ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Novembre

2013

Rapporto tecnico N.48

Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria

Marco Alessi , Hanna Bartoszewicz-Burczy,
Andrés Cortes, Fernando García, Daniela Pestonesi , Tadeusz Włodarczyk

Consiglio Nazionale delle Ricerche

Istituto di Ricerche sull'Impresa e Lo Sviluppo

RAPPORTO TECNICO CNR-CERIS

Anno 8, N° 48; Novembre 2013

Direttore Responsabile

Secondo Rolfo

Direzione e Redazione

CNR-Ceris
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
www.ceris.cnr.it

Sede di Roma

Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano

Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione

Enrico Viarisio
e.viarisio@ceris.cnr.it

Rapporto Tecnico, Anno 8, n.48; Novembre 2013

ESSENCE

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

__E__merging __S__ecurity __S__tandards to the __E__U power __N__etwork controls and other __C__ritical __E__quipment

Partners of the project are:

CNR-Ceris *(Coordinator) (Italy);* Università del Piemonte Orientale Amedeo Avogadro *(Italy);*
Deloitte Advisory S.L. *(Spain);* Antonio Diu Masferrer Nueva Empresa SLNE *(Spain);*
Enel Ingegneria e Ricerca S.p.A. *(Italy);* Abb S.p.A. – Power systhems division *(Italy);*
IEN - Institute of power engineering *(Poland);* PSE – Operator SA *(Poland).*

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

The Commission is not responsible for any use that may be made of the information contained therein, the sole responsibility lies with the authors.

Rapporto Tecnico, Anno 8, n.48; Novembre 2013

Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria.

Marco Alessi [a], Hanna Bartoszewicz-Burczy [b],
Andrés Cortes [c], Fernando García*, Daniela Pestonesi [d], Tadeusz Włodarczyk [e]

*Corresponding author: fgarciagutierrez@deloitte.es
☎ +34 91 514 50 00
Deloitte.
Pza.Pablo Ruiz Picasso, 1,
(28020) Madrid

ABSTRACT: Attack Scenario is a comprehensive report in which are listed current and future threats to the control systems of a power network, such as malicious cyber-attacks, human failure or simultaneous hardware breakdown, in order to establish a rank of them regarding the likelihood of their occurrence and the preparedness of the most frequent used control systems in Europe to handle them.

JEL code: L94

KEYWORDS: cyber security, malicious attack, power control center, hardware breakdown, security standards, power threats, scenarios definition.

[a] ABB SPA-POWER SYSTEMS DIVISION, Via Albareto 35, 16153 Genova, Italy, email: marco.alessi@it.abb.com .

[b] Energy Economic Section Institute of Power Engineering (IEn), Warsaw, Poland, email hanna.burczy@ien.com.pl .

[c] Deloitte Advisory, S.L., Plaza Pablo Ruiz Picasso, 1, Madrid, Spain; email: acortesmarlia@deloitte.es

[d] ENEL, Divisione Ingegneria e Ricerca, Area Tecnica Ricerca, Via Andrea Pisano 120, 56122, PISA, email daniela.pestonesi@enel.com .

[e] Departament Teleinformatyki Sekcja Bezpieczeństwa i Standardów IT Polskie Sieci Elektroenergetyczne Operator S.A., Warszawska 165, 05-520 Konstancin-Jeziorna, email tadeusz.wlodarczyk@pse-operator.pl .

SUMMARY

List of figures

List of tables

1. ESSENCE PROJECT

The Essence project (***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment)* is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.

Networked computers reside at the heart of critical infrastructures, these become then vulnerable to cyber-attacks that can inhibit their operation, corrupt valuable data, or expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, thus, pressure to ensure cyber security of control and communication systems is now very strong worldwide. Frameworks have been developed or are under development at present, but it is difficult to evaluate costs (which can be huge) and benefits of their adoption.

In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardization efforts;

2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;

3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;

4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

2. WHAT'S AN EMERGING SECURITY STANDARD?

Standards are a form of law or regulation that covers from professional conduct to technical interoperability. Standards can be defined in different ways according to the sector. Generally, they are “recommended practices in the manufacturing of products or materials or in the conduct of a business, art, or profession”[1].

A standard can also be “a basis for comparison; a reference point against which other things can be evaluated”[2].

Some standards are set by organisations, which write them in a technically complex way, showing the life cycle driven by some products, services and intellectual property. On the other hand, Standards Development Activities (SDA) are universally accepted as they are believed to be transparent, even though they cannot expose all interests.

Formerly, these policies were set by governments as traditional de jure Standards Setting Activities (SSA) through regulatory agencies. However, nowadays the participation of other agents and stakeholders is thought to be essential to improve quality and completeness of standards. This is why standards are being made by the private sector, as Voluntary Consensus Standards (VCS). Among these private agents, some examples would be consortia of businesses, trade associations and non-profit organisations, along with government agencies and private citizens, who work together as Standard Development Organizations (S.D.O.s). Some of these stakeholders can compete in the market, but they cooperate to develop the standard. It is necessary to show the rewards associated with creating standards to prevent the private sector from believing that they are money and time-wasting activities[3].

Standards are important because of the following reasons:

- They can alter or determine current and future research and development of products.
- They have a considerable impact on life and work.
- They can make easier or hinder the entry of new agents in an industry.
- They can consolidate existing businesses, or encourage them to improve current practices.

