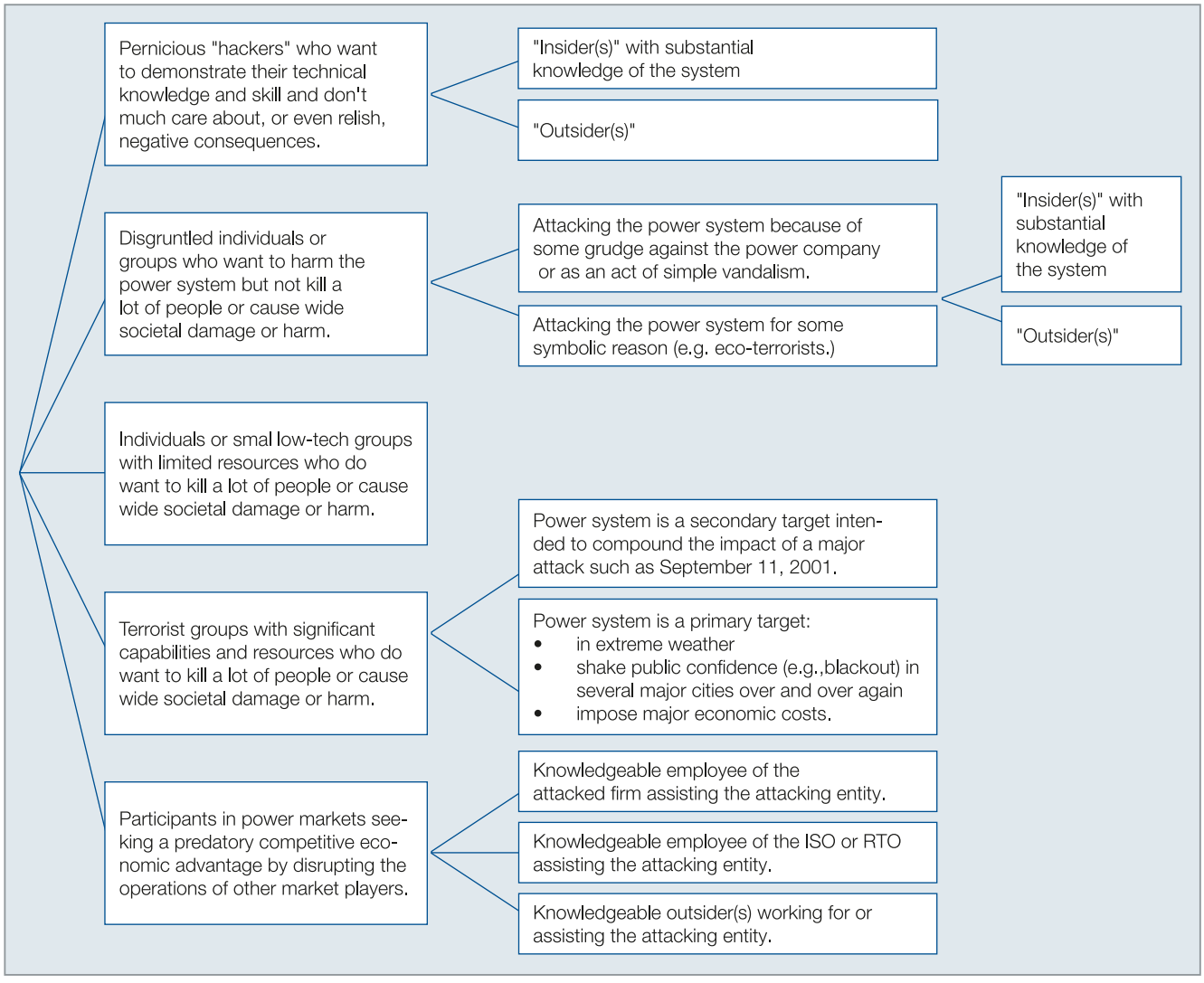


Figure 4: Simple Classification of Potential Power System Attackers

can contain evidence of crime [Type III] and can even be targets of crime [Type I]."[54] Figure 3 below shows the demarcations and overlaps between the mandates of the Computer Emergency Response Team (CERT) and the Law Enforcement Authorities (LEA) in the context of this classification and possible incidents.

➥ Figure 3: Characterization of Cybercrime and Cyber Security Incidents[55]

Since it is difficult for a non-nuclear critical energy infrastructure operator to determine an attacker's intent, when viewing a cybercrime attack or a cyber-related terrorist attack, the important point is the intended impact on the target. For the target itself, this point is not important during the first phase of coping with the attack, when the primary focus is on restoring systems as quickly as possible. Only when analyzing the attack later is it feasible to focus on making this determination.[56]

➥ Figure 4: Simple Classification of Potential Power-System Attackers[57]

Any cybercrime approach can be used by terrorists, so it is essential that non-nuclear critical energy infrastructure operators are aware of the attack vectors and possibilities for cybercrime.

2.4 Potential IT-based Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure

The diagram below illustrates attacks on non-nuclear critical energy infrastructure that cannot be classified as terrorism; however, terrorist groups could adapt them and use them for their purposes. Relevant protective measures to avoid or reduce damage will be presented later in this handbook.

The diagram shows an example of how a cyber attack on the power grid might occur and the possible consequences of such an attack.

➥ Figure 5: How a Cyber Attack Could Affect the Grid[58]

In 2007, scientists at the Idaho National Laboratory gave a clear demonstration of what an attack on a power supplier could mean. The U.S. Department of Homeland Security commissioned them to demonstrate how they could gain access to the control system of an electricity generator and manipulate it to malfunction physically from outside by feeding it false data. This demonstration, known as the Aurora Generator Test, had the following results: first the generator stuttered, then white steam poured out, and finally it ceased to function. It revealed that hackers were not only able to take over the protection and control system of a generator, but also that the generator could be physically destroyed. The loss of a generator or turbine in particular may lead to long replacement periods as parts have to be newly manufactured and installed. A report on the experiment aired on CNN.[59]

Another experiment simulating a cyber attack on the U.S. power grid was carried out in 2010. These hackers accessed the electronics of several transmission stations, targeting special systems that keep the voltage steady in power lines. These systems turned out to be weak points. If the attack had really taken place, half a dozen of these devices would have been destroyed and an entire state would have been without power for several weeks.[60]

In another incident from February 2011, it was discovered that hackers in China had attacked western oil and gas companies and stolen confidential data.[61] The attacks had targeted computers in oil and gas companies in the United States, Taiwan, Greece, and Kazakhstan. The attackers exploited known weak points in the operating systems. These incidents were not terrorist attacks, but terrorists could easily adapt the methods and use them for their own purposes.

Experts identified further attacks on central data processing centers of oil and gas company installations in the Middle East in October 2012. Over 30,000 computers belonging to Saudi oil company Saudi Aramco had already been paralyzed and disabled by malware (known

54 ENISA: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime(2012), p. 12

55 ENISA: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012), p. 13

56 A written claim of responsibility, if there is one, may make identification easier. However these claims cannot always be trusted, as cyber criminals can abuse them too.

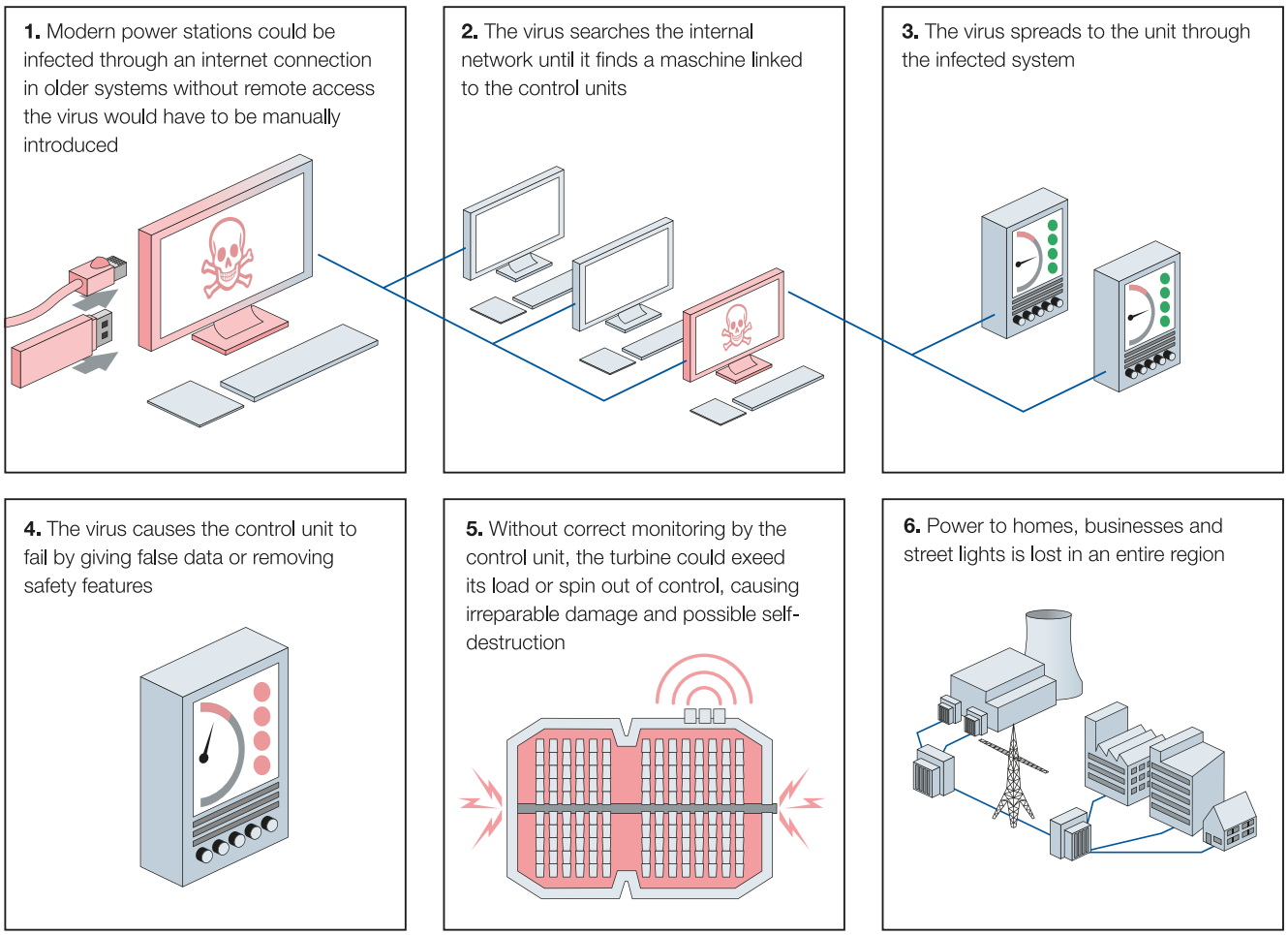
57 NAP: Terrorism and the Electric Power Delivery System (2009), p. 15.

58 Financial Times, URL: http://www.ft.com/cms/s/0/00148d60-c795-11e0-a03f-00144feabdc0.html#axzz2EBla2YKG (12/05/2012)

59 Staged cyber attack reveals vulnerability in power grid: CNN U.S., URL: http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (11/21/2012)

60 Attack on the power grid in Spectrum der Wissenschaft, URL: http://www.spektrum.de/alias/energieversorgung/angriff-auf-das-stromnetz/1123846 (11/21/2012)

61 Cf. McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), URL: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf (12/02/2013)



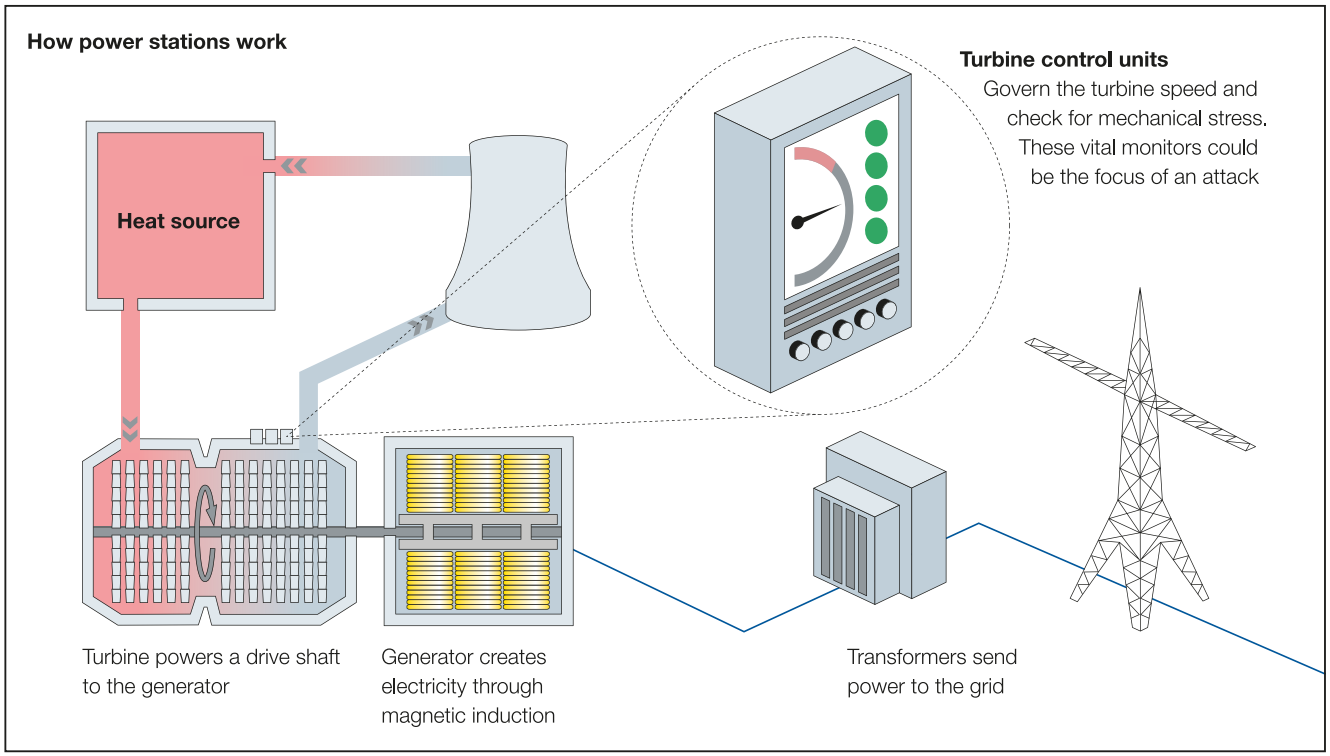


Figure 5: How a Cyber Attack Could Affect the Grid

as "Shamoon") in August 2012. The same malware was used against the RasGas Company in Qatar.[62]

In November 2012, an attack took place on the Internet infrastructure of 50Hertz, an electricity transmission network operator in northern and eastern Germany. Using a botnet, the unidentified attackers carried out a DDoS attack on the company's websites and email infrastructure.[63] Electricity supplies were not directly affected in this case, but could easily have been targeted in the attack.

2.5 Summary and Recommendations

Countries and their societies, industries and economies are dependent on fully functioning infrastructure, especially critical infrastructure. The operators of critical infrastructure, and increasingly non-nuclear critical energy infrastructure, face cyber attacks as a core challenge. At the same time, demand for energy is always on the rise. As the German government put it, "New solutions must be found that support the transition to liberalized markets, decentralized and volatile power generation structures, and electromobility – while also ensuring the maximum possible level of cost-effectiveness, security of supply, and environmental compatibility."[64] In this context, the security of critical infrastructure is a core issue in national, international, and corporate security dialogue and policies.

Threats relevant to critical infrastructure operators can be classified in a number of ways, but terrorist threats are clearly intentional threats. Although greater interconnection and integration of computerized control systems are making infrastructure easier to operate[65], they are also increasing the risk of manipulation and targeted attacks, such as cyber attacks. This makes cyber-related threats particularly important for non-nuclear critical energy infrastructure operators because, especially with cascade effects, a well co-ordinated cyber attack could cause far more damage than a physical attack. This makes critical energy infrastructure a potentially attractive target for terrorist attacks, since terrorists aim to cause as much damage and garner as much publicity as possible, unlike criminals whose focus is on profit. Because of close links in the systems and cascade effects, cyber attacks on non-nuclear critical energy infrastructure have great potential to cause long-term power outages.

Since recent cyber attacks on critical infrastructure have been increasingly successful, better protecting these infrastructure from attacks is a high priority. Insider threat is always one of the most potentially damaging, and some recent attacks may have involved compromise by employees. Rapidly-evolving technology and sophistication in the use of technology, the potential use of proxy actors and botnets for hire, and increasingly interdependent physical and cyber security systems are all increasing the complexity of the threat and the complexity of defending against it.

Although governments can help, most of the critical infrastructure is owned by the private sector in many countries. Therefore, public-private co-operation is essential. Non-nuclear critical energy infrastructure companies can introduce protective measures ranging from internal measures, such as training, awareness-raising and holistic protection concepts aimed at internal perpetrators, to activities steered by the government, such as a protection concept that views all critical infrastructure simultaneously and reduces dependencies and cascade effects. Non-nuclear critical energy infrastructure companies also need to focus on identifying and managing, if not limiting, their dependencies for purposes of protecting their companies in the event of a business partner's outage or the discovery of malware or other problems in an installed system. Safeguarding Supervisory Control and Data Acquisition (SCADA) systems makes it essential to take up these measures again.

62 RasGas, new cyber attack against an energy company, URL: http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html (01/29/2013)

63 European renewable power grid rocked by cyber-attack: EurActiv, URL: http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541 (12/10/2012)

64 German Federal Ministry of Economics and Technology (BMWi), URL: http://www.e-energy.de/958.php (12/04/2012)

65 For example, without computerized control systems a high number of personnel are involved to monitor the infrastructure and its systems and processes.

3. Good Practices in ICT Risk Management Frameworks to Address Cyber-related Terrorist Risks

OSCE Organization for Security and Co-operation in Europe

3. Good Practices in ICT Risk Management Frameworks to Address Cyber-related Terrorist Risks

This chapter addresses setting up an organizational ICT risk management framework in the energy sector. First we discuss ICT's general role and relevance for various subtasks in the energy sector and identify the key components that depend on ICT. On this basis, we then sketch an ICT risk management framework, referring to relevant international standards and particular approaches utilized in risk management for energy infrastructure. The chapter closes with a summary and recommendations for dealing with cyber-related risks in the non-nuclear energy sector.

3.1 Role and Relevance of ICT in the Energy Sector

Dependencies exist in many areas within non-nuclear critical energy infrastructure, such as between oil suppliers and primary energy producers. The supplier requires energy for raw materials extraction or delivery, and the energy producer needs the supplier. Conflicts of interest may occur if, for instance, the supplier demands a high price for its oil while also demanding energy at low cost. If the supplier demands both of the above from the primary energy producer, it may be that the latter can no longer operate cost-effectively. For this reason, it is important for both parties to work together. This also applies for measures taken to protect against cyber attacks and manage those attacks that occur. Non-nuclear critical energy infrastructure companies must therefore integrate the entire non-nuclear critical energy infrastructure supply chain into their own ICT risk management.

Because electrical power is generated and consumed simultaneously, operating an electric power system requires a system operator that constantly balances power generation and demand.[66] These system operators manage the electrical circuit and steer generation, transmission and distribution of electric power, aided by IT and network-based command and control systems that monitor sensitive processes and functions. The efficient functioning of the electricity industry is highly dependent on these steering systems.

As the electricity industry develops and technology advances, some power suppliers are already starting to upgrade their power grids.[67] New technologies, additional IT systems and networks are being integrated, particularly in transmission and distribution systems. In the course of this development, the industry and the government have developed the vision of a more reliable, efficient power grid that will enable the integration of alternative forms of power generation. The use of intelligent power networks known as "smart grids" requires greater use of IT systems, networks and interoperable communications in order to automate system operators' manual processes and actions.