In the past, standards were published after the product or practice had been developed and used by the public. However, nowadays standards are developed at the same time products and services are designed, and products cannot be sold until standards are ready to be published.

[1] Glossary, Metropolitan Water District of southern California, http://www.mwdh2o.com/mwdh2o/pages/yourwater/glossary/glossary01.html

[2] WordNet, Cognitive Science Laboratory, Princeton University http://wordnet.princeton.edu/perl/webwn?s=standard

[3] John W. Bagby, professor of Information, Science and Technology of the Pennsylvania State University. *The Emerging Standards War in Cyberspace Security*. http://faculty.ist.psu.edu/bagby/SIG/EmergingCyberspaceSecurityStandardsWar.pdf

Cybersecurity standards are a mix of I.C.T. interoperability and technical standards and professional or behavioural standards. They include standards from financial accounting, financial audit, I.T. audit, information assurance security, systems/network security, telephony/wireless security, intellectual property security and so on.

Standards are deeply studied in the Technical Report Deliverable 1 of Essence project: "Considerations on SCADA Standards", written by Ugo Finardi, Elena Ragazzi and Alberto Stefanini. According to this document, implementing security standards can be a big cost for private companies. Moreover, these costs cannot be evaluated reliably before the implementation of the measures. This implies that medium or small businesses are likely unable to afford implementing standards.

Another problem is that companies can determine the risk of sharing information on critical infrastructure information, but the benefit of implementing cyber security standards is much harder to be evaluated. Besides, the benefit is not only for the company but also for stakeholders involved and society in general, who have not to pay for it.

The only place where the implementation of standards has been carried out is the U.S.A. If Europe tried to develop similar standards, it would be easier as in Europe there are far less companies in the power system sector. Even though the competition is increasing and new small companies are being founded, mostly renewable energies plants, critical infrastructures are still operated by few companies. In many cases, transmission and distribution are controlled by the government, so the costs of implementing standards would be shared between private and public agents.

A problem which can arise in Europe which has not in the U.S.A. is that some companies have voluntarily adopted some security standards. These standards can be very different, and it can be difficult to come to an agreement on a common framework if some companies have already made big investments in security. Frequently, building a totally new security system can be cheaper than upgrading the old system.

In "Considerations on SCADA Standards", seven standards or guidelines have been compared. The NIST 800-53is the only standard which is fully developed and uses a terminology clear enough. If a standard is implemented, the European stakeholders have to be involved in the process.

Finally, this document came to the following conclusions:

- The implementation of a common framework on cyber security must take into account differences in the European power systems: different size, reliability, market structure, role of public agents, national regulations, etc.

- There are different ways to implement a new security standard in Europe: voluntary, voluntary with economic incentives, mandatory in some countries in some critical assets, mandatory in some countries in the entire sector, mandatory in the EU in all sectors, etc. However, the more sectors and countries are involved, the more difficult will be to reach a common standard, because of the lack of a common European authority and different interests. A solution could be implementing different frameworks depending on the sector and country (all standards should respect minimum requirements) to assess different solutions and converge to a common standard in the long term.

- The cost of the implementation of the measures is afforded by the facility owners, while the benefits are shared by the public. On the other hand, voluntary application of standards cannot ensure that they are correctly implemented, as bigger companies can afford it but smaller cannot. This means that the public regulator should share expenditures with the operator, and ensure the correct implementation of the measures.

3. WHY ATTACK SCENARIOS DEFINITION?

The European Union (EU) electric power system is very large and geographically dispersed. It covers the area from Portugal (West) to Poland (East) and from Italy (South) to Finland (North). Physically, the system consists of generation plants: thermal, nuclear, hydro and renewable power plants to produce electricity, transmission and distribution networks including transmission and distribution lines and substations, control centres, communications systems and other infrastructure facilities required to produce electric energy and perform reliable transfer to final consumers. All elements of the electric system have different vulnerability sources, which are potential subjects of disruption or destruction.

Deregulation of European energy system, due to EC Energy Directives, has increased competition in the energy system and according to Third Party Access changed also traditional energy players. Former vertical integrated utilities have been moving to separate entities as: transmission system operators (TSO), distribution operators (DO), independent power producers (IPP), generation operators (GO), market actors, customers, metering providers, and others.

The electric sector has undergone significant reorganization in the last decades, mainly in order to increase competition. Liberalization, privatisation and additionally environmental constraints to the electrical sector, have made electric security system more complex and crucial for the economy in all members countries as well as exacerbated the system vulnerability.

Competitive energy markets, growth in distributed generation with use of renewable energy sources and growing dependence on imported energy, increase the complexity of the operational level of infrastructures which control all necessary processes.

Physically the electric system is composed of power plants and the whole group of components to store fuel, generate electricity, including protection, monitoring and control system and delivering the energy to the grid, power transmission and distribution system and system and market operators. Power flows from generating plants to customers through the transmission and distribution network. Electricity is not economically storable in large amounts, what is produced must be the instant used. The electric power infrastructure is designed to deliver electricity to final users with continuity and quality of supply.[4]

There are several types of generating plants: fossil fuel (coal, oil and gas), nuclear, hydro and renewable distributed generation (wind, solar, geothermal, biomass, biogas). The largest ones are fossil fuel and nuclear plants and they contain fundamental critical assets including facilities necessary to generate electricity (generators, power turbines), control room and substation to deliver energy to the grid.