➥ Figure 6: Common Smart Grid Components[68]

Future smart grid applications can go beyond just transmission and distribution subtasks; they could also increase the relevance of information and communications technology in storage and trading.[69]

Almost everyone agrees that smart grids are necessary, yet governments and industry have entirely different approaches and solutions for putting them into practice. This is due in part to the differing goals that motivate the various par-

66 US GAO 2011, Electricity Grid Modernization, p. 3 f
67 US GAO 2011, p. 4
68 US GAO 2011, p. 6
69 US GAO 2011, p. 6

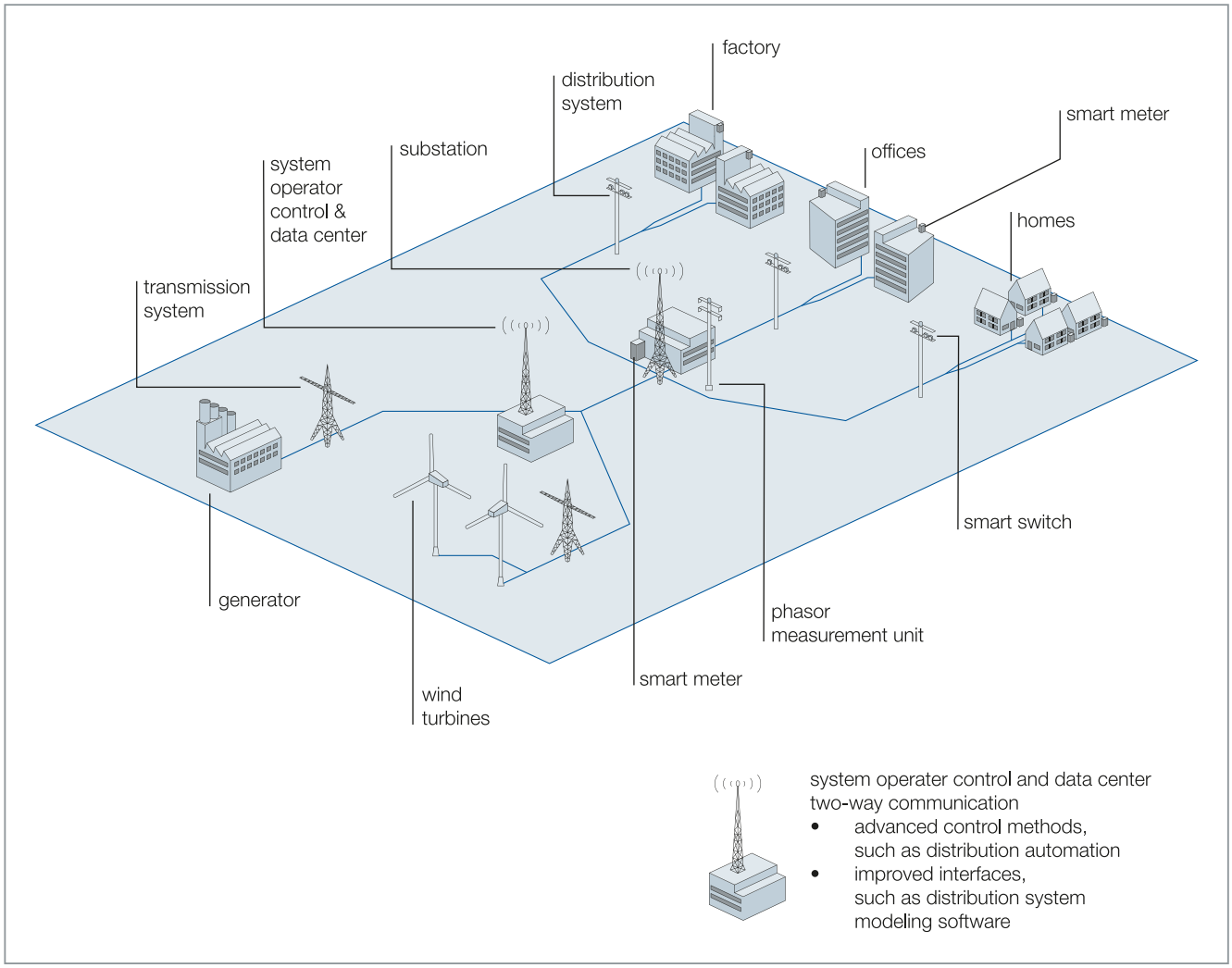


Figure 6 : Common Smart Grid Components

ties, but also to technological and legal constraints, since what is technically possible is not always permitted by law.

Generally, governments aim to ensure a secure power supply and maximize non-nuclear critical energy infrastructure's contribution to national economic output. Non-nuclear critical energy infrastructure companies' goals are generally purely economic; they focus on how to make maximum profit. A third party, the final energy consumer is only indirectly involved. They are generally interested in cheaper energy costs and security of supply. These diverse aims complement or oppose one another. The state and the non-nuclear critical energy infrastructure operators now face the task of finding the most efficient and effective route. One possibility would be to set up a roundtable – working groups at the national level.[70] Such a group would offer the parties an unprecedented way to meet and, under the leadership of the government, vote on which approach to take.

ICT has a central role to play in implementing smart grids and operating non-nuclear critical energy infrastructure. The following sections will examine and analyze further roles. ICT infrastructure is widely classified as critical by national governments and industry, like energy infrastructure.[71] Modern infrastructure increasingly uses linked ICT systems. This makes it more vulnerable to chain reactions in which an initial error or malfunction in one system may lead to the failure of many other systems.

70 The Federal Republic of Germany has already created a working group with a similar aim, namely, dealing with the switch from nuclear power to renewable energy sources: the "Plattform Erneuerbare Energien," set up by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU). Cf. URL: http://www.erneuerbare-energien.de/ (02/13/2013)

71 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf (03/13/2013)

No.	Threat	Explanation
1	Unauthorized use of remote maintenance access points	Maintenance access points are deliberately created external entrances to the ICS network and are often insufficiently secure.
2	Online attacks via office or enterprise networks	Office IT is usually linked to the network in several ways. In most cases, network connections from offices to the ICS network also exist, so attackers can gain access via this route.
3	Attacks on standard components used in the ICS network	Standard IT components (commercial off-the-shelf (COTS)) such as systems software, application servers or databases often contain flaws or vulnerabilities, which can be exploited by attackers. If these standard components are also used in the ICS network, the risk of a successful attack on the ICS network increases.
4	(D)DoS attacks	(Distributed) Denial-of-Service attacks can impair network connections and essential resources and cause systems to fail – in order to disrupt the operation of an ICS, for instance.
5	Human error and sabotage	Intentional deeds – whether by internal or external perpetrators – are a massive threat to all protection targets. Negligence and human error are also a great threat, especially in relation to the protection targets confidentiality and availability.
6	Introducing malware via removable media and external hardware	The use of removable media and mobile IT components of external staff always entails great risk of malware infection. See the Stuxnet case, for example.
7	Reading and writing news in the ICS network	Most control components currently use clear text protocols, so communication is unprotected. This makes it relatively easy to read and introduce control commands.
8	Unauthorized access to resources	Internal perpetrators and subsequent attacks following initial external penetration have it especially easy if services and components in the process network do not utilize authentication and authorization methods or if the methods are insecure.
9	Attacks on network components	Attackers can manipulate network components in order to carry out man-in-the-middle attacks or to make sniffing easier, for example.
10	Technical malfunctions or force majeure	Outages resulting from extreme weather or technical malfunctions can occur at any time – risk and potential damage can only be minimized in such cases.

Table 3: Top 10 Threats to Industrial Control Systems

ICT systems support the energy sector as follows:

- For monitoring and distribution
- To buy and sell power and fuel
- To report errors
- As an automatic protection system for detecting faults and, if necessary, rapidly separating the system from the network
- For general data transmission – including actual and predicted demand, installation status information, etc.

SCADA systems are a key element for the secure operation of all installations in the energy sector. These systems collect data using sensors, display the information, and save it to support installation monitoring. They are part of the process control systems used to measure the transmission and distribution of electrical power or the pressure inside gas pipelines, among other things. The advantages of a SCADA system include the ability to monitor several processes simultaneously and enable proactive management.[72] However, the advantages of having a single point of control and comprehensive networks covering all systems also bring the risk that they may become the focus of cyber-related terrorist attacks.

As part of its cyber security analyzes, the German Federal Office for Information Security (BSI) has drawn up a list of the most critical threats currently facing Industrial Control Systems (ICS), including SCADA systems. Threats are ranked by considering factors such as perpetrator groups, the distribution and ease of exploiting vulnerabilities, and the possible technical and economic consequences of an attack. To gain the information, databases of actual occurrences were also analyzed.

➥ Table 3: Top 10 Threats to Industrial Control Systems[73]

3.2 Potential Vulnerabilities in ICT

Cyber attacks are only possible if the threats described above encounter vulnerabilities in IT systems and networks. Most vulnerabilities in these systems are introduced during development or later, during implementation. In a McAfee study in 2011, 200 industry executives from critical energy infrastructure enterprises in 14 countries were surveyed on security practices, attitudes and policies. 80 percent of those surveyed said that they had been victims of a large-scale DoS attack during the past year. One year earlier, the figure had been just under 50 percent. According to McAfee, "85 percent had experienced network infiltrations."[74] The threat of cyber extortion has increased dramatically. Within one year the number of affected companies rose by a quarter. These cases of blackmail are evenly distributed across critical infrastructure sectors.

The moment where malware was discovered in Iranian nuclear power plants in 2010 was the moment when many security managers became aware of threats emanating from other countries. More than half of those surveyed assume that attacks on critical infrastructure in their home countries involved government actors.[75] It is not far from this assumption to the logical conclusion that terrorists too may use known vulnerabilities in critical infrastructure in order to cause enormous damage. Experts agree that attacks on critical infrastructure may appear more worthwhile than an attack on a military installation, but they do not have the same emotional effect as images of bombing civilian targets. However, the upper levels of terrorist organizations will be taken over by the next generation sooner or later, and they may have greater affinity with IT than their predecessors. This may lead to a significant increase in terrorist cyber attacks.[76]

To gain a comprehensive picture of vulnerabilities, threats and resulting risks, risk management should be carried out according to the methodology suggested in chapter 3.4. The risk identification process step focuses explicitly on identifying vulnerabilities so it plays an important part in determining future attack vectors. These vulnerabilities only lead to damage when they are exploited by an appropriate threat,[77] so they do not necessarily require corrective action. Initially, they only need to be detected and continually monitored for changes.[78]

72 Information about malfunctions is received almost in real time, making it possible to react extremely quickly to prevent the error from developing into an emergency or a crisis. This is usually referred to as proactive management.

73 BSI-A-CS 004, (2012)

74 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 6

75 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 9

76 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 15

77 See chapters 2.3 and 2.4.

78 Cf. ISO/IEC 27005, p. 16

Vulnerabilities may be identified in the following areas:[79]

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

The following table gives examples of ICT-related assets and suggests how attackers could target and exploit them.

Asset	Description of Possible Vulnerabilities and Attack Vectors
Software	Applications or system software may have accidentally or deliberately introduced flaws that can be exploited to subvert the purpose for which the software was designed.
Hardware	Vulnerabilities can be found in hardware, including microprocessors, microcontrollers, circuit boards, power supplies, peripherals such as printers or scanners, storage devices, and communications equipment such as network cards. Tampering with such components may secretly alter the intended functionality of the component or provide opportunities to introduce malware.
Seams between hardware and software	An example of such a seam might be the reprogrammable read-only memory of a computer (firmware) that can be improperly and clandestinely reprogrammed.
Communication channels	The communications channels between a system or network and the 'outside' world can be exploited by an adversary in many ways. Adversaries can pretend to be an authorized user of the channel, jam it, and thus deny use to its rightful users, or eavesdrop on the channel to obtain information intended to be classified or kept secret.
Configuration	Most systems provide a variety of configuration options that users can set based on their own tradeoffs between security and convenience. Because convenience is often valued more than security, many systems are – in practice – configured insecurely.
Users and operators	Authorized users and operators of a system or network can be tricked or blackmailed into doing the bidding of an adversary, or they may sell their services.
Service providers	Many computer installations rely on outside parties to provide computer-related services, such as maintenance or Internet service. An adversary may be able to persuade a service provider to take some special action on its behalf, such as installing attack software on a target computer.

Table 4: Cyber Vulnerabilities[80]

79 Cf. ISO/IEC 27005, p. 16

80 Based on Fred Schreier: On Cyberwarfare, p. 48

Smart grids are particularly vulnerable to targeted exploitation of potential vulnerabilities due to their increased dependency on IT systems and networks.[81] Some of the new challenges faced by smart grids arise from:

- Dependency on sensor data for network operation
- A larger surface for potential attacks

In addition, modern power installations are also highly dependent on automation, centralized control of installations and devices, and high-speed communications. Within the power systems, SCADA systems are highly critical.[82]

3.3 ICT-related Risk Management Frameworks for Non-Nuclear Critical Energy Infrastructure

Although this differs from one country to another, increasingly critical infrastructure is being operated by private rather than public organizations. This makes it even more important to develop a joint understanding for the secure operation of non-nuclear critical energy infrastructure. This is the only way to ensure that suitable mechanisms, including regulations, if appropriate, to facilitate communication and co-operation, as well as to maintain security of supply are put in place. The protection of critical energy infrastructure requires a joint understanding of the requirements that must be met as well as the vulnerabilities of all components that have an influence on the energy supply chain. One method of dealing with these aspects is to introduce a risk management framework.

When threats become risks…

"A threat has the potential to harm assets such as information, processes and systems and therefore organizations."[83]

3.3.1 Principles of Risk Management

Risk is an abstract and complex term that is considered in detail in the course of standardization. In general terms, risk can be taken to mean the effects of uncertainty on objectives.[84] Other approaches define risk as the combination of the probability of an incident and the extent of damage it would cause,[85] or the combination of the probability and impact of an event.[86]

The terms threat, vulnerability, and risk are often confused and are sometimes even used synonymously. To conform to standards, however, risk management requires a clear distinction between terms, which can be difficult in view of the different standards (see the following comparison between ISO 31000 and ISO 27000). Thus, it is important to establish one definition and use it consistently.

➥ Table 5: Comparison of ISO 31000 and ISO 27000[87]

The U.S. National Institute of Standards and Technology (NIST) provides a further example that also uses the term threat explained in chapter 2.3. This definition takes vulnerabilities into account as well as the consequences mentioned above.[88] In this context, the product of the interplay of threat, vulnerability, and consequence determines risk evaluation. The assumptions behind this

	ISO 31000	ISO 27000
Threat	-	Potential cause of an unwanted incident that may result in harm to a system or organization
Vulnerability	-	Weakness of an asset or control that can be exploited by a threat
Risk	Effect of uncertainty on objectives	Combination of the probability of an event and its consequence

Table 5: Comparison of ISO 31000 and ISO 2700087

81 US GAO 2011, p. 9

82 NAP: Terrorism and the Electricity Power Delivery System (2012), p. 2

83 ISO/IEC 27005:2011

84 Cf. ISO 31000:2009

85 Cf. ISO Guide 51:1999

86 Cf. ISO/IEC Guide 73

87 Cf. ISO 31000:2009 and ISO/IEC 27000:2009

88 U.S. NIST 2010, p. 9

model are particularly suitable for illustrating the dangers of terrorism, because the degree of impact is also taken into account.

➥ Figure 7: Generic Model of Risk[89]

ISO/IEC 27032 defines common risk management concepts and presents the concept of vulnerabilities, threats, and risks in their overall context.

➥ Figure 8: Definition of Concepts in ISO 27032[90]

Different principles and activities are needed to manage risk in an organization successfully. To enable a structured approach in dealing with risk, all required aspects must be combined and described in a comprehensive framework intended to support organizations in managing risks effectively and efficiently. The individual design of the risk management framework will depend on the size and complexity of the organization, its risk exposure, legal requirements, and the elements of risk management or management systems already on hand.

A variety of different approaches and standards for the actual design of a risk management framework already exist in different parts of the world.[91] At the international level, the International Organization for Standardization (ISO) has described the organizational framework and

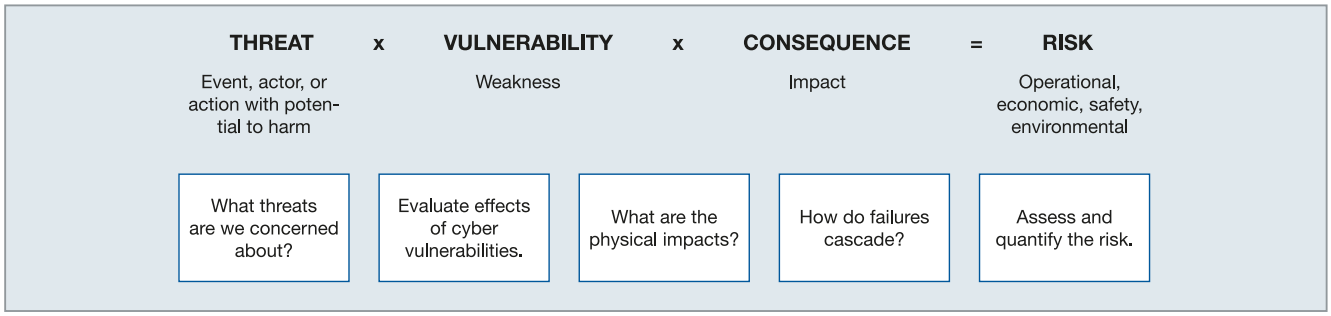


Figure 7: Generic Model of Risk

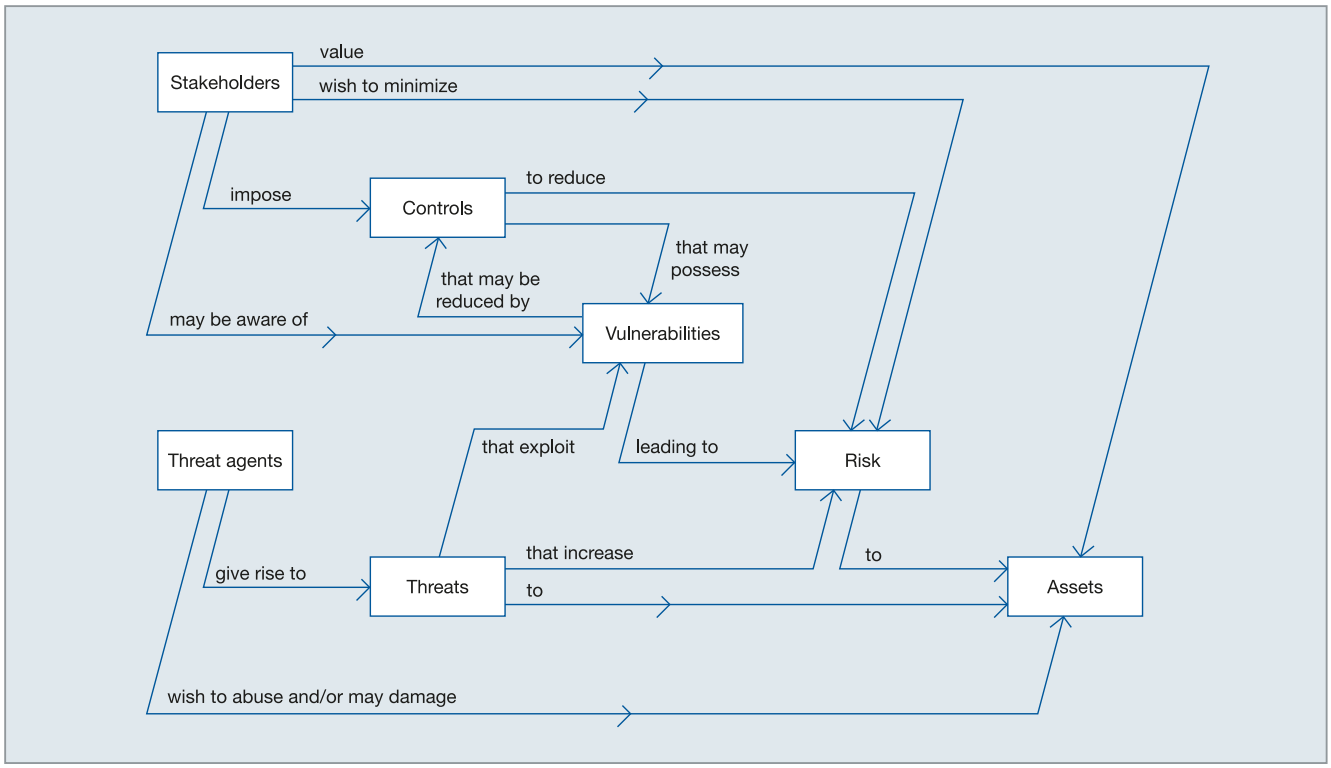


Figure 8: Definition of Concepts in ISO 27032

89 U.S. NIST, p. 9

90 ISO 27032

91 Because this guide is intended for an international audience, we do not provide a list of the different national standards. Instead, we focus on the international standards set out by the International Organization for Standardization (ISO).

the risk management process in ISO Standard 31000. The risk management process follows the PDCA principle[92] and is defined as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."[93] The actual methods for implementing risk management are described as a five-step process.

The ISO 27000 series adapts this process and presents a standard specifically for information security systems. ISO/IEC 27005 follows the general risk management approach of ISO 31000 and applies this to information security in particular. Due to the description of information security risk management, the implementation of the IT risk management described in the process makes a suitable basis for the development of an ICT-related risk management framework.