[4] Structure of Energy Sector Control Centers: Analysis of the Different Levels and Uses of Control Centers in the Energy System (Electricity and Natural Gas), Octavio: Energy System Control Centers Security, an EU Approach, March 2009.

In 2009 year total EU installed generation capacity amounted to 842 GW, in this: 455 GW of fossil fuels fired power plants, (54%), 135 GW of nuclear power (16%), 143 GW of hydro power stations (17%) and 109 GW of renewable power plants (13%).[5]

Total net electricity generation in the EU-27 reached 3000 TWh in 2009 year. In this, electricity generation came from combustible fuels amounted to 1662 TWh (55,4%), and nuclear 834 TWh (27,8%). Electricity generated from hydro and renewable energy sources amounted to 504 TWh what stated 16,8 % of total output.[6]

The transmission system include high-voltage overhead lines and underground cables (110 kV and above), substations, other equipment and installation indispensable for the proper operation, including control centres coordinating operations.

The substation is a high-voltage electric system facility, used to switch generators, equipment, and circuits or lines in and out of a system. It is also used to change AC voltages from one level to another, and/or change alternating current to direct current or direct current to alternating current.[7] The substation consists of: bus bars, circuit breakers, switches, transformers, auxiliary high voltage equipment, auxiliary equipment for control and protection (IEDs), substation SCADA.

The substation SCADA system supports remote or local operator control of substation equipment, such as opening or closing a breaker. The SCADA system provides three critical functions in operation at the substation: data acquisition, supervisory control and alarm display and control.

Bus bars are aluminium or copper conductors supported by insulators that interconnect the transmission lines, transformers, loads or generators, at the same voltage level. This is a static element that only provides a common connexion point to elements connected in the substation at the same level of voltage.

A circuit breaker is a device used to open or close an electric power circuit either during normal power system operation or during abnormal conditions. A circuit breaker serves in the course of normal system operation to energize or de-energize circuits (lines, cables, transformers, generators or loads).

Switches (or isolators) are elements designed to modify the topology in the substation. They can be operated with voltage, but do not have capacity to interrupt any current. Switches may be operated manually, in accordance with decision of an operator, either from the substation control room or by supervisory control from the remote control centre.

Transformers are electromechanical elements that modify voltage level. Besides the transformer losses (around 1 ÷ 3%), energy at both sides of the transformer is the same but at different voltage and current (the higher is the voltage the lower is the current for the same power level).

[5] Power Statistics & Trends 2011Synopsis, Euroelectric: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-EI-12-001/EN/KS-EI-12-001-EN.PDF

[6] http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-EI-12-001/EN/KS-EI-12-001-EN.PDF

The ratio is relation between voltages at both sides. Some transformers are capable to modify their ratio to certain extend without disconnecting the transformer. This capacity is used to help in the network voltage control.

In the substation there is another high voltage equipment with different objectives, mainly for voltage control or measurement. The most common control elements are:

- Reactance: equipment designed to take up reactive power from the network. The effect will be to reduce the voltage level.

- Capacitor: equipment designed to produce reactive current. The effect will be to increase the voltage level.

- Static VAr Compensator (SVC): device for providing fast-acting reactive power compensation on high-voltage electricity transmission networks. SVCs are part of the flexible AC transmission system (FACTS) family of devices. SVCs are used both on bulk power transmission circuits to regulate voltage and contribute to steady-state stability.

- Measurement high voltage elements. In electricity there are only two elements that can be directly measured: voltage and current. With both measures active or reactive power can be calculated. To measure voltage and current the following equipment is used: voltage transformers: connected in parallel, they measure the voltage between an active element and the ground.8

An overhead power line is an electric power transmission line suspended by towers or poles. Since most of insulation is provided by air, overhead power lines are generally the lowest-cost method of transmission of large quantities of electric power. Overhead lines have a specific transmission capacity which depends on wire characteristics and tower design.

Electric power can also be transmitted by underground power cables. This is more expensive option, since the life-cycle cost of an underground power cable is two to four times the cost of an overhead power line.

Compared to overhead lines, underground or underwater cables emit much weaker magnetic fields. Underground cables need a narrower strip of about 1-10 metres to install, whereas the lack of cable insulation requires an overhead line to be installed on a strip of about 20-200 metres wide to be kept permanently clear for safety, maintenance and repair. Those advantages can in some cases justify higher investment cost for underground cables.

Most high-voltage underground cables for power transmission are insulated by a sheath of cross linked polyethylene (XLPE). Some cable may have a lead jacket in conjunction with XLPE insulation to allow fibre optics to be seamlessly integrated within the cable.

[7] Structure of Energy Sector Control Centers: Analysis of the Different Levels and Uses of Control Centers in the Energy System (Electricity and Natural Gas), Octavio: Energy System Control Centers Security, an EU Approach, March 2009.

[8] Structure of Energy Sector Control Centers: Analysis of the Different Levels and Uses of Control Centers in the Energy System (Electricity and Natural Gas), Octavio: Energy System Control Centers Security, an EU Approach, March 2009.