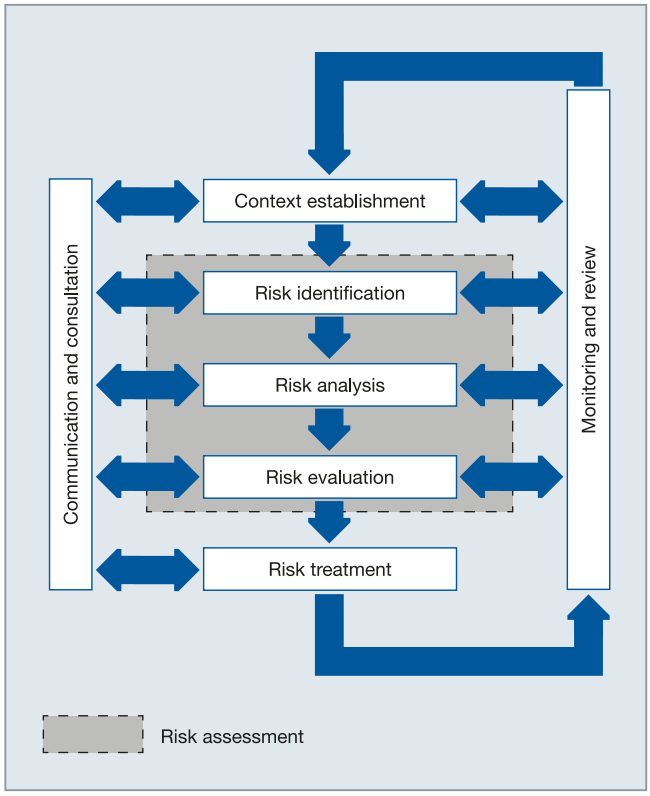


Figure 9: Overview of the Risk Management Process[94]

The first step is to establish a general context, while taking into account the targets and the definition of internal and external parameters. This is followed by the risk assessment, which represents the entire process of risk identification, analysis, and evaluation. A significant part of this process is the identification of potential dangers, events, developments or scenarios that could interfere with the organization's objectives. This process step should yield a comprehensive risk list. It is a particularly critical step because all risks not taken into account at this stage will be absent from all subsequent steps. For this reason, regular monitoring and review are particularly important; they should be planned as an essential part of the risk management process and include regular monitoring of individual process steps. In the context of risk identification, the overview of the situation could also be brought up to date regularly or on an ad hoc basis and new threats could be included in order to take account of future developments or changes in the risk environment.

Once the risks have been identified, their probability of occurrence and their impacts are determined to provide a basis for their evaluation. At this point, decisions are made on which risks need to be tackled and which priorities need to be set for implementing these measures. A variety of options is available for dealing with risks, such as avoiding, reducing, shifting or taking risks.

Risks are not static, however. Threats, vulnerabilities, probability of occurrence, and consequences can change suddenly and without warning. In order to ensure a complete and up-to-date overview of the risk landscape and identify changes, the risks need to be continually monitored and regularly reviewed. As with the 'feedback loop' in the U.S. NIPP risk management framework,[95] findings from these activities can be fed back as input into the various process steps, ensuring continual improvement in the risk management process.

In adapting the approach presented here to a particular organization or sector, it is important to take into account that the described approach is first and foremost a generic approach that takes account of basic functions. It needs to include an evaluation of the risks specific to an organization or affected sector. When establishing the general context, the process should be reassessed and possibly redefined in order to meet the individual requirements of the relevant organization or sector.

92 The PDCA Cycle, also known as the Deming Cycle, describes an iterative four-phase problem-solving process (Plan-Do-Check-Act). The ISO 31000 framework follows this model, essentially comprising the design, implementation, monitoring, and continuous improvement phases. We focus on the implementation phase here because it describes the actual process of risk management.

93 Cf. ISO 31000:2009, p. 2

94 ISO/IEC 27005:2011

95 NIPP 2009, p.4

3.3.2 Main Elements of the ISO/IEC 27000 series

The ISO/IEC 27000 series comprises a set of related Information Security Standards covering terminology, requirements, and general and specific guidelines. The series offers best practice recommendations for the individual components of the superordinate Information Security Management System (ISMS).

Standard Describing an Overview and Terminology	
ISO/IEC 27000	Overview and vocabulary
Standard Describing General Requirements	
ISO/IEC 27001	Requirements
ISO/IEC 27006	Certification body requirements
Standard Describing General Guidelines	
ISO/IEC 27002	Code of practice
ISO/IEC 27003	Implementation
ISO/IEC 27004	Measurement
ISO/IEC 27005	Risk management
ISO/IEC 27007	Guidelines for ISMS auditing
Standard Describing Sector-specific Guidelines	
ISO/IEC 27011	ISMS guidelines for telecommunication organizations
ISO/IEC 27031	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	Guidelines for cyber security
ISO/IEC 27033	Guidelines for IT network security

Table 6: Overview of the Components of the ISO/IEC 27000 Series[96]

3.3.3 Risk Management Approaches for Energy Infrastructure

Risk Solution and AEA Technology have been commissioned by the European Commission to develop a risk governance framework. The framework is designed to identify and deal with vulnerabilities in the energy sector and ICT sector. It aims to provide responsible parties in the energy sector with a standardized approach to quantifying and controlling risks in cross-border energy supply. The Risk Governance Framework is based on an analysis of what operators in the energy sector and Member States' governments are already doing and the actions that are required in the future in order to close existing security gaps in the system. In other words, it defines a minimum standard but leaves space for individual governments and operators to adapt it to their own needs.

The Risk Governance Framework is designed to be as useful as possible to the maximum number of stakeholders. To achieve this, it has been made flexible enough to allow each stakeholder to take into account the risks that exist in its own area of responsibility. For example, at the EU level, managing the risks to cross-border energy supply is the key driver for the use of this framework. At the Member State level, a network operator may wish to manage risks across other boundaries that are not necessarily cross-border. The framework can be used at every level, so before applying it one needs to specify at which of the following levels it is to be applied.[97]

- EU cross-border: Where an ICT system functional failure disrupts energy supplied in one Member State from reaching another Member State, or where the disrupted energy flow transits across a Member State en-route to its final destination.
- Non-EU cross-border: Where an ICT system functional failure in a non-EU country affects the flow of energy into a Member State.
- Member State national: Where an ICT system functional failure in one part of the country's national infrastructure affects energy supply to a significant proportion of the population within a single Member State.

96 ISO/IEC 27000

97 In the OSCE context, the following statements referring to the EU can be applied equally to the community of OSCE participating States.

- Inter-organizational: Where an ICT system functional failure in one organization affects the operations of another organization resulting in energy supply disruption within a single Member State.

- Intra-organizational: Where an ICT system functional failure in an energy company's own operations results in an energy supply disruption within its host Member State.

The generic approach to risk governance developed by the International Risk Governance Council (IRGC) is being used as a template structure for this process. This template breaks down the activities in the process into the following five elements:[98]

- Pre-assessment, which involves getting a broad picture of the risk.

- Appraisal, which identifies the knowledge needed for judgments and decisions.

- Characterization and evaluation, which assesses whether the risk is acceptable or not.

- Management, which identifies who needs to do what and when.

- Communication, which determines who needs to be told, when, and how.

As the European Commission Study explains it, "The energy/ICT Risk Governance Framework guides the user through four stages of pre-assessment, appraisal, characterization and evaluation, and management. At each stage it prompts users to consider the fifth element of communication. These steps can then be repeated to provide a basis for continual improvement."[99]

➥ Figure 10: IRGC Risk Framework[100]

Moreover, this framework recommends that every nation and organization should appoint an expert to be responsible for implementing the Risk Governance Framework and for pursuing its outcomes to reduce any perceived vulnerability. An example of best practice for an organization might include the following:[101]

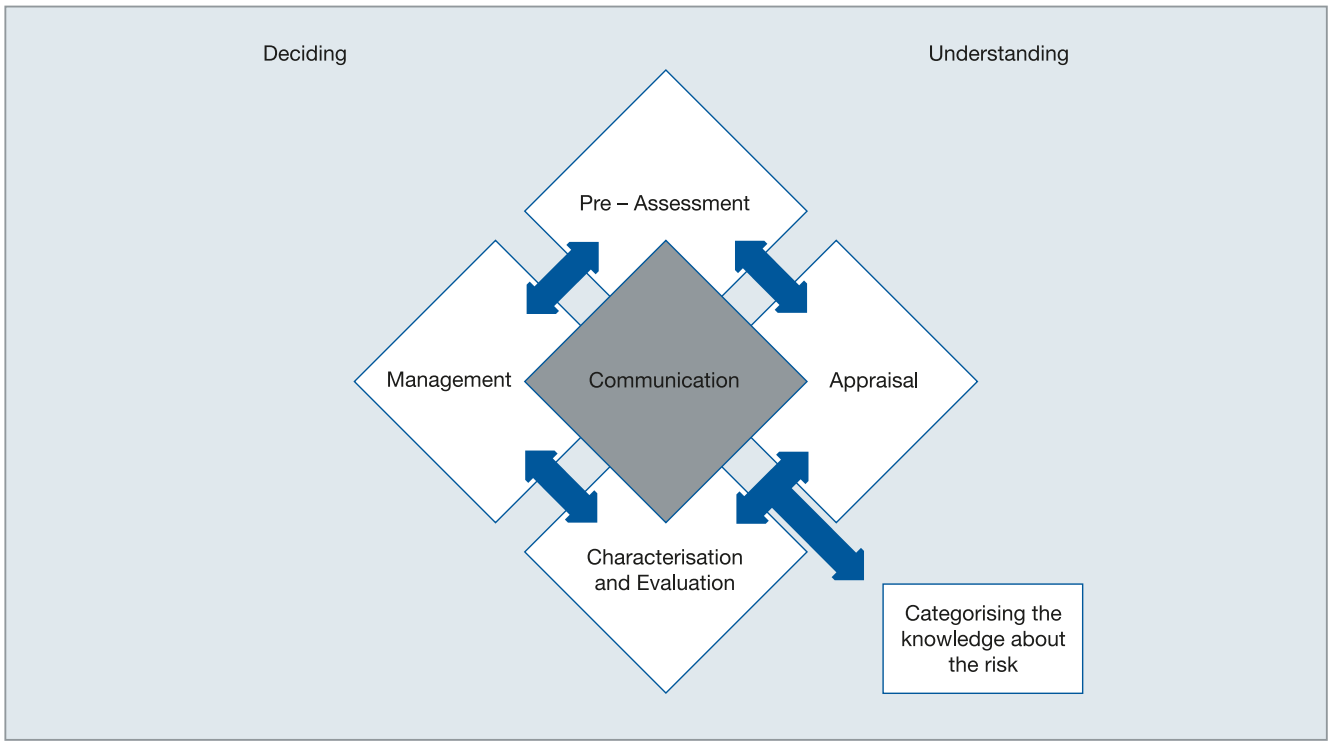


Figure 10: IRGC Risk Framework

98 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), p. 41

99 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), p. 41

100 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009)

101 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), p. 42

- A senior director or senior manager to sponsor the activity and give it the necessary authority within the organization.

- A risk manager who is an expert in the process and who can act as an internal consultant. This person would also usually take on responsibility for maintaining the master version of the risk register, tracking the progress of any agreed risk management actions that arise, and communicating the results of the risk assessments to other stakeholders such as the other parties involved in any cross border or cross boundary criticalities that have been identified. Potentially, the risk manager would also be responsible for communications with the European Commission.

- Energy and ICT infrastructure professionals would be responsible for identifying and evaluating the interface risks using the framework. This is best done as a collective exercise, for example in a series of workshops. The risk manager may be called upon to facilitate the workshops if necessary.

- Experts may be required to fully quantify the political, economic, and social impacts of energy disruption if a more detailed impact and concern (or risk) assessment is undertaken within a Member State. This goes beyond the qualitative risk ranking scales proposed here.

- Where further risk reduction measures are required for particular critical interfaces, the responsibility for delivering the agreed action plan should reside with the person best able to deliver it in each case.

The individual tasks in each phase are summarized in chapter 3.5. Further suggestions regarding how to proceed can be found in the appendix of the Study on Risk Governance of European Critical Infrastructure in the ICT and Energy Sector.

The aspect of Public-Private Partnerships (PPPs) should also be considered when implementing the Risk Governance Framework.[102] The Action against Terrorism Unit (ATU)[103] of the OSCE Secretariat published a policy brief on this topic[104] in September 2010 summarizing key policy recommendations for critical energy infrastructure. The recommendations were hammered out at an OSCE-sponsored public-private expert workshop called "Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks." The OSCE points out that these recommendations do not necessarily imply endorsement by all OSCE participating States or the OSCE Secretariat.

Key policy recommendations:

1. **Follow a comprehensive risk-based approach.**
   Arrangements to protect energy infrastructure should be dynamic and informed by an all-hazard and regularly updated assessment.

2. **Develop a multi-stakeholder co-operation framework.**
   A comprehensive approach to critical energy infrastructure protection as outlined above requires the co-ordinated involvement of multiple stakeholders, from different state agencies, from both the public and private sectors, as well as from stakeholders across borders.

3. **Design flexible security arrangements ensuring an adequate minimum level of protection.**
   The vulnerabilities and the risk environment of each critical energy infrastructure are specific and dynamic; their protection must take this into account to be commensurate to the risks and cost-effective.

4. **Place greater emphasis on preparedness and overall resilience.**
   Preparedness requires advanced contingency planning, testing and exercising, including plans for communicating with the public/consumers and energy markets. Regarding resilience, a need exists for more investments in network interconnections and alternative routes, as well as to increase storage capacity/strategic reserves.

5. **Identify and address cyber vulnerabilities of the energy sector.**
   Traditional physical security measures ("guns, gates and guards") are no longer sufficient in today's increasingly computerized and ICT-dependent world. The level of public and corporate awareness and understanding of cyber security issues needs to be dramatically raised and the development of cyber security expertise should be promoted.

102 See chapter 5.1

103 Cf. OSCE, URL: http://www.osce.org/atu (02/13/2013)

104 Cf. Protecting Critical Energy Infrastructure from Terrorist Attacks, URL: http://www.osce.org/atu/73638 (02/13/2013)

6. **Develop effective Public-Private Partnerships**
   The respective security roles and responsibilities of private stakeholders and state authorities should be clearly defined. Partnerships can be developed for joint critical energy infrastructure security assessment, review of security measures, elaboration of contingency plans, and incident response training.

7. **Enhance cross-border / international co-operation.**
   The disruption of a single energy infrastructure can impact far beyond the national borders of the country where it is located, whether in terms of supply discontinuation, or other damage, including economic (e.g., soaring prices in volatile energy commodity markets) or environmental damage. Countries should take stock of these direct and indirect dependences, which entail a vested interest in co-operating to ensure the integrity of energy infrastructure.

Of course, other countries and organizations have developed risk management frameworks. For example, the U.S. Risk Management Framework is an integral part of the U.S. NIPP.[105]

3.4 Summary and Recommendations

This chapter looked at Good Practices in ICT Risk Management Frameworks to address relevant terrorist risks. The topics it covered included the roles and relevance of ICT, key components that depend on ICT, risk management frameworks, future attack vectors, and the role of governments.

To sum up, it can be said that electrical systems are becoming increasingly complex and thus more susceptible to outages. System operators manage the electricity cycle with the aid of IT and network-based control systems that monitor sensitive processes and functions. Smart grids will increasingly replace existing power grids in the future, automating the manual processes and actions carried out by system operators and improving co-ordination of electricity generation and storage, while at the same time introducing new vulnerabilities.

ICT infrastructure are considered to be critical. Because ICT infrastructure are interlinked, there is a greater likelihood of chain reactions. SCADA systems are part of the process control systems and provide the option of controlling several processes simultaneously. However, having a single point of control and a tight network also means greater potential for possible attacks.

The protection of critical infrastructure in general and the interconnectedness of critical infrastructure and ICT systems are particularly important topics for both public authorities and private actors. In general, it must be kept in mind that more and more system vulnerabilities are emerging in the area of cyber security and being aware of, and prepared for, potential threats is increasingly important. Introducing a risk management framework provides one method of identifying and dealing with vulnerabilities.

The risk governance framework presented in chapter 3.4.3 comprises several phases. Within each phase, tasks are described which should provide support when implementing the framework. Below is a summary of the tasks in each one of these phases:[106]

Pre-assessment phase

1. Define the interfaces between the energy and ICT systems that are potential targets and need to be considered in the risk governance process. These are the interfaces between energy and ICT systems that if compromised could cause a disruption to cross-border energy supplies.

2. Define the principal actors to be included in the risk assessment process and their particular areas of responsibility with regard to the systems under consideration.

3. Define the principal documents, standards, and regulations that are pertinent to the systems being considered.

4. Consider whether changes in markets, supply chains, and technologies might have increased the risks of disruption to energy supply, in both the energy and ICT sectors.

105 For a brief description of the U.S. NIPP Risk Management Framework, see http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

106 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), p. 43 ff

Appraisal phase

1. Using the list of potential target systems from the pre-assessment phase, consider the impact resulting from a functional failure of each system and score each of them according to an agreed scale.

2. Review the concern assessment for the threat of energy disruption due to critical energy/ICT interfaces.

3. For each of the potential target systems identified in task 1, list the most likely threats that could successfully compromise the system and cause a failure, given the defenses that are in place today.

4. For each system with a criticality score, identify the likelihood of a threat being successful.

5. Categorize each risk event according to the quality of knowledge available.

Characterization and evaluation phase

1. Place each risk event that has been identified on a risk tolerability matrix. Use the impact and vulnerability values recorded in previous tasks.

2. Review results so far to reveal any missing information or concealed risk events.

3. Describe the prioritized risk events, with supporting rationale.

Management phase

1. Consider the available options for managing the priority risks and choose the ones that would be most effective. Form a risk management strategy.

2. Plan who should implement activities to manage risks by when, and gain their commitment.

3. Evaluate progress of risk management and if necessary improve the program.

The entire Risk Governance Framework and sample checklists and templates can be found in the appendix of the European Commission document.[107]

107 European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009)

4.
Good Practices in ICT-related Security Measures to Address Cyber-related Terrorist Risks

OSCE Organization for Security and Co-operation in Europe

4. Good Practices In ICT-related Security Measures to Address Cyber-related Terrorist Risks

This chapter summarizes good practices in the field of ICT-related security measures with a focus on cyber-related terrorist threats. In the process, it discusses relevant standards and strategies.

4.1 Addressing ICT-related Standards

Other sectors already have a variety of established standards with security requirements and measures that can be applied to non-nuclear critical energy infrastructure and ICT systems.[108] Work is currently underway to enhance these standards and produce additional standards. The following standards are particularly relevant for the cyber security of ICT systems in non-nuclear critical energy infrastructure:

- The ISO 27000 series should be mentioned first. It describes operational and technical requirements for information security management. The ISO 27001 standard for information security management provides the foundation, which is developed in more detail in ISO standard 27002. Higher numbered standards – many of them still in active development – specify sector-specific implementations.

- One of the most recent standards in this series, ISO 27032[109] specifically targets the problems arising from the complex interaction of Internet security, network security and application security. It, therefore, discusses controls for all cyberspace stakeholders (consumer and provider organizations). It is unique in that it explicitly targets topics such as controls against social engineering attacks, cyber security readiness, and awareness. Most importantly, it includes a framework for information sharing and co-ordination.

- IEC 62351 directly targets information security for power system control operations. It primarily implements standards for security affecting the communication protocols defined by the IEC TC 57 working group, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. These standards are mainly applicable for manufacturers. The M/490 SGIS[110] group intends to expand these standards to include specific technical aspects for smart grid cyber security.

- The IEC 62443 series (derived from ISA-99[111]) covers security for Industrial Automation and Control Systems (IACS). The focus is on operational best practices. The standard is driven by vendors and end-users from different industrial sectors, including major oil and gas companies.[112] It targets asset owners, system integrators and component providers with separate sub-standards. IEC 62443 tries to include and align with existing standards – in particular with NISTIR 7628 and ISO 27001/2. The series is published,[113] but major changes have been announced and are already available in draft form. The current phase is expected to be finalized in early 2013.

- NIST Special Publication 800-39, Managing Information Security Risk – Organization, Mission, and Information System View, is the flagship document for the FISMA[114]-related security standards and guidelines developed by NIST, referencing all further related NIST publications.

108 European Commission: WP 2.2 Inclusion of effective security measures for smart grid security and resilience (2012)

109 BS ISO/IEC 27032:2012 Guidelines for cybersecurity

110 European Commission EG-ENERGY, M/490 Mandate, SGCG-SGIS Working Group

111 ISA-99: Industrial Automation and Control Systems Security, series of standards from the International Society of Automation (ISA)

112 IEC 62443-2-4 A Baseline Security Standard for Industrial Automation Control Systems, URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf (02/14/2013)

113 Crucial sections were finalized between 2009 and 2011.

114 U.S. federal law: Federal Information Security Management Act of 2002 (FISMA)

For the ISMS framework, it references – like other NIST publications – the ISO 27000 standards as well as ISO 31000 / ISO 27005 (risk management). It recommends a unifying risk management approach.

- NISTIR 7628 (Guidelines for Smart Grid Cyber Security) targets cyber security for electric power infrastructure. The report focuses on security requirements. Part 1 lists high-level security requirements and heavily references other NIST standards for specific requirements. It identifies seven domains in the smart grid (Operations, Distribution, Transmission, etc.) and defines logical interface categories (e.g., interfaces between control systems within the same organization and within different organizations). Security requirements (e.g., integrity, authentication, bandwidth, real-time requirements) are then applied to these interface categories.

- Most of the security requirements in NISTR 7628 are covered by ISO 27001, 27002 and IEC 62351. Appendix A of the Catalog of Control System Security Recommendations has a 90 percent overlap with NIST but also contains additional cross-references to the security measures in the following standards: FIPS 140-2, NERC CIP, and IEEE 1402 (Guide for Electric Power Substation Physical and Electronic Security).[115]

- The North American Electric Reliability Corporation (NERC) has created the NERC Critical Infrastructure Protection (CIP) cyber security standards.[116] There are separate standards from CIP-002 through CIP-009 for building a comprehensive cyber security framework. CIP compliance has been mandatory for power suppliers since the Energy Policy Act of 2005 (EPAct). Audits started in 2011. CIP also uses a risk-based approach and focuses specifically on the "Cyber Critical Assets" group in the Bulk Electric System.

CIP-002	Critical Cyber Asset Identification
CIP-003	Security Management Controls
CIP-004	Personnel and Training
CIP-005	Electronic Security Perimeter
CIP-006	Physical Security of BES Cyber Systems
CIP-007	Systems Security Management
CIP-008	Incident Reporting and Response Planning
CIP-009	Recovery Plans for BES Cyber Systems

Table 7: Individual NERC CIP Standards (Requirements)[117]

NIST SP 800-53 (Recommended Security Controls for Federal Information Systems and Organizations)[118] provides security control selection for U.S. federal information systems based on a risk management framework. It also provides a set of baseline security controls as a minimum standard. Rev. 3 includes an appendix for ICS security controls. Contents from that appendix will be transferred to NIST SP 800-82 in the final revision.

NIST SP 800-82 (Guide to Industrial Control Systems Security) focuses specifically on SCADA systems and PLC/DCS. It shows threats and vulnerabilities along with mitigating measures. SP 800-39 is referenced for the overall framework.

All above-mentioned standards (with the exception of IEC 62351, which is too narrow in scope[119]) are based on classic risk-based approaches compatible with risk-management standards such as ISO 27005.

115 European Commission: WP 2.2 Inclusion of effective security measures for smart grid security and resilience (2012)

116 Derived from the NERC 1200 (and later 1300) standards

117 NERC: Mandatory Standards Subject to Enforcement, URL: http://www.nerc.net/standardsreports/standardssummary.aspx (02/13/2013)

118 Currently in Rev. 3 (2009) with updates from 2010

119 IEC 62351 focuses only on secure protocol implementation issues and is therefore more important for equipment manufacturers.

In the field of industrial components (SCADA), the ICE 62443 standard has been enhanced and adjusted to conform to the ISO/IEC 27000 series. The current draft is set to be finalized in early 2013. This standard is expected to gain broad acceptance due to the fact that the industrial sector was heavily involved in the improvements.

➥ Figure 11: IEC 62443 Standard Series[120]

Due to the high degree of overlap between the ISO 27000 series and the NISTR 7628 standard for smart grid security, the M/490 SGIS group has recommended the development of an industry-specific standard for smart grids within the ISO 27000 series. This standard would aim to cover important aspects of smart grid cyber security. It would also make developers and installers of ICT bear some of the responsibility, not just owners and operators.

Overall, a great deal is happening in the fields of standardization and regulation globally, and developments deserve close attention.

4.2 Creating National Cyber Security Strategies

Strategies define ends, ways, and means in relation to a specific sphere of activity. A national cyber security strategy (NCSS) is one approach to improving security and stability in the use of cyberspace. The extent to which national critical infrastructure is dependent on cyber applications generally plays a key role in this context. The NCSS therefore provides a "strategic framework for a nation's approach to cyber security."[121]

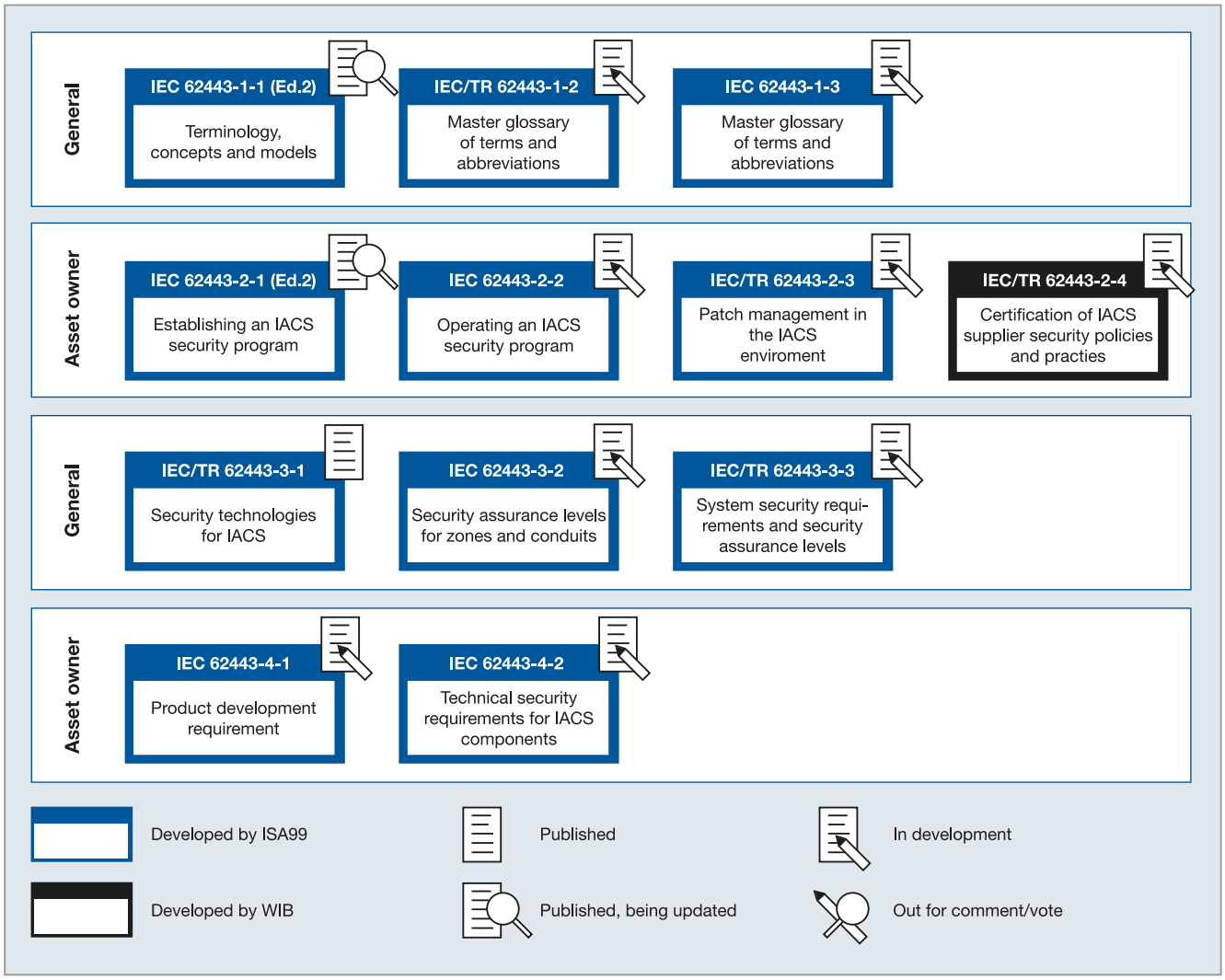


Figure 11: IEC 62443 Standard Series

120 Security for industrial automation and control systems (2011), URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf (02/14/2013)

121 National Cyber Security Strategies: ENISA (2012), p. 4

At present there is no common definition of cyber security at the international level. The 2013 release of the Cyber security Strategy for the European Union: An Open, Safe and Secure Cyberspace, provided a European definition for the term[122]. However, concepts of cyber security and other key terms vary from one country to another. The lack of an international strategy to improve cyber security makes international co-operation somewhat more difficult.[123] Most national cyber security strategies or international organizations' equivalent statements of principles attempt to compensate for this deficiency by explicitly addressing the specific role of international collaboration and indicating suitable measures that could promote and support co-operation between nations, such as confidence-building measures and norms of behavior in cyberspace.

4.2.1 EU Nations

In addition to the EU cyber security strategy and the proposed directive of the European Commission[124], ten EU Member States have published national cyber security strategies in the last four years. The ENISA provides a summary of each strategy:[125]

➥ Table 8: National Cyber Security Strategies (EU Nations)

Country	Summary
Estonia (2008)	Estonia emphasizes the necessity of secure cyberspace in general and focuses on information systems.[126] The recommended measures are all of a civil character and concentrate on regulation, education and co-operation.
Finland (2008)	The basis of the strategy is a view of cyber security as a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society.
Slovakia (2008)	Ensuring information security is viewed as being essential to the functioning and development of society. Therefore the purpose of the strategy is to develop a comprehensive framework. The strategic objectives of the strategy are mainly focused on prevention as well as readiness and sustainability.
Czech Republic (2011)	Essential objectives of the cyber security strategy include protection against threats that information and communication systems and technologies are exposed to, and mitigation of potential consequences in the event of an attack against ICTs. The strategy focuses mainly on unimpeded access to services, data integrity, and confidentiality of the Czech Republic's cyberspace and is co-ordinated with other related strategies and concepts.

Continued on next page

122 European Commission: Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace (02/07/2012), p. 3, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

123 European Commission: Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace (02/07/2012), p. 3, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

124 European Commission: Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final, 02/07/2013

125 National Cyber Security Strategies: ENISA (2012), p. 5 , and http://www.ccdcoe.org/328.html (March 2013)

126 In May 2007, Estonia was the first European state to experience a mass cyber attack on its government and banking networks and a political party website, only part of which could be blamed to an individual. See "Estonia fines man for 'cyber war'". BBC. 2008-01-25. Retrieved 2013-03-22. http://news.bbc.co.uk/2/hi/technology/7208511.stm.

Country	Summary
France (2011)	France focuses on enabling information systems to resist events in cyberspace that could compromise the availability, integrity or confidentiality of data. France stresses both technical means related to the security of information systems and the fight against cybercrime and the establishment of a cyber-defense.
Germany (2011)	Germany focuses on preventing and prosecuting cyber attacks and also on the prevention of coincident IT failures, especially where critical infrastructure are concerned. The strategy sets the groundwork for the protection of critical information structures. It explores existing regulations to clarify whether, and if so, where additional powers are required to secure IT systems in Germany by means of providing basic security functions certified by the state and also supporting SMEs by setting up a new task force.
Lithuania (2011)	Lithuania aims to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity, and accessibility of electronic information and services provided in cyberspace; safeguarding electronic communication networks, information systems and critical information infrastructure against incidents and cyber attacks; and protecting personal data and privacy. The strategy also defines the tasks, which when implemented would allow total security of cyberspace and entities operating in it.
Luxembourg (2011)	Recognizing the pervasiveness of ICTs, the strategy states that it is a priority to prevent any adverse effects on health and public safety or on the economy. It also mentions the importance of ICTs for citizens, society and for economic growth. The strategy is based on five action lines. These can briefly be summarized as CIP and incident response, modernizing the legal framework, national and international co-operation, education and awareness, and promoting standards.
Netherlands (2011)	The Netherlands aims for safe and reliable ICTs and fears abuse and (large-scale) disruption – and at the same time it acknowledges the need to protect the openness and freedom of the Internet. The Netherlands includes a definition of cyber security in the strategy: "Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."
United Kingdom (2011)	The UK approach is concentrating on the national objectives linked to evolving cyber security: making the UK the major economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace. The objective is to tackle the risks from cyberspace like cyber attacks from criminals, terrorists, and states in order to make it a safe space for citizens and businesses.

Table 8: National Cyber Security Strategies (EU Nations)

4.2.2 Non-EU Nations

This section briefly presents the cyber security strategies of three non-EU nations.[127] Other countries such as Australia,[128] India,[129] and New Zealand[130] have also published national cyber security strategies.

United States

The United States first published the National Strategy to Secure Cyberspace in 2003 as part of the National Strategy for Homeland Security. The document describes a set of activities in seven mutually dependent fields based on a collaborative model involving government, international partners, and the private sector:

- Economy: Promoting International Standards and Innovative, Open Markets
- Protecting Our Networks: Enhancing Security, Reliability, and Resiliency
- Law Enforcement: Extending Collaboration and the Rule of Law
- Military: Preparing for 21st Century Security Challenges
- Internet Governance: Promoting Effective and Inclusive Structures
- International Development: Building Capacity, Security, and Prosperity
- Internet Freedom: Supporting Fundamental Freedoms and Privacy

The U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World[131], released in May 2011, articulates U.S. international policies focusing on an open and interoperable, secure and reliable cyberspace, stability through norms of behavior in cyberspace, and the use of diplomacy, defense, and development to meet 21st challenges. In addition, recognizing the increasingly serious threats to U.S. critical infrastructure and the need for integrating physical and cyber security in protecting critical infrastructure, the United States released in February 2013 an Executive Order on Improving Critical Infrastructure Cyber security at the same time as, and to be implemented together with, a new Presidential Policy Directive on Critical Infrastructure Systems and Resilience (PPD-21)[132]. Both documents task U.S. government agencies at all levels to better identify and protect U.S. critical infrastructure and greatly enhance public-private co-operation and communication, including on threats and mitigation, since approximately 85% of U.S. critical infrastructure is owned and operated by the private sector.

Canada

Canada published a cyber security strategy in 2010[133] that is built on three pillars:

- Securing government systems: The first pillar aims to establish clear roles and responsibilities to strengthen the security of federal cyber systems and enhance cyber security awareness throughout the government.
- Partnering to secure vital cyber systems outside the federal government: The second pillar covers a number of partnering initiatives with the provinces and territories and involving the private sector and critical infrastructure sectors.
- Helping Canadians to be secure online: The third pillar covers combating cybercrime and protecting Canadian citizens in online environments. Privacy concerns are addressed in this pillar.

127 National Cyber Security Strategies: ENISA (2012), p. 7 f

128 Australian Government: Cyber Security Strategy (2009), URL: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf (02/15/2013)

129 Department of Electronics and Information Technology, Government of India, URL: http://deity.gov.in/content/cyber-security-strategy (02/15/2013)

130 New Zealand Government: Cyber Security Strategy (2011), URL: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf (02/15/2013)

131 International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, (May 2011), URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

132 U.S. White House: Executive Order on Improving Critical Infrastructure Cybersecurity, (02/12/2013), URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

U.S. White House: Presidential Policy Directive on Critical Infrastructure Systems and Resilience (PPD-21), (02/12/2013), URL: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

133 Canada: Canada's Cyber Security Strategy – For a stronger and more prosperous Canada (2010), URL: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx

Japan

Japan published a cyber security strategy in 2010[134] that can be divided into several key areas of action of its own:

- Reinforcement of policies taking account of possible outbreaks of cyber attacks and establishment of a response organization
- Establishment of policies adapted to changes in the information security environment
- Establishing active rather than passive information security measures

The main action points covered by the strategy include:

- Overcome IT risks to realize safety and security in the nation's life.
- Implementation of a policy that strengthens national security and crisis management expertise in cyberspace, and integrity with ICT policy as the foundation of socioeconomic activities.
- Establishment of a triadic policy that comprehensively covers the viewpoints of national security, crisis management, and nation/user protection. An information security policy with a focus on the nation's/users' viewpoint is particularly important.
- Establishment of an information security policy that contributes to the economic growth strategy.
- Building up international alliances.

4.2.3 Policy Recommendations for Cyber Security

The significance of cyber security has been recognized, as can be seen in the multitude of national strategies and statements of principles recently published on the topic by many OSCE participating States. However, the documents also reveal considerable differences in their definitions of cyber security and other key terms. While preparing its overview of all NCSS, ENISA has made recommendations for future co-operation of all EU Member States in the field of cyber security. These recommendations could be applied to international co-operation between all countries. The most important recommendations are listed below:[135]

Short-term:

- Clearly state the scope and objectives of the strategy as well as the definition of cyber security used in the strategy.
- Ensure that input and concerns from all governmental departments, national regulatory authorities, and other public bodies are heard and addressed.
- Collaborate with other Member States and with the European Commission to ensure that the cross-border and global nature of cyber security is addressed in a coherent fashion.
- Recognize that the constant development and evolution of cyberspace and cyber security issues means that the strategy will have to be a living document.
- Be aware that the above point does not just apply to emerging threats, but also to opportunities to improve and enhance the use of information and communication technologies for government, industry and citizens.

Long-term:

- Agree on a commonly accepted working development of cyber security that is precise enough to support the definition of common goals across the EU.
- Ensure that the cyber security strategies of the EU and its Member States do not conflict with the goals of the international community, but rather support the efforts to tackle cyber security challenges globally.

ENISA is compiling a good practices guide to support countries in developing, implementing, and maintaining an NCSS.

134 Japan: Information Security Strategy for Protecting the Nation (05/11/2010), URL: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

135 National Cyber Security Strategies: ENISA (2012), p. 12

The public and private sector should co-operate more closely in implementing the NCSS. ENISA recommends co-operating in the exchange of information, making best practices available, and conducting national and international exercises.

4.2.4 Policy Recommendations for "Smart Grid" Cyber Security

Smart grid security has gained a prominent position as a future challenge in the area of cyber security, especially for the energy sector. ENISA has issued a comprehensive study on this topic[136] that culminates in ten fundamental recommendations. Although primarily directed at EU institutions and Member States, the ideas contained in the paper's recommendations could be equally applied to other OSCE participating States:

- Recommendation 1. The European Commission (EC) and the Member States' (MS) competent authorities should undertake initiatives to improve the regulatory and policy framework on smart grid cyber security at the national and EU level.
- Recommendation 2. The EC in co-operation with ENISA and the MS should promote the creation of a Public-Private Partnership to co-ordinate smart grid cyber security initiatives.
- Recommendation 3. ENISA and the EC should foster awareness-raising and training initiatives.
- Recommendation 4. The EC and the MS in co-operation with ENISA should foster dissemination and knowledge-sharing initiatives.
- Recommendation 5: The EC should pursue efforts in collaboration with ENISA, the MSs cyber security authorities, private sector and possibly some non-EU partners, in order to develop a minimum set of security measures based on existing standards and guidelines.
- Recommendation 6. Both the EC and the MS competent authorities should promote the development of security certification schemes for components, products, and organizational security.
- Recommendation 7. The EC and MS competent authorities should foster the creation of test beds and security assessments.
- Recommendation 8: The EC and the MS, in co-operation with ENISA, should further study and refine strategies to co-ordinate measures countering large scale pan-European cyber incidents affecting power grids.
- Recommendation 9: The MS competent authorities in co-operation with CERTs should initiate activities in order to get CERTs involved to play an advisory role in dealing with cyber security issues affecting power grids.
- Recommendation 10. EC and the MS competent authorities in co-operation with the academic and R&D sector should foster research on smart grid cyber security, leveraging existing research programs.

4.3 Implementing a Risk-based Security Management Framework

Information Security Management Systems provide the basis for the implementation of any ICT security concept. They provide the processes, policies, and organizational structures necessary for continuous control of cyber security measures.

While the choice of applicable or certifiable standards may depend upon territorial considerations (i.e. North America vs. European countries), the pertinent standards – ISO 27001/2, NISTIR 7638, NERC CIP, and IEC 62433 – point towards a common (and compatible) overall approach: a security framework driven by a risk-management approach that identifies risks applying to the underlying ICT assets (NERC CIP even inserts a preliminary step: the identification of critical cyber assets).

The most widely certified ISMS standard, ISO 27001 (with over 7940 certifications worldwide[137]), is compatible or has been made compatible with all approaches and will be taken as a basis for an overarching ISMS.

A common approach in the more specific standards (IEC 62433, NERC CIP) is to define a baseline security or mini-

136 Based on ENISA: Smart Grid Security: Recommendations / Survey and Interview analysis (2012)

137 As of August 2012, URL: http://www.iso27001certificates.com/ (02/13/2013)

mum set of measures to be applied regardless of risk assessment. This concept is very similar to the one behind Germany's IT-Grundschutz Catalogues.[138] It is designed to create comparable results in light of the sometimes very individual results obtained in the world of a pure risk management-based approach such as ISO 27001. It may also simplify the implementation of the standards by reducing the initial overhead of risk identification.

4.4 Including IACS/SCADA in Information Security Management Systems

Industrial Automation and Control Systems security is rarely included in the framework of Information Security Management Systems. Problems arise from the fact that IT security has historically taken different routes, and while the processes themselves are compatible, many of the terms and definitions are different or even incompatible.