Distribution systems include the same elements as transmission networks but at different voltage levels and with a lower power i.e. below 100 kV, mostly 60 kV, 30 kV, 15 kV and low voltage, substations, other installation for delivering electricity to customers.

All elements of electricity network are controlled by information systems The Supervisory Control and Data Acquisition (SCADA) and Energy Management System (EMS) and DMS (Distribution Management System) are commonly in use for real-time communication and control.

SCADA/EMS (Energy Management System) supervises, controls, optimises and manages generation (load forecast, automatic generation control, monitoring and schedules, economic dispatch, balancing market load and transmission systems functions (such as a dispatcher power flow, contingency analysis, optimal power flow etc).

SCADA/DMS (Distribution Management System) supervises, controls, optimises power distribution networks. Both systems enable utilities to collect, store and analyse data from data points in national or regional networks, perform network modelling, simulate power operation, pinpoint faults, pre-empt outages, and participate in energy trading markets.

The commercial function SCADA/BMS (Business Management System) optimises business services for electricity consumers, supporting short term balancing mechanism, cost control, efficiency etc.

Main responsibility of every country is to guarantee energy security and especially electricity security. Incorrect electricity policy may lead to energy crisis, caused extraordinary social and economic financial losses.

Disrupted or destroyed electric system infrastructures in one member state has a serious impact on security of other member state sometimes causing a large-scale power system outage, and impose direct high economic costs for utility and economy and otherwise social or indirect impacts possibly leading to a threat to life and health of people. Even if attack itself does not result in immediately dramatic impacts to humans, a widespread and long duration outages could lead to significant loss of life because of stress and suffering and other factors.

In recent years the EU Commission has been concerned on the security of the country members infrastructure which is reflecting in EC document: Green Paper “European programme for critical infrastructure protection” (EC 2005), adopted Directive 2008/114/EC from December 2008 year on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and the European Programme for Critical Infrastructure Protection (EPCIP).

3.1. Intentions of potential attacks to the EU power Network controls and other Critical Equipment

There are many definitions, theories and approaches related to terrorism in literature. The most significant development in official definition and statements came after September 11th, 2001 attacks on World Trade Centers and Pentagon in USA.

Following above events an extraordinary session of the European Council took place with the aim of analysing the international situation and setting the fight against terrorism as a priority objective of the European Union.[9]

In 2001 year European Union in adopted documents: “Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism” and “Council Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism” provided the meaning of terrorists act and listed persons, groups and entities involved in the terrorists acts. The Article 1(3) of Common Position 2001/931/CFSP sets out the definitions of terrorists act as ”intentional acts, which, given its nature or its context, may seriously damage a country or an international organization and which are defined as an offence under national law. These include:

- attacks upon a person's life which may cause death;
- attacks upon the physical integrity of a person;
- kidnapping or hostage taking;
- causing extensive destruction to a Government or public facility, a transport system, an
- infrastructure facility;
- seizure of aircraft, ships or other means of public or goods transport;
- manufacture, possession, acquisition, transport, supply or use of weapons, explosives, or of nuclear, biological or chemical weapons,
- release of dangerous substances, or causing fires,
- explosions or floods the effect of which is to endanger human life;
- interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
- participating in the activities of a terrorist group, including supplying information or material resources, or funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the group.” [10]

The organized crime and terrorism have been identified as growing threats for the European security. European Union member countries are both: targets and a base for terrorism.

Logistical bases for Al Qaeda cells have been uncovered in the United Kingdom, Italy, Germany, Spain, Belgium (the European Security Strategy of 12 December 2003)[11].

[9] Defining Terrorism, Transnational terrorism, security and the rule of the low. October 1, 2008, EC project under 6FP.

[10] COUNCIL COMMON POSITION of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP) Official Journal of the European Communities L 344/93, 28.12.2001.

There have been identified different types of terrorists group, in relation to their roots, motives and ideological goals. Main categories are: nationalist-separatists, secular utopians and political-religious.

Nationalist-separatists (e.g. ETA, IRA, Kurdistan Workers Party), usually fight for homeland liberation. Second one are “Secular utopians” - left and right wingers fighting to replace state ideology. Left-wing terrorists (e.g. Marxist-Leninists, Columbia’s FARC and ELN, Maoists, anarchists, Red Brigades, Japanese Red Army) strive to replace capitalists with socialist/communists regime “dictatorship of proletariat”. Right-wind (e.g. skinheads, racist groups, Neo-Nazi, Neo-Fascist) seek to change democratic governments by a dictatorship.

This category also featured can include ecological and anti-globalization movements. Political-religious groups (e.g. al Qaeda, Hezbollah, Hamas, Al-Jihad al-Islami, Harkat-ul-Mujahedeen, Jihad Islamic) fight with all who do not belong to their political and religious factions.[12] Groups based on Islamic fundamentalism are the biggest threat at present. From XXI century numbers of Islamic group is growing. These groups are situated and operate in many countries, e.g. Al Qaeda operates in 60 countries.

List of international terrorist groups developed by EC and by National Counterterrorism Center is in Anex1.

Terrorist organisations constantly recruit people of different nationalities to their ranks, and over last decades a new generation of terrorists is arising, much better trained in information and telecommunications technologies, use violence on much scale and with the potential use of weapons of mass destruction.