The common approach of the above-mentioned standards is to include IACS in a risk-based security management framework. Figure 11 shows how IEC 62433 addresses the topics for different stakeholders (asset owner, system integrator, component provider). When doing so, the following main challenges need to be tackled:

- **Cope with conceptual differences in the security objectives**

  Industrial security is often synonymously used with safety; information security deals with confidentiality, integrity, and availability. To be able to operate on common ground, security objectives need to be defined in a common way.

  - The order of importance is usually given as integrity, availability and confidentiality for IACS.
  - These need to be combined with their health, safety, and environmental (HSE) impact.[139]
  - Resulting known IACS concepts such as the safety integrity levels (SIL) have to be included.
  - Impact on process functionality and production capacity also needs to be considered.
  - Modify risk management approach
  - IEC 62443 uses ISO 27005-compatible risk management but slightly modifies it for IACS to make it a multi-stage risk assessment process that starts at the top level and gradually goes deeper.

- **Modify vulnerability assessment strategies**

  Traditional approaches in ICT security often use a combination of penetration testing and configuration audits to identify vulnerabilities. Standard ICT system penetration testing can have potentially disastrous effects on ICS safety and may severely disrupt operations. Penetration testing should be specifically designed for industrial environments and use precautions to prevent possible physical impacts of testing-induced failures.

- **Introduce IACS patch management (separate from ICT patch management)**

  Patch management is the number one challenge in IACS. ICT security has adopted a policy of frequent patches to stay up-to-date against new vulnerabilities and attacks exploiting these vulnerabilities.

Installing patches in IACS environments has the potential to create interference or lasting damage if the system does not respond as expected. This creates the additional burden of identifying the patches that actually need to be applied and then testing them. Vendor testing cannot assure that all processes will be unaffected by changes; only tests in the actual environment can.

IACS patch management should take into account that:

- Some devices may be beyond patch management (e.g., because the supplier does not offer a patch at all).
- It may be impossible to test certain situations outside the production environment (and in some cases also impossible to test inside the production environment due to availability or safety considerations).

138 IT-Grundschutz Catalogues, Federal Office for Information Security (BSI)

139 Like in the case of a disgruntled employee releasing large amounts of sewage in Australia in 2001. See Marshall Abrams, Joe Weiss: „Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia", http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf. Retrieved 2013-03-22.

- It may not be possible to patch certain vulnerabilities thus creating the need for additional measures to mitigate effects.

It is therefore advisable to create a separate patch management process – separate from existing ICT patch management processes.

- **Increase perimeter security**

  A complete physical and logical separation of ICS networks is in many cases neither achievable nor desirable. Successful perimeter protection has to take into account that:

  - An air gap does not amount to complete protection. Several classes of malware have crossed airgaps by using USB media (W32.SillyFDC, W32/Agent.BTZ, W32. Downadup, and W32.Stuxnet).[140]

  - Many of the known exploits target IACS by hopping in the enterprise network. The initial attack vector is often email,[141] then using ERP & MES systems or engineering workstations as a jump-point to the production network.

As a result, good perimeter control is paramount. The foundation for this is:

- Strict network separation between production networks and the enterprise network.[142]

- Separation is achieved by using separate DMZ and perimeter networks.

- Functional integration is mediated via controlled gateways that proxy the information flow. Gateways need to be monitored thoroughly.

- **Manage connectivity and introduce a cellular concept (zones and conduits)**

  This concept is extended by ISO 62443 to create fine cells or zones. According to IEC 62433, zones are "based on functionality, location, responsible organization, and the results of the high-level risk assessment. The grouping of these assets shall reflect common security requirements for each zone and conduit."

  Such a zone might include a group of Process Controllers (PLCs) operating on a common process, while the MES (Manufacturing Execution System) uses its own zone.

  A conduit is the connection between two (or more) zones. It may be as simple as a firewall, but it may also include its own complete DMZ along with an application gateway, or it may be the proverbial USB stick to transfer data.

  Each zone then gets its own overall security goals and a target security level. Security levels are a way to qualitatively express the security needed for that zone. Security levels (and actual consequences) need to be defined by the asset owner.[143]

140 With new variants of this malware class being constantly discovered: Duqu, Flame, Mahdi, Gauss, many of which use USB for spreading. See „Gauss, evidence of ongoing cyber-war and cyber espionage campaigns". By Paganini, August 10th, 2012, http://securityaffairs.co/wordpress/8037/intelligence/gauss-evidence-of-ongoing-cyber-war-and-cyber-espionage-campaigns.html. Retrieved 2013-03-21.

141 See for example the "Night Dragon" series of attack starting in 2009: "Global Energy Cyberattacks: 'Night Dragon'". By McAfee Foundstone Professional Services and McAfee Labs. February 10, 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf. Retrieved 2013-03-22. Or the more recent, "DHS: Gas pipeline industry under significant ongoing cyberattack. ICS-CERT takes unusual step of issuing public warning to raise awareness". By Ellen Messmer, Network World, May 08, 2012, http://www.networkworld.com/news/2012/050812-pipeline-cyberattack-259069.html. Retrieved 2013-03-22.

142 In 2012, Qatar natural gas company RasGas had to isolate their company network from the internet to prevent further damage of its internal infrastructure in a virus attack: „RasGas: new cyber attack against an energy company". By Paganini, Security Affairs, August 31st, 2012. http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html. Retrieved 2013-03-22.

143 IEC 62443 Draft so far only gives general security levels such as "high", "medium" and "low".

4.5 Raising Awareness

In terms of security awareness, there is still a great discrepancy between the actual potential threat of targeted attacks and how they are perceived. This is mainly due to the fact that most attacks that take place in the areas of energy supply and industry are not made public, since the operators of affected installations have no desire to make these incidents known.[144] This approach creates a situation (incidents are perceived as isolated events) that strengthens this tendency to keeping incidents secret. Industry in some countries is asked, encouraged, and sometimes obligated to report these incidents.

Attacks on industrial control systems have become such an important topic in the hacker community since 2010 that relevant conferences devote entire tracks to the subject (e.g. Blackhat SCADA and ICS track). Since then, interest in the topic has grown, as the following examples show:

- In September 2012 ReVuln.com sold vulnerabilities for 9 ICS systems without informing the manufacturer of the vulnerabilities. ReVuln is a start-up company that also sells vulnerabilities for attack purposes.

- Special search engines already exist (ERIPP, SHODAN) for locating SCADA systems that are connected to the Internet. The majority of the systems located this way are obviously unintentionally connected to the Internet.[145]

Based on findings on incidents, action is needed to raise awareness of the evolving risk situation among those in charge of this area, particularly in the IACS field. This could be advanced best by:

- Exchanging information about actual incidents in their own industry segment[147]

- Developing (and implementing) awareness programs on security problems in the IACS and non-nuclear critical energy infrastructure fields

4.6 Sharing Information

An exchange of information among governments, organizations and companies not only contributes to the overall awareness of security issues, it is also a primary way of getting a picture of the current threat situation.[148]

In most cases, targeted attacks do not occur without warning. It can be assumed that terrorist attacks on critical infrastructure will not be confined to a single target. A similar tendency can be perceived in the field of "classic" industrial espionage: cyber attacks in this area are carried out as campaigns.

TrendMicro produced one of the first detailed reports about a campaign of this kind when it examined the distribution of a specific family of malware ("Lurid" download).[149]

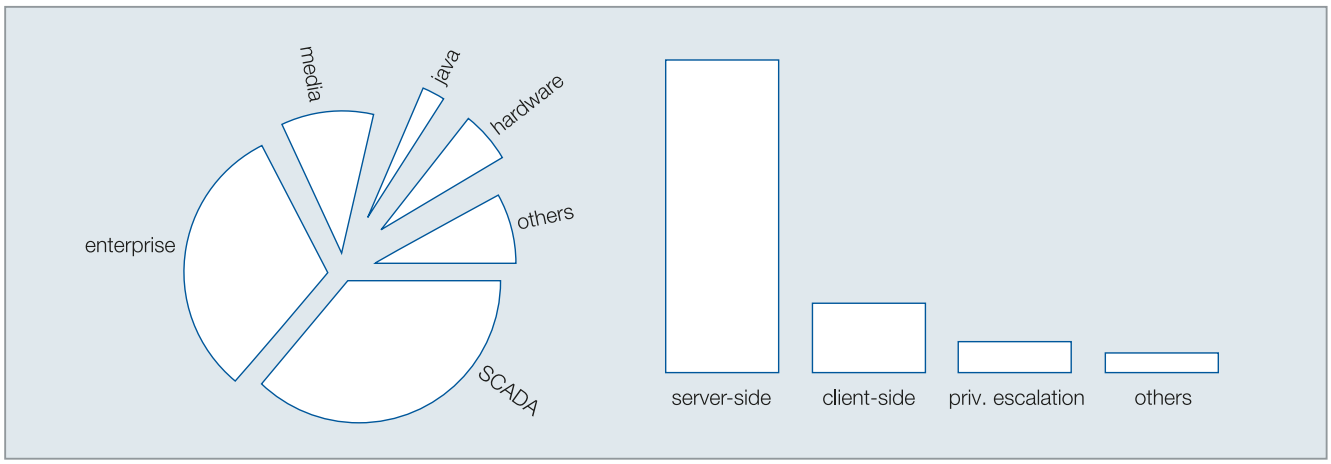


Figure 12: ReVuln Vulnerabilities on Offer[146]

144 A reason for that may be companies fearing the loss of their reputation in securing business activities. Another reason may be the prevention of sensitive information sharing since it may lead to additional vulnerabilities.

145 ICS-ALERT-12-046-01—INCREASING THREAT TO INDUSTRIAL CONTROL SYSTEMS http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-046-01.pdf (02/14/2013)

146 ReVuln, URL: http://revuln.com/ (02/13/2013)

147 The „Night Dragon" attacks mentioned above targeted many global oil, energy, and petrochemical companies. Ibid.

148 See chapter 5.3

149 TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf (02/14/2013)

The attack targeted high-profile diplomatic organizations as well as agencies linked to space and research institutions. Figure 13 shows a selection of the biggest single campaigns using their own malware. Altogether, 301 sub campaigns were identified and a total of 2,272 systems were affected.

A study by Kaspersky on the Red October campaign against diplomatic targets produced very similar findings.[151] The target groups were too small in each case to be discovered quickly or to set off cross-sector reactions. Rapid exchange of information within a sector can give a decisive advantage.

Basic techniques must also be tested on real targets. These can be secondary targets and do not necessarily need to be part of critical infrastructure. Ideally, attacks would already be detected at this stage. Achieving this requires a prompt exchange of a large amount of information, meaning that potentially confidential and incident-related information would be exchanged, including:

- Information about cyber attacks while they are happening
- Information about vulnerabilities discovered and components attacked

Campain	Count	Countries
strong	668	All 68 of the compromised counters were in Vietnam
ejun0708	63	5 in Russia, 3 in Ukraine and 1 each in Czech Republic, Kazakhstan, Sitzerland, Tajikistan and Belarus
ejun0614	42	27 in Russia, 3 in China, 3 in Kyrgyzstan, 2 in Tajikistan and 1 each in UK, US, S. Korea, Czech Republic, Pakistan, Germany and Kazakhstan
strongNewDns	34	All 34 of compromised counters were in Vietnam
ejun0509	32	31 in Russia, 1 in Ukraine
ejun0511	29	21 in Russia, 4 in Ukraine, 2 in Kazakhstan, and 1 each in Czech Republic and Azerbaijan
7–28	28	24 in Vietnam and 1 each in UAE, Cambodia, Thailand and China
ejun0503	25	23 in Russia and 1 each in Ukraine and Czech Republic
0dayaug12.exe	22	20 in Belarus and 2 in Kazakhstan
C:\\WINDOWS\ system32\desp.exe	22	12 in US, 5 in Russia, 3 in The Netherlands and 1 each in Switzerland and the European Union

Figure 13: Lurid Report Examples of the Scope of Malware Campaigns[150]

150 TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf (02/14/2013)

151 Securelist, URL: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (02/14/2013)

Figure 14: European National/Governmental CERTs (ENISA)

- Information about access paths

- The national CERTs are currently the main starting point for information exchange in this context. Most European countries already have a CERT,[152] and ENISA is attempting to establish a unified standard for national CERTs.[153]

➥ Figure 14: European National/Governmental CERTs (ENISA)[154]

Information exchange of this kind offers distinct advantages when it takes place within a peer group (energy industry, critical infrastructure). For example, peers and stakeholders can work together to develop indicators of possible perpetrators and attacks, compatible best practices, and targeted countermeasures. Yet there are obstacles to this type of information exchange. A particular problem arises with cross-border communication. The time delay of information exchange at government and expert meetings is usually too long. Direct incident-related communication among national CERTs in this field is not yet adequately co-ordinated. There is room for improvement in this area. This topic is addressed in more detail in chapter 5.3.

152 Securelist, URL: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (02/14/2013)

153 Deployment of Baseline Capabilities of National/Governmental CERTs, URL: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012 (02/14/2013)

154 Deployment of Baseline Capabilities of National/Governmental CERTs, URL: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012 (02/14/2013)

4.7 Monitoring Security and Managing Incidents

The proper monitoring and management of security incidents require a variety of different aspects which go beyond the mere detection of and reaction to such incidents. Further steps should be considered, including – but not limited to – incorporating cyber attacks in recovery planning, re-examining regulations and addressing ICT trends.

4.7.1 Detecting Security Incidents

No security measure in the world can completely eliminate the risk from a dedicated cyber attacker. Software-based systems have bugs, and some bugs translate to security vulnerabilities. So the likelihood of an attacker finding an exploitable vulnerability in a given system only depends on the time the attacker has access to it. In other words, with time there will be an exploitable vulnerability in any system. Once an attacker gains access, it also takes time to cause damage.

If the attacker is detected before he can cause damage and you react, no damage will be done. Simply put, if the reaction time is faster than the time needed for an attacker to cause damage, the systems are secure. In ICT security this concept is known as Time Based Security (TBS).[155] This relationship holds true for all cyber attacks, especially on critical infrastructure and in the energy sector, where damage is more palpable.[156]

Above all, this shows the paramount importance of security monitoring – without detection, no security measure can guarantee an acceptable level of security, no matter how much it costs. Security monitoring has been neglected in the past, especially in industrial automation and control contexts, where process and availability monitoring has typically been much more important.

While process and availability monitoring is concerned with the status of a system, security monitoring registers events that may help to identify security breaches, such as:

- Failed and successful logins
- Connection attempts to services
- Abnormal sensor readings
- Attempts to communicate outside security boundaries (e.g. cross-cell communication)
- Error situations that did not lead to availability or integrity problems

Many organizations have adapted security monitoring systems under different names, with the most common term being security information and event management (SIEM). Centralized or semi-centralized systems are used in order to be able to:

- Aggregate and correlate data from different sources
  - To help identify distributed attacks or probings
  - To help identify anomalies by using independent sensor systems
- Alert personnel when the automated analysis of aggregated events shows anomalies or signs of security breaches
- Store tamper-proof logs from compromised systems that may be used later in forensic investigations

4.7.2 Reacting to Incidents

Once an incident is detected, there needs to be a way to react. Incident Response (IR) is a part of classical information security standards and should be designed to:

- Identify an ongoing attack (security incident)
- Contain the incident (stop or mitigate the attack)
- Investigate underlying vulnerabilities (e.g. by forensic investigation)
- Eradicate the root causes of the incident
- Share the information learned (e.g. with the national CERT)

155 First published in 1999 as "Time Based Security"

156 See the serious „Shamoon" malware attack on Saudi Aramco energy company: „Saudi Aramco, are we ready for an escalation of cyber attacks?" By Paganini, Security Affairs August 21st, 2012 http://securityaffairs.co/wordpress/8175/hacking/saudi-aramco-are-we-ready-for-an-escalation-of-cyber-attacks.html, Retrieved 2013-03-22.

Incident Response processes are modeled as part of Business Continuity Management and several standards (most notably ISO 22301 – Business Continuity Management, ISO 62443, NISTIR 7628, and NERC CIP).

Interdisciplinary experts or expert teams that are capable of analyzing problems at the point where IACS and ICT systems meet are crucial for analyzing incidents in non-nuclear critical energy infrastructure. Training, exercises, and the availability of qualified personnel are key areas determining the success of incident response.

Since such experts are rare, and smaller organizations may not be able to maintain enough qualified personnel internally, it is important to obtain external help beforehand. While some CERTs supply these services, energy-specific assistance is still missing.[157] For example, this gap can be addressed with knowledge transfer and training for IT/ICS engineers and other relevant personnel.

4.7.3 Considering Cyber Attacks in Recovery Planning

Recovery planning for outages and damage is very advanced in the energy sector. Disaster recovery plans are mandatory for many organizations. Recovery planning is already a standard feature in all standards and includes the following steps:

- Establish recovery plans and prepare actions
- Keep backups and redundant systems
- Exercise recovery plans and test restore procedures

These steps do not change for targeted cyber attacks, but one crucial element does need to be added: When outages occur as a result of an ongoing cyber attack, standard recovery scenarios are likely to result in the same attack happening again, as long as the root cause is not eliminated.

Root cause analysis has only been part of ISO 22301 (Business Continuity Management)[158] since 2012. And NERC CIP-009-5 only mentions it indirectly when it calls for the preservation of data to enable an analysis of the cause of the events that triggered the recovery.

4.7.4 Re-examining Regulations

The practice of controlling individual systems and processes and monitoring them within the boundaries of a single location or company is proving to be too limited in light of the increasing complexity of infrastructure and growing numbers of participants. It is becoming more and more difficult to relate the outages that occur to the fundamental issues, particularly in relation to smart grid infrastructure.

End-to-end monitoring of the entire transmission path from producer to consumer makes it possible to identify and connect faults and their causes across systems. This is the only method that enables the detection of certain types of manipulative attacks (e.g., sabotage).

However, exchanging this data, especially across national borders, quickly leads to legal issues with respect to privacy and data protection. Here there is a need for the complex international legal material to be reworked, including explicit regulations stating requirements in relation to the energy industry. This is particularly desirable for the politically sensitive realm of final consumer privacy.[159]

4.8 Addressing ICT Trends

To steer increasing global energy consumption more efficiently, the electricity grid is being transformed into a digital infrastructure. This is currently understood to be the best way to cope with many of the challenges of the future. Digitizing the grid, however, brings new risks that must be countered by appropriate new security measures. Security measures implemented in smart meters, for example, improve them by making them more efficient and guaranteeing better continuity of service.[160] Inadequate security in the energy sector can have direct consequences for other sectors, such as endangering public safety.

157 According to ENISA, there are no CERTs specializing in the energy sector

158 According to ENISA, there are no CERTs specializing in the energy sector

159 See chapter 5.4

160 IBM: End-to-End security for smart grids (2011)

Smart Meter

A smart meter is an energy meter (e.g. for electricity or gas) that shows actual energy consumption and the actual time of use to the final consumer. The European Smart Metering Alliance (ESMA) says that meters can only be categorized as smart if they are controlled by at least one microprocessor. Depending on the model, smart meters communicate their data automatically to the energy supplier. This procedure and the related processes, system solutions, and services are summed up as smart metering.

Progress is being made in implementing security measures in all critical infrastructure sectors. Measures include security technologies, security policies, encryption, authentication, and network connectivity. However, the application of new security measures to new threats and vulnerabilities is only progressing slowly.[161] For the McAfee study in 2011, the 200 supervisors in critical infrastructure areas were asked to state which security measures were used in their companies. In order to make the answers more easily comparable, those surveyed were asked to select the measures used in their companies from a list of possible security measures:[162]

- Software maintenance and security patches
- Standardized desktop configuration
- Sharing information with industry/ government partners
- Threat-monitoring service subscription
- Bans or restrictions on USB devices or other removable media
- IT network authentication with shared secrets, tokens, or biometric identifiers
- Offsite IT network authentication with shared secrets, tokens, or biometric identifiers
- Firewalls to public networks
- Network access control measures
- Database-specific security and access controls
- Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
- Firewalls between corporate systems
- Security information management tools
- Data loss prevention tools
- Role and activity anomaly detection (Anomaly Detection Systems, ADS)
- Application whitelisting
- Tools to monitor network activity
- Encryption use (in online transmission, data stored in the network, laptop hard drives, databases, emails, and portable mechanisms)
- Regulation of mobile devices (anti-virus software, reflash, not attached to the network)
- Monitoring of new IT network connections through audits or network behavior analysis tools

A comparison between the sectors Water/Sewage, Oil/ Gas and Energy showed that the energy sector had done little to develop security measures from 2009 to 2010 – but overall it was still more advanced than the other two sectors.