Basic motivations for this groups are: action to demonstrate their skills in order to occur in social consciousness, persecution of others, make revenge and retaliation, intimidating actions aimed at a group of people to force the action corresponding to the interests of the terrorists, steps to victory over the opponent, action to destruction of any human community and activities aimed at the destruction of any human population.[13]

Targets selected by terrorist groups depend of their goals, but choice of their attacks in many cases depends on opportunity to achieve high losses of human life with minimal risks to the attackers, as well as, or inflict more damage to governmental institutions and to economy.

Terrorist groups usually are intended to influence an audience and more often attacks concern civilian systems than military targets, which are generally much better protected.

By choosing energy power system as a target, terrorists can relatively easy reach their goals, taking into account the fact that society life depends on electricity. Moreover, the electric power system is linked up with every other civilian infrastructure (transportation, communication, food production, public health) that are able to effectively operate without electricity supply in a short time. Larger power outages may be difficult and time consuming to restore, moreover single point failure in energy system linkage to other critical infrastructure and increase scale of attack.

[11] European Security Strategy of 12 December 2003

[12] P.Toft, A.Duero. A. Bieliauskas: Terrorists targeting and energy security. Institute of Energy, JRC of EC, Petten,.Elsevier 2010

By blowing a substation or transmission lines terrorists could cause cascading failures and damage parts that would take months to repair or replace.

Terrorist groups also often choose as targets the energy transmission infrastructure.

From 139 active nationalist-separatist terrorist groups 22 attacked energy transmission infrastructure (16%), and respectively from 124 secular-utopias 9 groups chose energy infrastructure, and 9 groups from 119 political - religions groups. [14]

Total number of terrorists group attacking energy transmission infrastructure is presented on the next figure.

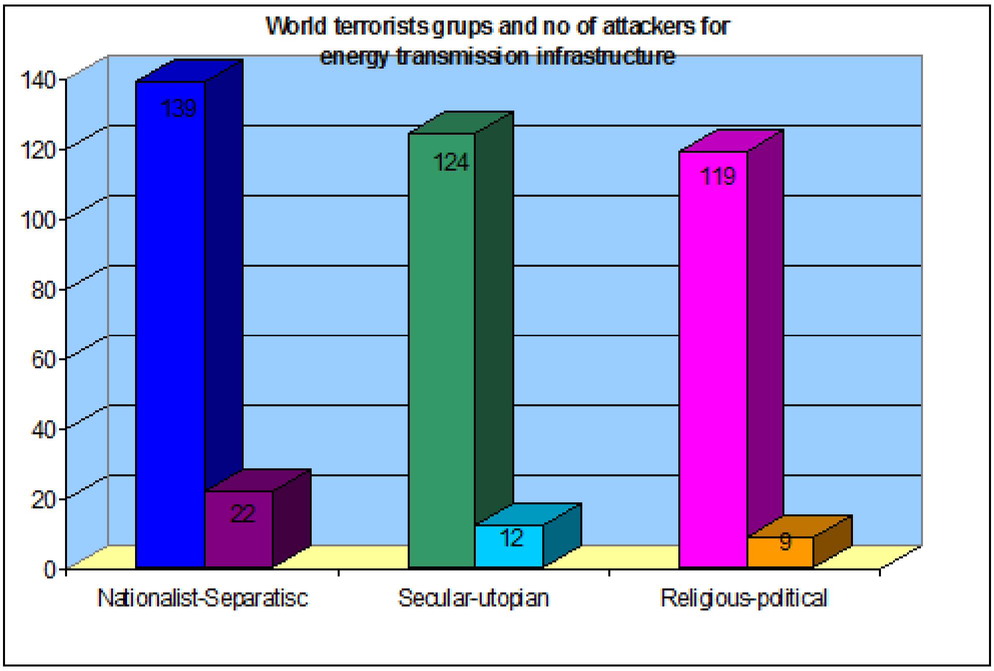

Figure 1: World terrorist groups and number of attackers for energy transmission infrastructure

[13] B. Hołyst, Terroryzm, Lexi-Nexis, Polska 2011.

[14] P.Toft, A.Duero. A. Bieliauskas: Terrorists targeting and energy security. Institute of Energy, JRC of EC, Petten,.Elsevier 2010

According to National Counter Terrorism Center there are several countries such as Iran, Cuba, Sudan, and Syria which sponsored terrorism. Without state sponsors, these groups would have greater difficulty obtaining funds, weapons, materials, and secure areas they require to plan and conduct operations. Altogether, there were 47 international terrorist groups.

In 2001, 3,295 people were killed, while in 2004 6,060 people lost their lives as a result of terrorist attacks. [15].

3.1.1 Internet use by terrorists

Globalization, including easy access to communication, Internet, media, and transportation has enabled larger-scale operations by criminals and terrorists around the world.

Presently Internet becomes a tool increasingly used by terrorists, and allows them to extend their range of worldwide activities. Terrorists use Internet and popular media network to do their campaign of propaganda, psychological operations, as well as, to disseminate false and manipulate information. Using Internet they can promote their own ideology on a global scale to reach the audiences around the world. By using a global network of Internet connections terrorist organizations coordinate their actions with different parts of the world. In addition, compared to the very expensive network security techniques, cost of preparation and implementation of computer attack is irrelevant.

The Internet is also a source of information and has become for terrorists one of the main tools as source of data about objects which potentially can be goals of their attacks.