161 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 14

162 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 14

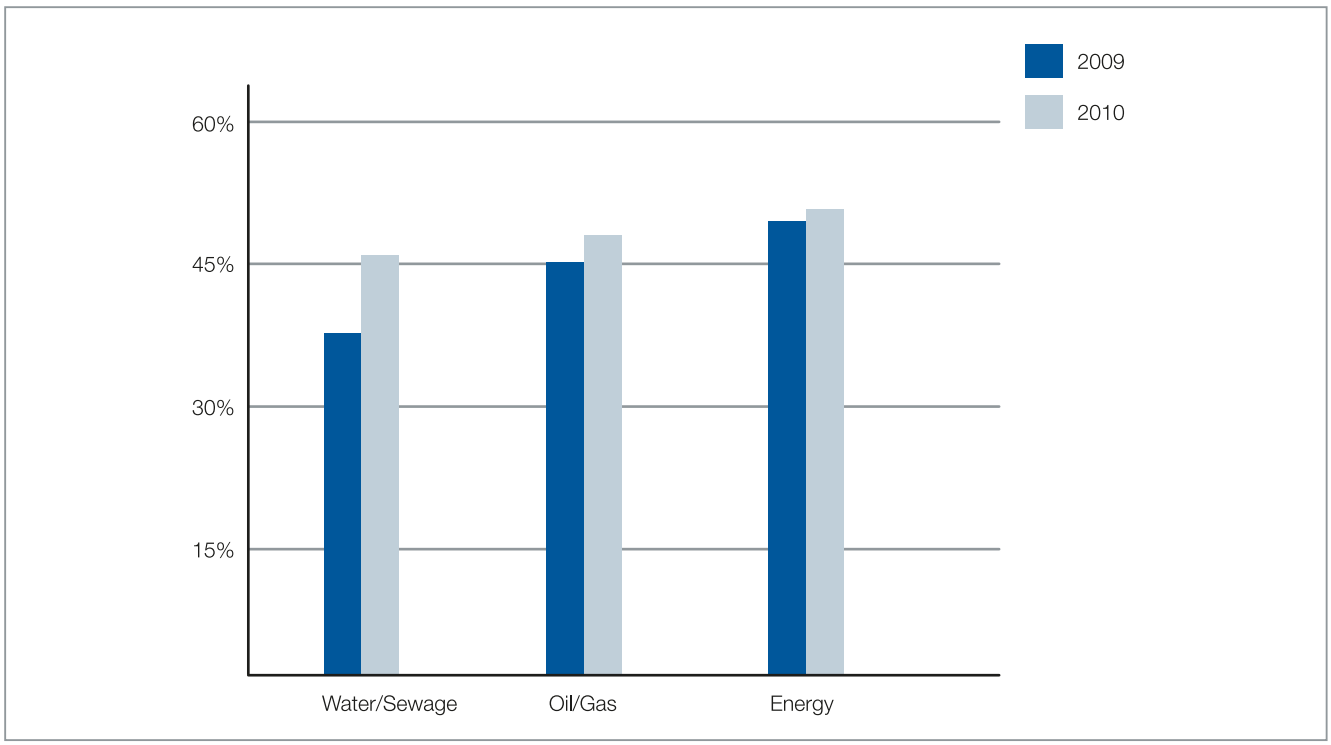


Figure 15: Measuring Improvement: Security Measure Adoption Rates[163]

Only a small number had installed more advanced security measures, such as tools to monitor network activity or detect role anomalies.[164] Yet these are precisely the measures that should be implemented in all sectors of critical infrastructure in view of the current threats and vulnerabilities.

The country comparison shows that China has a rate of implementation of almost 60 percent for these measures, followed by Italy and Japan.

➥ Figure 16: Reported Security Measure Adoption Rates by Country[165]

4.9 Summary and Recommendations

Organizational security measures are already well covered by international standards, although they must continue to evolve just as the threats and vulnerabilities evolve. However, these information security standards are not designed to meet the needs of non-nuclear critical energy infrastructure, which faces varied threats including, terrorist attacks on the non-nuclear critical energy infrastructure's cyber systems. As a result, every organization and operator still has to find its own way of: 1) dealing with security risks; and 2) adapting the general standards to its own specific requirements. Standards for implementing technological security measures in the field of industrial automation and control are already at an advanced stage of development. However, the areas of energy and other critical infrastructure are not yet completely covered. Further action is needed in this area, as well as a more integrated view of physical and cyber security for critical infrastructure.

Risk needs to be understood with an appreciation for the peculiarities in security practices found in the ICT and Industrial Control System (ICS) realms. ICT and ICS security practitioners need to formulate policies to address risks and threats and those policies must be approved by management. The bottom line is that time and effort must be dedicated to developing integrated ICT/ICS cyber security training for ICT, cyber security and engineering designers and specialists.

The technical security measures relating to ICT systems must be enhanced considerably in order to counter current and future smart grid security risks.[166]

163 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 14

164 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 15

165 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 15

166 WP 2.2 Inclusion of effective security measures for smart grid security and resilience, European Commission (2012)

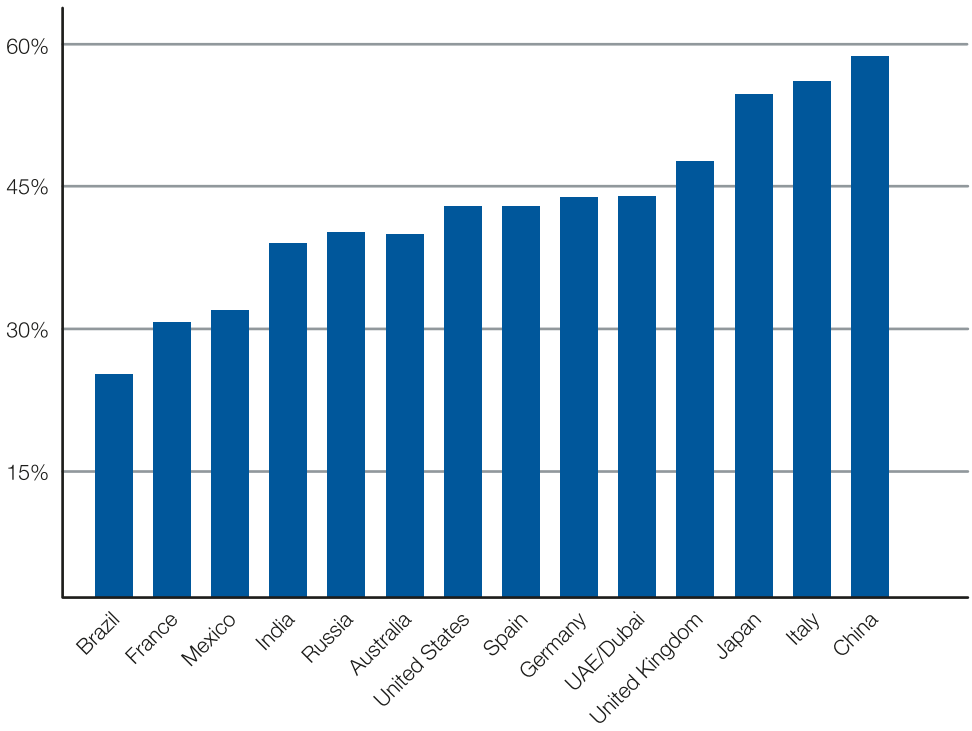


Figure 16: Reported Security Measure Adoption Rates by Country

The central recommendations for industry players based on existing good practices are:

- Raise awareness and build a culture of security.
- Develop training programs for engineers and designers that include an understanding of the cyber security aspects of ICT and ICS.
- Adapt a risk-based security management framework.
  - Assess and monitor risks as they evolve; keep track of changing threats, vulnerabilities, and infrastructure.
  - Apply security measures to mitigate these risks.
  - Implement continuous improvement.
- Share information about vulnerabilities and incidents.
- Monitor security and manage incidents.

It should be noted that the constant, fast pace cyber security itself as well as energy/IACS related standards requires some kind of framework to be flexible and capable of change.

- Public bodies and (national) authorities should:
- Raise awareness and build a culture of security.
- Support information exchange about attacks, attackers, and vulnerabilities in critical infrastructure through Public-Private Partnerships for information exchange.
- Improve the regulatory framework regarding:
  - Mandatory information exchange and privacy
  - Mandatory cyber security standards for non-nuclear critical energy infrastructure and critical infrastructure
  - Help push cyber security standards acceptance for IACS
- Provide guidance regarding applicable standards and regulations.

Detailed policy recommendations for public bodies are discussed in the next chapter.

5.
Good Practices in CIP within the OSCE

Organization for Security and Co-operation in Europe

5. Good Practices in CIP within the OSCE

Energy security, defined as the safe, affordable, and sustainable provision of energy[167], has become a strategic concern for all nations. Energy security is impossible without safe and secure energy infrastructure. Yet as the preceding chapters have clearly shown, today's energy infrastructure is generally speaking, vulnerable. Most risks to energy infrastructure are universal in nature, but their impacts on different critical infrastructure sectors is very specific. Thus, there is a need for a unifying and comprehensive CIP framework that provides the basis for general and specific action to safeguard infrastructure components and critical processes in different critical infrastructure sectors. The main purposes of an overall CIP framework are:

- To bring together relevant public and private stakeholders
- To advance co-operation on the co-ordination, harmonization, and possibly the integration of joint and individual goals, strategies, processes, structures, capabilities, and capacities in different areas of action
- To advance the safety and security of critical infrastructure and critical processes.[168]

Most OSCE participating States have adopted overall CIP frameworks by developing national CIP strategies. Many countries have also published national cyber security strategies in order to address the dangers emanating from cyberspace (see Chapter 4.2). These strategies provide an umbrella to advance co-operation among many different stakeholders. Although the precise structure and content of these strategies is a matter of national policymaking, several generic building blocks can still be identified. By designing national CIP frameworks around these building blocks, national policymakers, as well as infrastructure owners and operators can provide enough commonality for joint action while at the same time ensuring adequate leeway for individual action within each critical infrastructure sector. The remainder of this handbook will, therefore, focus on six building blocks:

- Partnerships,
- Threat and vulnerability analyzes,
- Information exchange,
- Regulatory incentives and dialogue between regulatory oversight bodies,
- Business Continuity Management; and
- Exercises.

5.1 Partnerships

Today there is broad consensus that co-operative approaches are needed to co-ordinate and advance CIP. As a consequence, calls for Public-Private-Partnerships (PPP) have become the mantra of the CIP community. PPPs build on the basic premise that active participation of public and private stakeholders will help establish safety and security guidelines that are appropriate for identified risks and necessary levels of preparedness. In addition, PPPs hold the promise of avoiding regulation by way of legislation, thus providing an incentive for the corporate sector to engage with the public sector.

However, the need for partnerships to protect critical infrastructure goes beyond public-private interaction. Two additional co-operative avenues are required as well:

- Public-Public Partnerships describe the need for cross-government co-operation. Broad interagency interaction is indispensable to advance CIP as different authorities set norms, rules, and standards that guide safety and security in different critical infrastructure sectors. In some cases, public

167 In 2006, the European Commission outlined three main objectives for Europe's energy policy: sustainability, competitiveness, and security of supply. See: A European Strategy for Sustainable, Competitive and Secure Energy, COM(2006) 105 final, Brussels, March 8, 2006, pp. 17-18.

168 Based on: Heiko Borchert and Karina Forster, "Protecting Critical Energy Infrastructures: How to Advance Public-Private Security Cooperation", in Protecting Critical Energy Infrastructure from Terrorist Attack, OSCE CTN Newsletter Special Bulletin, January 2010, pp. 14-17, here p. 14.

authorities tend to follow diverging agendas when it comes to CIP. Some of them adhere to the power of market forces, whereas others are strong believers in the government's legislative role. These differences, however, can become serious stumbling blocks for co-operation when engaging with the private sector. This has several implications, as will be discussed later on.

- Private-Private Partnerships are the corporate sector's answer to cross-organizational co-operation. Dependencies between different critical infrastructure sectors are a key and well-recognized feature of CIP. This requires new collaborative approaches along corporate supply chains within and across different critical infrastructure sectors. This is far from easy, since it means that companies competing with each other must co-operate when exchanging sensitive information. Some critical infrastructure sectors that have become early victims of cyber villains have recognized the benefit of co-operation in a competitive environment. Others are still learning about the importance of co-operation and have been shielded from attacks. As a result, a great deal of care and attention is needed to set up proper roles and expectations for Public-Private Partnerships.

Public-Private Partnership

Public-Private Partnerships (PPPs) are contractual co-operation between public authorities and private-law organizations. PPPs aim to share work and promote collaboration between private partners and public authorities, so that the private partner takes on the responsibility for providing the most efficient service while the public authority ensures that the goals being pursued are in the public interest. Public authorities anticipate that a partnership with the private economy will relieve pressure on public budgets because the private company must provide some or all of the funds itself, which means it will strive to ensure that the projects are cost-effective.

For example, the U.S. Department of Homeland Security recognizes the importance of building effective Public-Private Partnerships in their National Infrastructure Protection Plan (NIPP). The NIPP Partnership Framework enables co-ordination and collaboration between private sector owners and operators and governments at all levels. This is accomplished through the establishment of Sector Co-ordinating Councils (SCCs), consisting of private industry, and Government Co-ordinating Councils (GCCs), comprised of representatives across various levels of government. SCC and GCC functions include comprehensive planning, methodology development, risk assessment, protective programs and resiliency strategies, incident management, training, exercises, and identification of research and development requirements.

While this approach to building partnerships has produced positive results for the U.S. Department of Homeland Security, there is no "one size fits all" model for establishing CIP partnerships. However, experience suggests that each stakeholder follows specific interests. By identifying and leveraging their common interests, a mutually beneficial environment for co-operation can be created (Figure 17). The following steps seem to be worth considering when doing so:

- Step 1: Analyze and identify the motivation of each partner to be included in CIP partnerships in order to clarify mutual expectations and contributions.

- Step 2: Define ambitions and goals of CIP partnerships based on overall national CIP goals; clarify the purpose of CIP partnerships and the tasks to be accomplished (see also step 5).

- Step 3: Screen the existing regulatory framework relevant for each critical infrastructure sector; identify mandatory and self-binding norms, rules and principles; assess the adequacy of the existing regulatory framework in view of expected risks and existing preparedness levels; discuss how to close possible gaps.

- Step 4: Provide mechanisms, protections, and legal certainty for the exchange CIP-related information among all stakeholders involved (see Section 5.3).[169] And provide mechanisms for voluntary efforts, including the development and exchange of best practices, consultation, and dialogue to ensure ongoing and effective partnering.

- Step 5: Set up an institutional structure that fosters cross-organizational co-operation and information exchange; clarify the roles and contributions of each partner (e.g., government agencies, owners and operators of critical

169 The best way to assure legal certainty very much depends on the existing national regulatory framework. In addition to passing legislation, stakeholders might also want to consider self-binding rules.

infrastructure, product suppliers, associations); identify single points of contact for each partner; establish guidelines for co-operation.

- Step 6: Start small by focusing on one or two critical infrastructure sectors; grow steadily while building on the readiness of all stakeholders to co-operate and consider threat levels.[170]

- Step 7: Define critical milestones to review what has been achieved and identify potential next steps.

- Step 8: Provide for a constant review process to revisit and update partnerships to ensure continual progress commensurate with the overall risk landscape and the safety and security measures that are needed to provide an optimal level of protection.

➥ Figure 17: Characteristics of Cyber-related Public-Private Partnerships[171]

5.2 Threat and Vulnerability Analyzes

Threat and vulnerability analyzes are a key instrument to link public and private provisions for safety and security. Joint situational awareness and joint situational understanding regarding key risks and likely consequences for different critical infrastructure sectors is paramount. If public and private actors fail to agree at this point, co-operation will be challenging. Because perceptions matter, joint threat and vulnerability analyzes across all critical infrastructure sectors are perfect enablers to advance mutual understanding of what needs to be tackled, why, and how. In particular, joint threat and vulnerability analyzes promote awareness for critical dependencies between different sectors and thus shed light on an important aspect of national and corporate resilience.

There can be no single unifying structure for conducting risk and vulnerability analyzes that fits the national framework of each OSCE participating State. There are too many differences, in particular with regard to the division of power and responsibility (e.g. centralized vs. decentralized political systems, federal division of power). Despite these differences, however, several good practices can be identified across the OSCE community:

- Single set of risk categories: In the Netherlands and in the United Kingdom, a national security strategy process drives the identification of national security risks. These risks also include specific critical infrastructure relevant scenarios. By integrating critical infrastructure into overall national security policymaking, they are creating a unified framework. Both countries identify a set of illustrative risk categories at the national level. These categories are used as common ground for risk analyzes at sub-national levels as well. This guarantees a consistent set of risk categories that can be used to establish risk profiles at every level of the national political system.[172]

- Methodological guidance: The Swiss Federal Office for Civil Protection, which co-ordinates Switzerland's CIP activities, has invested major efforts into defining sound methods for CIP-related risk analyzes. The following aspects are particularly noteworthy. First, with "Risiken Schweiz" (Risks for Switzerland), a unifying platform was established that serves as an instrument to identify national security risks with the help of different stakeholders. Second, a National Risk Catalogue provides a generic overview of key risks thereby differentiating between natural, technical a, and societal risk categories. Based on this catalogue, ideal-type risk scenarios have been elaborated that provide additional background information. All relevant stakeholders can use these scenarios. Third, national experts have devised a toolbox for national security risk assessment. The toolbox consists of four categories of consequences (e.g., impact on people, environment, economy, and society) and a universal definition of different scales to assess a scenario's likelihood and probability. Finally, a guideline to identify national critical infrastructure elements and objects has been published as well.[173] Within this overall framework, federal authorities now interact with cantonal authorities to advance risk analyzes at the sub-national level.[174] Most importantly, all of these initiatives were set up with the help of private sector experts.

170 Experience suggests that dealing with actual threats is a key driver of co-operation.

171 Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (Washington, DC: Intelligence and National Security Alliance, 2009), p. 6.

172 Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (Washington, DC: Intelligence and National Security Alliance, 2009), p. 6.

173 Schweizerische Eidgenossenschaft, URL: http://www.infraprotection.ch (02/13/2013)

174 Schweizerische Eidgenossenschaft, URL: http://www.kataplan.ch (02/13/2013)

		Interests	Capabilities	Limitations
Telecommunications companies, Software and Hardware Suppliers and Internet Service Providers (ISPs)		Want to deliver services and protect the privacy of costumers Want to be reliable suppliers: optimal performance is just as important as permanent availability, perhaps more so Must be assured that regulation will not stifle development and disadvantage them in economic competition	Have specialized technicians able to identify abnormal activity quickly Are well-positioned to block 'downstream' attacks Are well-placed to distribute security software to their customers and enforce standards through connection agreements with subscribers	Are reticent to involve themselves too deeply in security-related info-sharing due to privacy and liability issues Would likely be unwilling to incur higher costs for security
Government in role of regulator		Want reliability and protection to ensure critical infrastructure protection Depends on the integrity and protection of internet transactions to protect the privacy of citizens and the economic well being of the country	Can provide a necessary legal enforcement role for cyber security Can also provide a platform for international action and outreach Can provide incentives to encourage greater participation in cyber security P3	Have difficulty co-ordinating response across large bodies Have fractured and diffuse authority Are hindered in ability to share information by classification processes Security provision may conflict in some cases with private concerns
Users: large corporations, small businesses, individuals, Information Sharing and Analysis Centers (ISAC), government and private organizations and academia	Individuals	Want accessibility on demand Need greater protection of personally identifiable information and personal computers Are suspicious of government role on the internet and would require strict rules and strong oversight for regulators	Have large numbers of machines that could possibly be used to voluntarily collect and distribute information regarding potential or actual attacks	Are often at risk of cyber security incidents Are untrained and unaccustomed to guarding against attacks
	Government	Depends on availability of the internet to provide public services, communicate, store and access vast amounts of information and to support national security operations	Have large networks that are already tracked for threat information, a useful dataset for threat analysis	Adopt newer, safer technology slowly Do not co-ordinate responses well
	Businesses (small businesses fall in closer with individual users)	Want accessibility on demad Have a strong interest in secure networks to advance e-business and safeguard communications and protect proprietary and competitive data Must be assured regulation will not adversely effect business and innovation	Often have sophisticated security organizations or contract out to security providers Share information throught industry trade associations, standards organizations and government liaisons Participate in the development of standards	Adopt new technology and practices more slowly as the size of the institution increases Have limited participation in info sharing due to privacy and liability concerns

Figure 17: Characteristics of Cyber-related Public-Private Partnerships

- Cross-border issues: In a globalized world, supply chains cross different nations thus prompting the need for multinational co-operation on CIP. In order to address their shared challenges, Canada and the United States, to name but one example, adopted a bilateral action plan in 2010. In particular, the plan will "identify concrete deliverables to support joint infrastructure objectives and enhance engagement." In so doing, the Action Plan sets out three objectives: Building partnerships for infrastructure resilience, improving information sharing, and advancing risk management. In terms of risk analysis, the Action Plan foresees the setup of a "virtual Canada-U.S. Critical Infrastructure Risk Analysis Cell (…) to share infrastructure risk-informed analysis, vulnerability assessments, and prioritization methodologies, processes, and best practices. It also envisions developing and production of collaborative analytic products with cross-border applicability."[175] In order to conduct assessments on critical infrastructure that support threat and vulnerability analysis, the Action Plan also established a cross-border Regional Resiliency Assessment Program (RRAP). The cross-border RRAP examines all-hazard threats, vulnerabilities, and consequences associated with critical infrastructure of mutual interest to the U.S. and Canada. Conducting assessments of this infrastructure enables all stakeholders to identify resilience, dependencies, interdependencies and cascading effects involved with potential failure or disruption of critical infrastructure. The combination of the Virtual Risk Analysis Cell (VRAC) and RRAP allows the U.S. and Canada to assess threat and vulnerability while providing a vehicle for exchanging information and best practices.