Terrorists groups can easily use the Internet to gather detailed information on the electric system worldwide, identify the position of weak points of the system (location transformers, cooling system in nuclear power plants, etc.) and select their entrance. The internet: GPS Maps, Google Maps, and others geographic programs, give detailed information on different part of an electric power system. Available satellite data combined with direct observation on the ground allows to trace individual parts of the system and to prepare detailed plans for attacks.

Another advantage of the combat information is negligible risk to the attackers because of the possibility of attacks from long distances. The action can be performed with commercially available terminal located e.g. in the internet cafe, and chances of capturing the perpetrators of the act are slim.

[15] http://www.nctc.gov/site/other/fto.html

3.1.2 The electric system as a potential terrorists target

The electric systems are exposed to cyber and physical threats of different nature. Cyber threats are attacks on control and communication system which may cause SCADA/EMS or other cyber assets failure or malfunction.

The main physical threats are faulty equipment, aging, exploited material used in various processes, random accidents, malfunctioning of an automatic protection system, natural events like storms, floods, fires, hurricanes or earthquakes, or intentional deliberate attacks.

Main difference between natural disaster and deliberate attack to power system is that terrorists select the critical components and the most vulnerable parts of the system and equipment as targets. Great danger is also a high likelihood of an attack with the use of chemical and biological weapons. Often consequences of terrorists attack could be much more dramatic, when a combined cyber attack and a physical attack on several vulnerabilities contribute simultaneously, particularly effected by terrorists with great knowledge of the electric system. Additionally an attack during a period with extreme weather might lead to deaths of many people.

Threats can be incidental or results of malicious behaviour of attackers. Still a lot of threats result from human errors or insufficient understanding of procedures.

Another threat is potential loss of domestic or imported fuel supply as result of political and/or military actions, embargoes, transmission, and transportations problems. Such cases may lead to limitation of energy fuels, not sufficient fuel quality, and as consequence, to further disruptions of the operation of the electricity infrastructure.

Power system by its nature (geographic extent and dynamism) sometimes is not reliable, but is designed to resist a variety of natural disruption and continue to operate. Most of the outages are local and losses are not significant. Large scale power disruption can cause regional or international cascading power failure (blackouts) and affect millions customers.

Examples of blackouts of European power system and their impacts to society in number of affecting people are presented in the following table.

Table 1: blackouts of European power system and their impacts

	Country	Date	Number of affecting people
1.	Denmark	1999	Power to 100 000 customers interrupted
2.	France	1999	Power to 3,6 million customers interrupted
3.	Portugal	2000	Power to 5 million customers interrupted
4.	Denmark	2003	Power to 5 million customers interrupted
5.	England, London	2003	Power to 410 000 customers interrupted
6.	Denmark, Sweden	2003	Power to 5 million customers interrupted
7.	Italy, Austria, France,	2003	Power to 57 million customers interrupted
8.	Slovenia and Switzerland		
9.	Germany, Münsterland	2005	Power to 80 000 customers interrupted
10.	Poland, Szczecin	2008	Power to 500 000 customers interrupted

Sources: Terrorism and the electric power system, NRC, USA, and Structure of Energy Sector Control Centers: Analysis of the Different Levels and Uses of Control Centers in the Energy System (Electricity and Natural Gas), Octavio: Energy System Control Centers Security, an EU Approach, March 2009.

Minutes lost per customer per year in European Union countries in 1999-2007 due to system supply interruptions shows Figure 2.[16]