5.3 Information Exchange

Information exchange is the lifeline of CIP. As joint situational awareness and joint situational understanding must be guaranteed at all times, the smooth, reliable, and regular exchange of information among all actors involved is critical for the success of CIP. Information sharing falls into three broad categories, which should be integrated into a comprehensive approach:

- Public-public information sharing pertains to the flow of information between different public authorities at various levels of a government. Public-public information sharing is a prerequisite for unified government action vis-à-vis the private sector.

- Public-private information sharing deals with information exchange between public and private stakeholders. It is of vital importance because in most OSCE participating States, private companies own and operate most of the critical infrastructure.

- Private-private information sharing is indispensable as supply chains cut across different companies operating in various infrastructure sectors and industry segments. This illustrates the need for private-private information sharing within and across critical infrastructure sectors.

For all of these information flows, proper governance principles and structures need to be established. Again, the specifics of different critical infrastructure sectors and existing regulatory frameworks will define the major design principles for a CIP-related information exchange architecture. That said, four key questions should be answered:[176]

- **Why?** Information sharing is an everyday task Therefore it should be seamlessly integrated into all elements of a country's CIP strategy. In the best cases, information sharing will be an integral part of the following key CIP tasks:

  - Strategy Definition: Setting up a national CIP strategy requires broad public-private interaction. This enables information to flow between both sectors to help advance mutual understanding of each stakeholder's ambitions, goals, contributions, and constraints. Information exchange for strategy definition will help frame the big picture to address those issues that are key to national and corporate preparedness and resilience.

175 Canada-United States Action Plan for Critical Infrastructure (Washington, DC/ Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (02/13/2013)

176 Canada-United States Action Plan for Critical Infrastructure (Washington, DC/ Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (02/13/2013) Final Report and Recommendations (Washington, DC: National Infrastructure Advisory Council, 2012); Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (Washington, DC: Department of Homeland Security, 2012)

- Threat and vulnerability analyzes: Public and private perceptions of risks, threats, and vulnerabilities as well as mitigating strategies sometimes differ, so information exchange on risks and vulnerabilities is indispensable. When it comes to sharing risk-related information, trust is key. However, nurturing an environment that fosters trust is anything but easy. Experience from different OSCE participating States shows that risk-related information exchange works best when small, agile groups kick off the process, which can later be broadened in terms of the actors to be involved and issues to be addressed.

- Identification of Critical Assets and Definition of Protection Goals: In addition to national critical assets, there are assets that are critical to corporate supply chains and individual companies. Information exchange can help promote awareness of the criticality of these components. The level of protection deemed necessary for national critical infrastructure defines what kind of safety and security measures need to be adopted. While governments may set the necessary protection goals, they are usually no longer in charge of running the actual infrastructure. Consequently, information exchange is indispensable to making sure that safety and security goals are appropriate to the overall risk assessment and for corporate preparedness.

- Crisis Prevention, Crisis Management, Post-Crisis Reconstitution: When it comes to preventing CI-related incidents and handling their consequences, information exchange is a prerequisite. Without mutual information about each partner's level of preparedness, individual points of contact, emergency procedures, and emergency capabilities, planning for the worst will be impossible. Here, real-time information sharing will be crucial, in particular when dealing with cyber-related incidents. This will lead to specific information security requirements that need to be taken into account when designing information-sharing principles and protocols.

- Supporting Activities: There are many activities that can support national CIP initiatives. Among them, research and development as well as standardization play a key role. Both directly tap into the corporate sector's ability to provide safety and security capabilities to address critical infrastructure-related risks and vulnerabilities. Taking these supporting activities into account will broaden the CIP agenda. This makes sense as national preparedness must be seen in light with other policy goals such as national prosperity and national innovation. Setting up an institutional framework that allows for ongoing dialogue among public and private experts on these issues will ensure that activities in different policy fields can be related, consistent, and where appropriate, harmonized. This is important in order to provide a national security science, technology, and industry base that is ready to support CIP.

- **What?** What kind of information should be shared very much depends on the task to be supported and the actors involved. In general, information can be incident-related or non-incident-related. This distinction is useful as it helps differentiate whether: (1) the recipient is expected to take immediate action, and if there is a need; (2) for real-time information exchange; and (3) specific information security provisions. All three aspects are relevant for incident-related information, thus driving the design of very specific exchange mechanisms that focus on swift and seamless interaction among many different stakeholders.

  Non-incident related information, by contrast, can refer to general insights about threats, vulnerabilities, and risks, long-term development trends within and across different critical infrastructure sectors, general security foresight information, long-term regulatory policy issues, and best-practice exchange. This information can be shared more or less freely and without specific time considerations, thus lifting the burden for specific information exchange requirements.

  Preparing for terrorist cyber activity targeting the energy sector will require very specific information. Such details are beyond the scope of this handbook, but generic considerations are summarized in Table 9.

Public Sector Information	Private Sector Information
• Insights about cyber capabilities of key terrorist organizations • Information about linkages between different terrorist and non-terrorist groups • Insights about past attack vectors • Insights on possible future attack vectors deduced from analyzes of cybercriminal underground websites	• Information about major asset categories in the energy sector (e.g., gas, oil, electricity, renewables data; reliability indicators; information from energy trade exchanges) • Technical vulnerability information for specific hardware and software products used by energy infrastructure operators • Anonymized information about the impact of past attacks • Insights on recovery needs to deal with different forms of attacks • Insights from attack patterns in other critical infrastructure sectors that could serve as early warning indicators for the energy sector

Table 9: Public-Private Information Exchange to Address Terrorist Cyber Risks in the Energy Sector

- **How?** In order for information to move smoothly among national CIP stakeholders, key rules and organizing principles need to be established. Several OSCE participating States have set up dedicated organizations and/or initiatives to promote public-private information exchanges.

- The institutional footprint of these solutions varies according to national preferences. In almost every case, participants have agreed on a set of key rules and principles that guide information exchange. Central to these rules and principles is the color-coding of information by those willing to share insights with others, i.e., the supplier of information determines its use by others. In most cases, access to information is restricted to public authorities, members of sector-specific information exchanges, members of information exchanges established in other critical infrastructure sectors, and a combination of all three categories, for example. CIP-related information is sensitive information. Thus there are countries that have adopted specific guidelines to share CIP-related information and avoid unauthorized access to this information. Canada, for example, has adopted a guideline that amends the country's Access to Information Act and stipulates what information should be considered confidential.[177]

  Information exchange guidelines also include rules of behavior that need to be respected by individual experts participating in the sharing of information (e.g., attendance of meetings). In addition, there are selection criteria for the admission of new experts (e.g., incumbents must agree to admit new members, background screening, personal interviews with public authorities managing information exchanges). In most countries, information exchanges started as sector-specific initiatives. As these exchanges matured, cross-sector issues were increasingly addressed. Information security and SCADA security, for example, are of importance to several critical infrastructure sectors and thus tend to be organized as cross-sector information exchange. In addition to face-to-face meetings, online platforms support the electronic exchange of information.

177 "Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada", URL: https://www.publicsafety.gc.ca/prg/ns/ci/lbl-snstv-info-eng.aspx (02/12/2013)

Campain	Organization	Website
European Union	Critical Infrastructure Warning Information Network	https://ciwin.europa.eu
Germany	Allianz für Cybersicherheit (Cyber security Alliance)	https://www.allianz-fuer-cybersicherheit.de/
Switzerland	MELANI (Reporting and Analysis Center for Information Assurance)	http://www.melani.admin.ch/
Spain	National Center for the Protection of Critical Infrastructure	http://www.cnpic-es.es/en/index.html
Netherlands	CPNI.NL	http://www.cpni.nl
United Kingdom	Centre for the Protection of National Infrastructure	http://www.cpni.gov.uk
United States	Information Sharing Environment	http://www.ise.gov
	National Infrastructure Co-ordinating Center	http://www.dhs.gov/national-infrastructure-coordinating-center
Others	Multi-State Information Sharing & Analysis Center	http://msisac.cisecurity.org
	Information Technology Information Sharing & Analysis Center (IT-ISAC)	https://www.it-isac.org
	Electricity Sector Information Sharing Analysis Center (ES-ISAC)	http://www.esisac.com/

Table 10: Selected CIP-related Information Exchange Platforms in OSCE participating States

- **With Whom?** Selecting the right experts to join information exchanges is probably the trickiest part. This is not only a question of quantity but also quality:
  - In terms of quantity many information exchanges started small in order to remain agile and develop a basic level of trust. There is no general rule on the maximum number of participants. What is important, however, is a very low turnover in terms of replacements, i.e. the composition of the group should remain stable in order to nurture trust.
  - In terms of quality, experience from different countries suggests that the level of seniority within the representing organization is important to implement action that might be required as a result of information exchange. Expertise and experience are additional factors considered important to members of information exchanges. In some countries, members of information exchanges have also deliberately excluded certain experts. Members of the law enforcement community, for example, are not part of information exchanges in certain countries as revealing certain types of information would require them to initiate action that might be detrimental to the willingness of participants to share information at all. Still other countries at least provide linkages to the law enforcement community.

5.4 Regulatory Incentives and Regulatory Dialogue

Incentives can shape behavior to achieve a desired outcome. Positive and negative incentives (e.g., sanctions) are part of the regulatory framework in many different policy areas. Over the past couple of years, energy policy in many OSCE participating States was subject to regulatory incentives in order to stimulate the use of renewable energy. So far, incentives have rarely been used to stimulate safety and security-relevant behavior.

Given the reluctance to use positive incentives in the security domain, there are hardly any examples that could be used as best practices. One rare example is the 2007 Pitt review that analyzed lessons to be learned from the 2007 summer flooding in the United Kingdom. In his report, Sir Michael Pitt argued that striving for economic efficiency and effectiveness might have come at the cost of resilience in particular to low probability, high consequence events such as floods. He argued that "regulators should be given an explicit duty to take resilience into account." By discussing and approving resilience-related plans of critical infrastructure operators and subsequently agreeing to the capital and operating expenditure needed to implement these plans, economic regulators could provide positive incentives for companies to invest in resilience.[178]

Pitt's suggestion referred to those industries that are subject to price approval by an economic regulator. Apart from those industries, positive market-oriented incentives include tax breaks, modifications of company valuations and changes in liability law. U.S. Senator Lieberman, for example, suggested that owners and operators of ICT infrastructure could be exempt from civil liabilities related to cyber incidents if they meet specific conditions such as full compliance with security measures to be certified by a third party.[179]

Negative incentives (e.g., sanctions) are more common, including for safety and security-related goals. In Germany, for example, the Federal Agency for Electricity, Gas, Telecommunications, Postal and Railway Markets (Bundesnetzagentur) can impose sanctions against telecommunications operators that violate Germany's telecommunication law (e.g., fines, supervision).[180]

Incentives, however, only work if intended goals can be accomplished. Thus there is a need to monitor stakeholder compliance. Germany and France require energy infrastructure operators to submit safety and security concepts that must also address IT security issues. The implementation of these requirements is subject to inspections by the respective public watchdogs.[181] This provides a monitoring mechanism. Governments interested in providing CIP-related regulatory incentives are well-advised to establish compliance-oriented dialogue among public and private stakeholders:

- On the public side, governments need to bring on board all public agencies with responsibility for CIP-relevant regulation. In most cases these agencies will partner with the Ministries of Energy, Transport, Infrastructure, Health, and Economy. Traditionally, these Ministries have been tasked to provide a general framework for the relevant critical infrastructure sectors. Ministries of the Interior (or those Ministries tasked with CIP), by contrast, are latecomers when it comes to CIP-related regulation. Thus there is a basic need to establish an inclusive public regulatory dialogue in order to come to terms with the complex interplay between vertical, sector-specific regulations put in place in the past and horizontal regulation taking into account the broad principles of CIP. This is especially true for information security regulation that cuts across all critical infrastructure sectors.

- Public-private regulatory dialogue is needed as well. In many OSCE participating States technical standards and national laws for critical infrastructure sectors go hand in hand. Most laws do not directly stipulate safety and security goals but rather refer to technical standards and guidelines. This provides for political leeway: Standards evolve, and as they mature, changes might be needed. While the general provisions of the respective laws remain in place, underlying standards and guidelines can be adopted.

178 Learning lessons from the 2007 floods. The Pitt Review (London: Cabinet Office, 2008), para 16.1-16.46, URL: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf (03/12/2013), http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf (03/12/2013))

179 SEC. 105(e), p. 2105, Cyber Security Act of 2012, (03/12/2013). Lieberman's Cyber Security Act was not adopted by the U.S. Congress.

180 Telekommunikationsgesetz (TKG) §115, June 22, 2004, URL: http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf (03/12/2013)

181 Telekommunikationsgesetz (TKG) §109; Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, no. 6600/SGCN/PSE/PPS of September 26, 2008, p. 26–31, URL: http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1338.pdf (03/12/2013)

However, as the technological complexities grow and critical infrastructure sectors become ever more intertwined, there is a need for cross-sector dialogue on norms, standards, and guidelines. This dialogue must inform the public-private regulatory dialogue in order to identify whether changes in one sector will prompt the need for action in other critical infrastructure sectors as well.

5.5 Business Continuity Management

CIP and Business Continuity Management (BCM) are two sides of the same coin. CIP looks at preparedness and resilience from a national perspective thus focusing on the overall readiness of a nation to cope with incidents that can have destabilizing effects. BCM does the same from a corporate perspective, thereby putting a major emphasis on the provision of those processes and resources that are key to achieve business objectives. Given the complementarity of CIP and BCM, several OSCE participating States are looking at opportunities to bring together both strands. Switzerland can be seen as a showpiece in this regard.

Under the leadership of the Federal Office for National Economic Supply (FONES), several risk analyzes for different critical infrastructure sectors have been conducted. In 2011 the most recent risk analysis for ICT in the electricity sector was updated. The analysis provides a generic description of the sector's structure and its key processes, identifies and assesses six critical risks, and provides suggestions to mitigate these risks. Among the six critical risks, the breakdown of the primary network management system, critical applications, and the blackout of Swissgrid's[182] data center are discussed. Swiss power utilities and VSE, the sector's leading association, were involved in conducting the sector-specific analysis.

Based on the analysis and with support by FONES, VSE and Swiss power utilities started to work on a sector-wide ICT Continuity guideline for the electricity sector,[183] which was published in 2011. The guideline takes recourse to the preceding risk analysis and contains generic recommendations on minimum standards for ICT Continuity Management in the electricity sector along with specific implementation recommendations. These specific recommendations focus on five critical infrastructure components: network management system, critical applications for network management, data center, telecommunications, and control and communication systems.[184] For the time being, the new ICT Continuity guideline for the electricity sector is voluntary, not mandatory. VSE has already started to offer training courses on how to handle the guideline in practice. Thus it can be expected to influence operators' activities in the future.

Close interaction between FONES, VSE and Swiss power utilities was key in agreeing on the new ICT Continuity guideline. Collaboration between these stakeholders and the Swiss Office for Civil Protection was also instrumental in harmonizing different methods that were used by the two lead agencies. As a result, Switzerland's new national CIP strategy provides a general framework for BCM to plug in.[185]

5.6 Exercises

Regular exercises and tests ensure that personnel become confident in handling and acting on material. They increase their ability to respond and their confidence in what they are doing. Exercises and tests also help identify further vulnerabilities, because in crisis situations people tend to become stressed and react hastily and without thinking, and most of all, wrongly and irrationally.[186]

ENISA,[187] NATO,[188] and the individual OSCE participating States[189] conduct regular cyber security exercises. Depending on the focus of the exercise, individual critical infrastructure operators can take part in order to train and improve their emergency and crisis management. Besides being a chance to practice together, these exercises provide an opportunity to discuss good practices and background information.

182 Swissgrid is the owner and operator of the Swiss transmission grid.

183 The guideline covers the national transmission grid and pan-regional distribution grids as well as the respective transformation levels. Regional and local distribution grids are not covered.

184 ICT Continuity. Handlungsempfehlungen zur Sicherstellung der Versorgung (Aarau: Verband Schweizerischer Elektrizitätsunternehmen, 2011), URL: http://www.strom.ch/uploads/media/VSE_ICT-Continuity_12-2011_D_01.pdf (03/12/2013)

185 Nationale Strategie zum Schutz kritischer Infrastrukturen, (2012), URL: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsys-related1.82246.downloadList.57269.DownloadFile.tmp/strategieski2012d.pdf (02/12/2013)

186 BSI-Standard 100-4, p. 83ff

187 Exercises under the heading Cyber Europe. Cf. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe (02/13/2013)

188 Exercises under the heading Cyber Coalition and Cyber Atlantic

189 E.g. the LÜKEX in the Federal Republic of Germany, cf. URL: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Infos_ueber_Luekex.html (02/13/2013)

Exercises on this scale[190] require months or even years of preparation and must therefore be planned for the long term. This presents a problem for critical infrastructure operators because they do not usually make long-term plans in such detail. A solution to this dilemma could be an exercise plan covering several years that would include operators' own tests and exercises, as well as the national and international exercises. For government actors this would mean that their planning must be binding in terms of timing and content. Last minute changes to the schedule, content or exercise objectives could result in some or all critical infrastructure operators not taking part. To cover the broadest possible scope of exercises without placing too many demands on participants, a staggered exercise program is recommended. This might mean that in the first exercise year, one critical infrastructure sector conducts exercises with the state. In the following years the sectors rotate, and every 5 or 10 years all of the sectors conduct exercises with the state as a group. If the participants use a Key Performance Indicator (KPI) system for the exercises, improvements and deteriorations in crisis management can be identified. Due to the diversity of participants and scenarios, these KPIs should be kept as general as possible, e.g., measuring reaction times.

The exercises should always be followed by an evaluation. The evaluation should address successes and deficits clearly. It should not sidestep shortcomings or else participants might be lulled into a false sense of security, believing that they are fully prepared for an attack, for instance. This misleading impression can have negative consequences for the entire critical infrastructure and the country if an attack ever does occur on the critical infrastructure or another area and the agreed methods and processes do not work.

5.7 Summary and Recommendations

CIP must address different challenges. While not comprehensive, safety and security provisions for critical infrastructure and processes were set long before CIP was established as a policy field. Second, the risk landscape is constantly evolving. To respond to this, safety and security standards, concepts and measures must be dynamic. Third, risks to any nation's critical infrastructure can emanate far beyond national borders, thereby international co-operation in CIP underscores the importance of international co-operation. Finally, the real burden for CIP rests mainly on the shoulders of the private sector, which owns and operates most critical infrastructure worldwide. Thus there is a serious need for close public-private interaction and also trust based on clearly defined roles and responsibilities.

- Comprehensive CIP frameworks are needed to deal with all of these challenges. These frameworks must be tailored to the specific requirements of each nation and each critical infrastructure sector. Design flexibility is key, but it must not lead to fragmented CIP approaches because of the universally-recognized value of compatible, risk-based measures, especially in an essential and global sector, such as the energy sector. Instead, there is a need for conceptual building blocks that facilitate joint action and enhance flexibility at the same time. This chapter discussed six building blocks:

- Comprehensive partnerships are needed to set up and advance CIP. These partnerships should be established along three avenues: Public-Public Partnerships to advance interagency interaction in the public sector; Public-Private Partnerships to enable co-operation between ministries, public agencies and private critical energy infrastructure owners and operators; and Private-Private Partnerships to stimulate corporate interaction along supply chains within and across critical infrastructure sectors. There is no "one size fits all" method for establishing these partnerships, but different suggestions can be considered: (1) Clarify mutual expectations and contributions by analyzing and identifying partners' motivations; (2) define ambitions and goals for CIP partnerships; (3) screen the existing regulatory framework; (4) provide legal certainty for the exchange CIP-related information; (5) provide a co-operative institutional structure; (6) start small; (7) define regular review milestones; and (8) revisit and update partnerships to ensure continual progress.