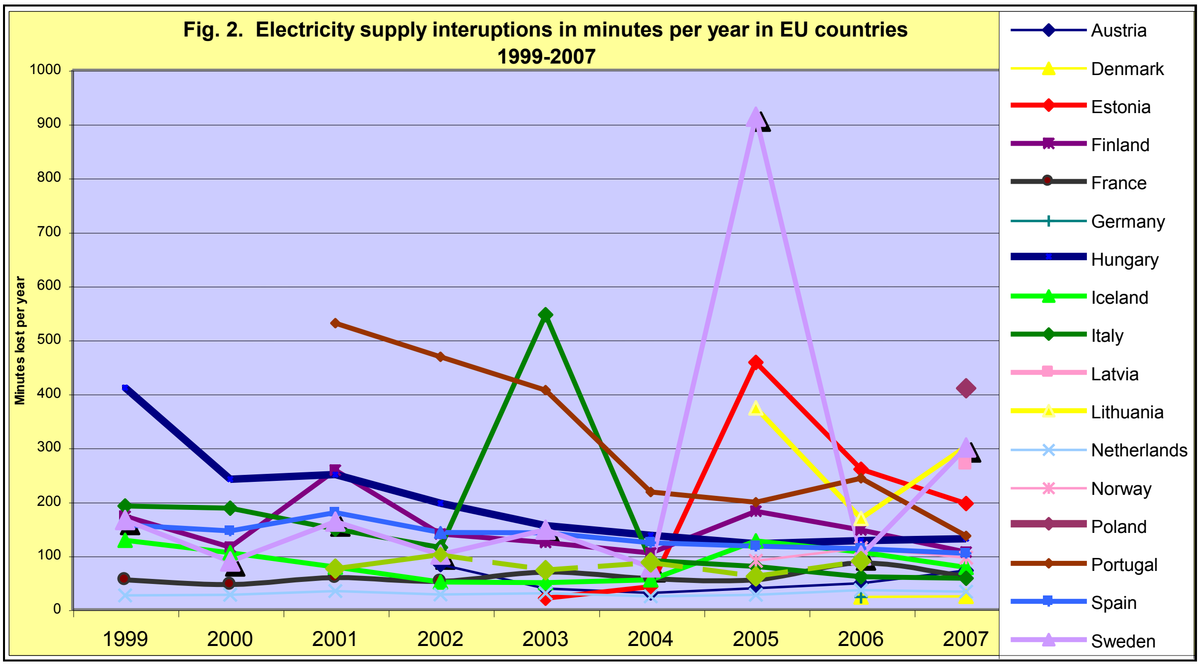

Figure 2: Electricity supply interruptions in minutes per year in EU countries

[16] 4th Benchmarking Report, on Quality of Electricity Supply 2008, Council of the European Energy Regulators, December 2008, pp. 177, (www.energy-regulator.eu))

Power system is an attractive target for terrorists because of its size and imperfections in security and is very vulnerable to attack. System control centers, generators and auxiliary equipment, high voltage substations, large power transmission lines and towers are goals of potential attacks and they can all bring significant economic, political, social and media effects. Even small terrorist groups with minimal resources can potentially achieve major effects.

The most common types of attacks are: bombing, (vehicle bomb, person-borne/delivered), person followed by armed attack, letters, parcels or packages containing an explosive, arson and vandalism.

Typical methods of electronic attack are: malicious software (Malware) viruses, Trojan horses, worms, spyware, hacking, phishing, denial of service (DoS), IP spoofing, replay attack and man in the middle attack.

Many physical attacks on electric system have been documented around the world over the last few decades. For example, a database for 27 countries outside USA for the period 1994-2004 reported a total number of about 192 terrorist attacks. Among them, about 58% of the attacks took place in Colombia, 8% in Iraq and 6% in Spain, 3% in Russia, Pakistan and France. Remaining 21 countries accounted together for 19%. About 59 % of the attacks were targeted at electricity transmission, 13% at substations and 12% at power generation. [17]

Another source “The Energy Incident Data Base R. Mullen” indicate ca. 2500 attacks that have been conducted against transmission lines and towers in various parts of the world over 1996-2006. Also, substations and switchyards were attacked more than 500 times over the same period. [18]

Transmission and distribution lines are relatively easy to attack, and have been historically most often selected as targets for terrorist attacks, followed by towers and high voltage substations. Increased use of ICT and deep interdependence of electric system and communications infrastructure makes control centers especially vulnerable to physical and cyber attacks.

A significant number of terrorist attacks and military power on the system took place in Iraq, aimed at targets as power plants and transmission and distribution equipment facilities (also across Asia, e.g. in Thailand, additionally many examples come from Africa).

In the last decades physical attacks on the European electric system have occurred the most frequently, but have been restricted to small groups with limited technical knowledge and affecting some parts of system, but the probability of large attack to EU power system is high. Recent terrorist attacks in Europe (in Madrid and London) have increased risk of similar attacks directly on the European electric infrastructure. More and more data regarding electric power grid have been available to any individual worldwide, so it is possible to fulfil an attack even on several targets at the same time.

[17] R. Zimmerman, C. Restrepo, N. Dooskin, J. Freyissinet, R. Hartwell, J. Mille, W. Remingto: Diagnostic tools to estimate consequences of terrorism attacks against critical infrastructure. Center for Rik and Economic Analysis of Terrorism Events, University of Southern California, LA, California, draft report #05-014, May 31, 2005. pp. 66.

[18] Terrorism and electric power delivery system, National Academy of Sciences.2012

An example of frequent terrorists attacks in Europe was Algerian war in XX century where power energy plants, substations and lines were attacked by OAS. Also, the Irish Republican Army detonated bombs on power substations in the United Kingdom in the past. Terrorism related to the activity of the Irish Republican Army is still a serious threat in the Northern Ireland, and unfortunately in spite of peace process and settlement being reached at the government level, there are still frequent major social unrest and street actions, and in the recent time direct attacks on uniformed service personnel.

A classification of potential power system attackers would be:[19]

1. Malicious “hackers” with substantial knowledge of the system who want to demonstrate their skills in order to occur in social consciousness. They don’t care much about negative consequences. They can be insiders or outsiders.

2. Disgruntled individuals or groups who want to harm a power system, but not to kill a lot of people, or cause wide societal damage. They attack in revenge or retaliation utilities or staff, sometimes as an act of vandalism; sometimes they attack for some symbolic reason e.g. eco-terrorists. They can be insiders with substantial knowledge of the system or outsiders.

3. Individuals or small low-tech groups with limited resources who want to kill a lot of people or cause wide social damage or harm.

4. Terrorists groups with significant capabilities and resources set to kill a lot of people or cause wide social damage or harm. In this approach, power system can be primary or subsequent to the primary objective is to force the measures appropriate to the interests of the terrorist group.

5. Participants in power markets seeking economic advantage by disrupting the operations of other market players. They include knowledgeable employees of the attacked firm assisting the attacking entity. They can be knowledgeable employees as well as knowledgeable outsiders working for assisting the attacking entity.