- Risk and vulnerability analyzes are important to advance joint situational awareness and joint situational understanding with regard to CI-relevant risks and vulnerabilities. Good practices to design the respective processes include:

  - The definition of a single set of risk categories and scenarios that can be used across all levels of the national and policymaking system and in each sector

190 In relation to the number of participants and the complexity of the material

- Methodological guidance especially with regard to key metrics in order to avoid assessment outcomes that cannot be compared because they were not harmonized in the beginning

- Dedicated approaches to cross-national risk analysis such as common processes for information exchange and joint risk assessment

- Joint situational awareness and joint situational understanding are impossible without the smooth flow of information among public stakeholders, between public and private actors, and within the private sectors. Designing information exchanges to support CIP requires public and private stakeholders to define what information and why information should be exchanged, what kind of information is needed for the respective tasks, how information could be shared and protected, and who should be involved in information sharing. Among other things, good practices on information sharing suggest that:

  - Information exchanges should start small and build in order to remain agile and nurture trust.

  - Clear rules are needed for information sharing and to establish individual responsibility in handling shared information.

  - Face-to-face meetings can be complemented with electronic information sharing platforms.

  - The task to be accomplished very much drives information security requirements, with incident-related information being fundamentally different from non-incident-related information.

- The responsibility for CIP mainly rests with the private sector. The public sector can stimulate investments in critical infrastructure safety and security by providing targeted incentives. Market-based incentives include, among other things, tax breaks, modifications of company valuations that take into account individual levels of preparedness, and exemptions from civil liabilities. Other important incentives include the government sharing threat information. Good practices also suggest broad engagement especially when regulations are being considered, is needed to identify and analyze the impacts of safety and security norms, standards, and principles across critical infrastructure sectors.

- Building on the idea of stimulating corporate safety and security activities, governments should advance CIP, in part, by using Business Continuity Management (BCM). BCM has become standard practice for many companies. By bringing in line national CIP frameworks with key BCM principles, governments acknowledge corporate preparedness activities. Good practices also suggest that BCM can be used to advance ICT-related continuity management in critical infrastructure sectors, thus advancing national and corporate resilience at the same time. Governments also sometimes do this in their national preparedness programs.

- Exercises are a great way to assess current strengths and weaknesses. By practicing together, public and private stakeholders gain valuable insights about each others' capabilities and constraints. Setting up exercises that provide real value added is demanding. Therefore careful planning is needed with regard to the goals to be accomplished, critical infrastructure sectors to be involved, and risks/attack vectors to be analyzed. Thorough assessments and after action reviews should round off every exercise.

6. Suggestions for Future OSCE Roles to Advance Cyber Security in Non-Nuclear Critical Energy Infrastructure

OSCE Organization for Security and Co-operation in Europe

6. Suggestions for Future OSCE Roles to Advance Cyber Security in Non-Nuclear Critical Energy Infrastructure

Based on Ministerial Council Decision 6/07 dated November 30, 2007, the OSCE participating States have been discussing the organization's role in advancing non-nuclear critical energy infrastructure protection. Several conferences and workshops made it clear that the OSCE can play a valuable and complementary role that supports and strengthens national CIP activities and CIP-relevant programs in other international organizations. Based on these findings,[191] OSCE contributions to address cyber security issues in non-nuclear critical energy infrastructure sectors (and possibly beyond) can be put in three broad categories:

Mobilizing political support

- The OSCE could raise awareness on the threat of cyber-related terrorist activities targeting critical energy infrastructure and other critical infrastructure sectors and the likely consequences of these malicious activities.

- The participating States could explore incorporating considerations relevant to protecting non-nuclear critical energy infrastructure from terrorist attack in other cyber/ICT security-related efforts of the OSCE, when appropriate and feasible.

Promoting co-operation

- The OSCE could foster multilateral exchange of information on methods to assess the costs of cyber risks and the benefits of cyber security provisions, using the energy sector as a reference case.

- The OSCE could serve as a hub to extend the reach of information-sharing activities launched by other organizations (e.g., extend the reach of ENISA to Central Asia via the OSCE).

- The OSCE could promote and facilitate the formation of public-public, public-private, and private-private CIP partnerships by organizing good practices workshops, disseminating information, and compiling good practices manuals and handbooks.

191 See for example: Report of the Secretary General on Opportunities for Co-operation between the OSCE and Relevant International Organizations in the Field of Protection of Critical Energy Infrastructure from Terrorist Attacks, SEC. GAL/202/08, 30 October 2008; Executive Report on the OCEEA-ATU Expert Meeting on Protection Critical Energy Infrastructure from Terrorist Attack, SEC. GAL/153/08, August 29, 2008; Executive Report on the Public-Private Expert Workshop on Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks, Vienna, February 11-12, 2010

Enhancing national capabilities

- By organizing good practices workshops and disseminating information, the OSCE could promote the strengthening of capabilities for key cyber security tasks such as:

    - Detection: Identify malevolent action in cyberspace, advance pattern recognition with regard to future attack vectors, and analyze attacks in other critical infrastructure sectors in view of possible lessons to be learned for energy infrastructure owners and operators.

    - Protection and response: Develop methods and concepts to provide ICT security across critical infrastructure sectors, exchange experience on how to organize cyber incident-related crisis management within and across critical infrastructure sectors.

    - Mitigation: Establish ICT Continuity plans for the energy sector and other critical infrastructure sectors linked with the energy sector.

- The OSCE could facilitate institutional capacity-building to advance cyber security in the energy sector by supporting national interagency co-operation and co-ordination and supporting the creation of cyber-related information exchange structures, mechanisms, and protocols.

- Although many countries do this themselves, the OSCE could stimulate the cross-border exchange of information on emergency planning and capabilities related to cyber incidents in the energy sector and other critical infrastructure sectors linked with the energy sector.

- The OSCE could promote training to advance cyber literacy among key personnel working for critical infrastructure sectors and critical infrastructure watchdogs in the public sector.

- The OSCE could serve as a facilitator to stage cyber-related exercises in co-operation with other international organizations that have a more limited membership or a different geographic focus (e.g., ENISA).

7.
Further Reading

8.
Glossary

9.
Abbreviations

OSCE Organization for Security and Co-operation in Europe

7. Further Reading

1. Speake, Graham: Applying ISA/IEC 62443 to Control Systems, Manufacturing Enterprise Solutions Association, MESA(2012), URL: http://www.yca-yokogawa-usersgroup.com/uploads/3/1/8/5/3185440/mesatutorial_-_isa99_security.pdf

2. Booz & Company for the European Commission: Study: Stock-Taking of existing Critical Infrastructure Protection Activities (2009), URL: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

3. Borchert, Heiko and Karina Forster: Protecting Critical Energy Infrastructures: How to Advance Public-Private Security Cooperation, in Protecting Critical Energy Infrastructure from Terrorist Attack, OSCE CTN Newsletter Special Bulletin (2010), pp. 14-17. URL: http://www.osce.org/atu/41367.

4. Bundesamt für Sicherheit in der Informationstechnik, Dr. Harald Niggemann: Cyber-Sicherheit – Bedrohungslage und Maßnahmen, URL: http://prisma-zentrum.com/download/120904%20Innovation%20B_Vortrag_Folien%20Referent.pdf

5. Bundesministerium des Inneren: Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden (2008), URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf;jsessionid=D97DF90DA95A17955BF369CFED0FF9EE.2_cid287?__blob=publicationFile

6. Bundesrepublik Deutschland: Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz), 24.02.2012, URL: http://www.gesetze-im-internet.de/atg/

7. Bundesrepublik Deutschland: Telekommunikationsgesetz (TKG), 22.06.2004, URL: http://www.gesetze-im-internet.de/tkg_2004/

8. Cabinet Office: Learning lessons from the 2007 floods. The Pitt Review (2008), URL: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf

9. Canada-United States Action Plan for Critical Infrastructure (Washington, DC/Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

10. Commission of the European Communities: On a European Programme for Critical Infrastructure Protection (2005), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF

11. Computerworld: Shamoon malware attacks, URL: http://www.computerworld.com/s/article/9230547/Kill_timer_found_in_Shamoon_malware_suggests_possible_connection_to_Saudi_Aramco_attack

12. CSO-Online: Cyberattacks on natural gas pipeline companies, URL: http://blogs.csoonline.com/critical-infrastructure/2165/ics-cert-alert-natural-gas-pipelines-under-attack

13. European Commission: A European Strategy for Sustainable, Competitive and Secure Energy (2006), URL: http://europa.eu/documents/comm/green_papers/pdf/com2006_105_en.pdf

14. European Commission: Critical Energy Infrastructure Protection (2008), URL: http://ec.europa.eu/energy/infrastructure/critical_en.htm

15. European Commission: Cyber security in the Digital Agenda (2012), URL: http://ec.europa.eu/digital-agenda/en/cybersecurity

16. European Commission: European Programme for Critical Infrastructure Protection (2006), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

17. European Commission: Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common

level of network and information security across the Union, COM (2013) 48 final (02/07/2013), URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

18. European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf

19. European Commission: Study: Stock-Taking of Existing Critical Infrastructure Protection Activities (2009), URL: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

20. European Commission: Work Package 2.2 – Inclusion of effective security measures for smart grid security and resilience (2012), URL: http://ec.europa.eu/information_society/policy/nis/docs/smartgrid/wp2_2security_measures.pdf

21. European Commission/Harnser Group: A Reference Security Management Plan for Energy Infrastructure (2010), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf

22. European Network and Information Security Agency (ENISA): Good Practice Guide Network Security Information Exchanges (2009), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

23. European Network and Information Security Agency (ENISA): Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012), URL: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

24. European Network and Information Security Agency (ENISA): Incentives and Challenges for Information Sharing in the Context of Network and Information Security (2010), URL: http://www.enisa.europa.eu/media/news-items/enisa-analyses-the-incentives-and-challenges-to-public-2013-private-information-sharing

25. European Network and Information Security Agency (ENISA): National Cyber Security Strategies (2012), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

26. European Network and Information Security Agency (ENISA): Smart Grid Security (2013), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/

27. European Network and Information Security Agency (ENISA): Smart Grid Security – Recommendations for Europe and Member States (2012), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

28. European Network and Information Security Agency (ENISA): Smart Grids Security (2013), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

29. Fred Schreier: On Cyberwarfare, in: DCAF Horizon 2015 Working Paper No. 7 (2012), URL: http://www.dcaf.ch/Publications/On-Cyberwarfar

30. French Premier Ministre: Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, (2008), no. 6600/SGCN/PSE/PPS of September 26, 2008, URL: http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1338.pdf

31. Gabriel Weimann: Cyberterrorism: The Sum of All Fears?, Studies in Conflict & Terrorism (2005), URL: http://dx.doi.org/10.1080/10576100590905110

32. Government of Canada: National Strategy for Critical Infrastructure (2009), URL: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf

33. G8 presidency of the Russian Federation: Official Website of the G8 presidency of the Russian Federation in 2006: Global Energy Security (2006), URL: http://en.g8russia.ru/docs/11.html

34. Homeland Security Project: Cyber Security Task Force: Public-Private Information Sharing (2012), URL: http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf

35. ICS-ALERT-10-301-01A – CONTROL SYSTEM INTERNET ACCESSIBILITY, URL: http://ics-cert.us-cert.gov/pdf/ICS-ALERT-11-343-01A.pdf

36. IEC 62443-2-4: Baseline Security Standard for Industrial Automation Control Systems, URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf

37. ifo Institut für Wirtschaftsforschung e.V.: ifo Schnelldienst 07/2011 (8.4.2011), URL: http://www.cesifo-group.de/de/ifoHome/publications/docbase/details.html?docId=15521107

38. Intelligence and National Security Alliance (INSA): Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (2009), URL: http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

39. Kaspersky: The „Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies, URL: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

40. Kuratorium Sicheres Österreich (KSÖ): Cybersicherheit in Österreich (2012), URL: http://www.kuratorium-sicheres-oesterreich.at/themen/detail-ansicht/thema/cybersicherheit-in-oesterreich/

41. McAfee: In the Crossfire – Critical Infrastructure in the Age of Cyber War (2010), URL: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

42. McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), URL: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

43. Mehmet Nesip Ogun: Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research (2012), URL: http://dx.doi.org/10.1080/19361610.2012.656252

44. Ness, Larry: Terrorism and Public Utility Infrastructure Protection (2008), URL: http://www.ensec.org/index.php?option=com_content&view=article&id=154:terrorismandpublicutility-infrastructureprotection&catid=84:energyinfrastructureprotection&Itemid=324

45. Netherlands: Ministry of the Interior and Kingdom Relations, National Risk Assessment method Guide 2008 (2008).

46. National Infrastructure Advisory Council (NIAC): Intelligence Information Sharing. Final Report and Recommendations (2012), URL: http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

47. Public Safety Canada: Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada, URL: https://www.publicsafety.gc.ca/prg/ns/ci/lbl-snstv-info-eng.aspx

48. Securing America's Future Energy: How Vulnerable Are Energy Facilities to Cyber Attacks? (2010), URL: http://www.secureenergy.org/sites/default/files/1111_SAFEIntelligenceReport3120100120.pdf

49. Sicherheitsforum Baden-Württemberg: SiFo-Studie 2009/2010 – Know-how-Schutz in Baden-Württemberg (2010), URL: http://www.sicherheitsforum-bw.de/index.php?option=com_content&view=article&id=54&Itemid=82

50. Siemens AG: IT-Security in der Prozessautomatisierung mit Siemens SIMATIC PCS: 7 ARC Whitepaper Simatic PCS7, URL: http://www.automation.siemens.com/mcms/process-control-systems/SiteCollectionDocuments/efiles/pcs7/support/marktstudien/ARC_WhitePaper_Siemens_SIMATIC_PCS7_Security_de.pdf

51. Siemens AG: Operational Guidelines für Industrial Security (2011), URL: http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_de.pdf

52. Statistisches Bundesamt: Fachserie 4 Reihe 6.1 Produzierendes Gewerbe (2010), URL: https://www.destatis.de/DE/Publikationen/Thematisch/Energie/Struktur/BeschaeftigungUmsatzKostenstruktur.html

53. T-Systems: Best Practice – Das Kundenmagazin von T-Systems Ausgabe 04/2011 (2011), URL: http://www.t-systems.de/news-media/ausgabe-04-2011/754902

54. Techworld: ReVuln showcases vulnerabilities in SCADA software, but won't report them to vendors - Meldung auf techworld.com, URL: http://news.techworld.com/applications/3412614/revuln-showcases-vulnerabilities-in-scada-software-but-wont-report-them-to-vendors/

55. The National Academies Press (NAP): Terrorism and the Electric Power Delivery System (2012), URL: http://www.nap.edu/openbook.php?record_id=12050&page=1

56. The Smart Grid Interoperability Panel (SGIP): Introduction to NISTIR 7628 – Guidelines for Smart Grid Cyber Security (2010), URL: http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

57. TNO: Good practices manual for CIP policies for policymakers in Europe (2011), URL: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2011-09-21%2010:30:22.0&Taal=2

58. TrendMicro: The „Lurid" Downloader – Report of a targeted malware campaign by TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf

59. U.S. Congress: Cyber Security Act of 2012 (2012), URL: http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf

60. U.S. Department of Energy: A Comparison of Cross-Sector Cyber Security Standards (2005), URL: http://www.inl.gov/scada/publications/d/a_comparison_of_cross-sector_cyber_security_standards.pdf

61. U.S. Department of Homeland Security: A Comparison of Oil and Gas Segment Cyber Security Standards (2004), URL: http://scadahacker.com/library/Documents/Standards/Comparison%20of%20Oil%20and%20Gas%20Segment%20Cyber%20Security%20Standards.pdf

62. U.S. Department of Homeland Security: Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (2012) , URL: http://www.dhs.gov/xlibrary/assets/mgmt/mgmt-classified-national-security-program-implementation-directive.pdf

63. U.S. Department of Homeland Security: Information Sharing Strategy (2008), URL: http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf

64. U.S. Department of Homeland Security: National Infrastructure Protection Plan, NIPP (2012), URL: https://www.dhs.gov/national-infrastructure-protection-plan

65. U.S. Department of Homeland Security: Energy Sector-Specific Plan (2010), URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf;

66. U.S. Department of Homeland Security: Communications Sector-Specific Plan (2010), URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf

67. U.S. Government Accountability Office (GAO-11-117): Electricity Grid Modernization (01/12/2011), URL: http://www.gao.gov/new.items/d11117.pdf

68. Verband Schweizerischer Elektrizitätsunternehmen: ICT Continuity. Handlungsempfehlungen zur Sicherstellung der Versorgung (2011), URL: http://www.strom.ch/uploads/media/VSE_ICT-Continuity_12-2011_D_01.pdf

8. Glossary

Botnet
A botnet is a group of computers that are controlled from a single source and run related software programs and scripts. While botnets can be used for distributed computing purposes, such as scientific processing, the term usually refers to multiple computers that have been infected with malicious software.

Computer worm
A computer worm is a computer program or script that replicates itself once it has been run. Unlike a computer virus, a worm spreads without infecting other data files or boot sectors with its code. Worms spread via networks or removable media such as USB sticks.

Critical Infrastructure (CI)
Those physical resources, services, and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of societies or the effective functioning of States and governments.

Critical Infrastructure Protection (CIP)
The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

Critical Energy Infrastructure Protection (CEIP)
The programs, activities and interactions used by owners and operators to protect their critical energy infrastructure.

(Distributed) Denial-of-Service ((D)DoS)
An attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a (D)DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. One common method of attack involves saturating the target machine with external communications requests to overload the server, so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. In general terms, DoS attacks either force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service.

Industrial Automation and Control Systems
A new designation for ICS systems that includes the automation aspect. New standards tend to reference IACS instead of ICS.

Infrastructure
The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

Man-in-the-middle attack (MITM)
This type of attack is a form of active eavesdropping in which a third party deludes two communications partners by making them believe that they are directly talking to each other. It is usually applied to annul a secure coding (e.g. SSL connections in online banking). In fact both communication partners encrypt their data but in such a way that the man-in-the-middle can read and forward it to the other.

Risk
The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Risk Assessment
A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management
A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Sniffing
The term refers to the monitoring and reading of data (through software or hardware) that flow over computer networks. While commercial sniffers are

used to analyze and maintain networks, there are also sniffers that aim at the interception of data.

Supervisory Control and Data Acquisition (SCADA)
SCADA systems are a type of industrial control system (ICS) – they control and measure physical processes with the help of sensors and PLCs (Programmable Logic Controllers). SCADA is often used synonymously with ICS or IACS for the whole branch of technology dealing with cyber-physical interaction.

Threat
Any event that has the potential to disrupt or destroy critical infrastructure or any element thereof. An all-hazards approach to threats includes accidents, natural hazards, and deliberate attacks.

Threat Assessment
A standardized and reliable method for evaluating threats to infrastructure.

Vulnerability
A characteristic of an element of the critical infrastructure's design, implementation or operation that renders it susceptible to destruction or incapacitation by a threat.

9. Abbreviations

ATU - Action against Terrorism Unit/Transnational Threats Department/OSCE

BCM – Business Continuity Management

BSI – Federal Office for Information Security

CEI – Critical Energy Infrastructure

CERT – Computer Emergency Response Team

CI – Critical Infrastructure

CIIP – Critical Information Infrastructure Protection

CIP – Critical Infrastructure Protection

COBIT - Control Objectives for Information and Related Technology

COTS - Commercial Off-The-Shelf

DB AG – Deutsche Bahn AG

DDoS – Distributed Denial of Service

DoS – Denial of Service

EEX – European Energy Exchange

ENISA – European Network and Information Security Agency

ES-ISAC – Electricity Sector Information Sharing and Analysis Center

ESMA - European Smart Metering Alliance

EU – European Union

FONES - Federal Office for National Economic Supply

ICT – Information and Communication Technology

IEA – International Energy Agency

IEC – International Electrotechnical Commission

IRGC - International Risk Governance Council

ISMS – Information Security Management System

ISO – International Organization for Standardization

ITIL – Information Technology Infrastructure Library

IT-ISAC – Information Sharing and Analysis Center

KPI – Key Performance Indicators

LEA – Law Enforcement Agencies

MELANI – Melde- und Analysestelle Informationssicherung

NATO – North Atlantic Treaty Organization

NCSS – National Cyber Security Strategy

NERC – North American Electric Reliability Corporation

NIPP – National Infrastructure Protection Plan

NIST – National Institute of Standards and Technology

NNCEI – Non Nuclear Critical Energy Infrastructure

PDCA – Plan, Do, Check, Act

PPP/3Ps – Public-Private Partnership

ROE – Return on Equity

SCADA – Supervisory Control and Data Acquisition

UK – United Kingdom

US – United States

USA – United States of America

10. List of Figures and Tables

The Organization for Security and Co-operation in Europe works for stability, prosperity and democracy in 57 States through political dialogue about shared values and through practical work that makes a lasting difference

Organization for Security and Co-operation in Europe
Wallnerstrasse 6
A-1010 Vienna, Austria
Tel.: +43 1 514 360
info@osce.org

OSCE Organization for Security and Co-operation in Europe