Electric power system may be potential target for criminal activity, in particular deliberate acts of vandalism, sabotage (which is closely related to terrorists act) and continue to be among the most likely targets for potential future attacks of any kind.

[19] Terrorism and electric power delivery system, National Academy of Sciences.2012

3.2 How security standards provide 'refuge' against malicious attacks

Disruption of the power system for a longer time can result in loss of lives and impose great economic costs. Usually deliberate attack is more violent and brings greater losses than equipment failures or accidents.

There are many things that can be done by utilities, policy makers, regulators, and others to reduce vulnerability and make electric power system more resistant to terrorists attack.

Any increase in reliability minimizes impact of potential terrorist attack and can cause the electric power system will be less interesting as a target for terrorist groups.

Reliability of power systems can be enhanced by standards developing, by incorporating devices, redundancy and back-up systems and investments (but on the other hand this can decrease security through greater complexity). They all increase costs of activities and utilities cannot always afford them.

Developing reliability standards shall be expensive to implement but considerably increases security of the system, what is a priority to utilities.

Other measures to improve safety concern include extension of staff training, additional audits exchanging information on security by seminars, conferences, workshops, brochures, newsletters and they all are less expensive.

4 LIST CURRENT AND FUTURE THREATS

Increases in the use of the Internet and in the interconnectivity of computers and computer-controlled facilities are revolutionizing the communication and business for people, governments, companies, organizations and the rest. There has been a host of benefits: people can get vast amounts of information about every topic imaginable, financial and business transactions are done almost instantaneously, 24 hours a day, and electronic mail, media websites and computer bulletins allow people to be informed about the world in real-time. Use of SCADA (Supervisory Control and Data Acquisition) systems allows communicating with systems, downloading real-time data and controlling their correct operation.

Nevertheless, there are some drawbacks too: this connection between all the people, governments and infrastructures means risks to their computer systems, and so it does to the critical infrastructures and operations they carry out. These include telecommunications, power distribution systems, water supply, public health services, national defence, law enforcement, government services and emergency services. Communication and control of energy systems coexist with corporate IT environments, using in operation data from other systems, neighbouring control centers, substations or from some engineering systems and computers. Such interconnections, along with the grids size and its physical exposure create vulnerabilities and risk of hacking and cyber attacks. The ease and speed of the access is then a double-edged knife as it allow individuals and organisations to interfere with these operations from remote locations for malicious purposes, such as sabotage and fraud.

Cyber threats can be divided into intentional or unintentional. Unintentional threats include disruption of the system due to software upgrades or maintenance procedures, which cause the damage without intention. In this work, only intentional threats will be studied.

Possible attackers to energy systems are very different in organization, knowledge and motivation. The following table shows a classification of these attackers. Anyway, it is not a definitive classification, as threats are continuously growing and evolving[20]:

[20] Stouffer K., Falco J., Scarfone K.: National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security, Gaithersburg, 2011

Table 2 : Threats classification

Threat	Description
Criminal groups	Criminal groups are using more and more cyber intrusions mainly to gain money. For example, they could try to get confidential information from companies to commit identity theft, or to blackmail them, or to extort them by threatening the dissemination of sensible information (or by merely demonstrating that they are able to do damage and demanding a ransom), or commit fraud, or forgery (changing values in bills, for example).
Foreign intelligence services	Foreign intelligence services can use cyber intrusions to gather information or espionage. Several nations are trying to develop information warfare methods, programs and abilities. These methods can impact seriously on the supply, communication or economic infrastructures of the other country, affecting citizens and military power.
Hackers	They have certain knowledge about computers and communication systems, and they can break into systems violating the security measures. Sometimes hackers crack into networks for the thrill of the challenge or to boast in the hacker community. Others hack into systems to take revenge, stalking or to gain money. Although cyber security is increasing, hacking programmes are becoming more sophisticated and easy to use, so even hackers who have not extensive computer abilities can download programmes and attack their victims.
Hacktivists	They are politically-motivated hackers who attack publicly accessible web pages to send a political message and e-mail servers to overload them.
Insiders	Dissatisfied employees, outsourcing vendors and other people who have permission and physical and cyber access to the system facilities. As they know the target system, they do not need very much knowledge of computer intrusion. They can cause damage or steal system data. Insiders include also contractors hired by the company and poorly trained employees who can unintentionally install malware in the systems.
Spyware and malware writers	Individuals or organisations who write malicious code designed specifically to damage or disrupt a software: viruses, worms, Trojan horses, etc.
Phishers	Individuals or groups who carry out phishing attacks trying to steal identities or information to gain money. They can use spam, spyware or malware too.
Spammers	Individuals or groups who distribute spam (undesired e-mail) using a false or hidden identity to sell products, conduct phishing attacks, introduce spyware or malware, or attack the system.
Bot-network operators	A bot-network consists of some computers whose defences have been broken and whose control has been taken over by the attacker. Each computer is called a “bot”, and is created when it is penetrated by malware. Generally, bot-networks are used to coordinate attacks, and to send spam, malware attacks and phishing attacks to other computers. Sometimes, a spammer purchases the services of a bot-network and pays the operator for sending publicity.
Terrorist groups	They attack unlawfully persons or property to coerce a government, the civilian population or a segment of them, to get political or social objectives, cause mass damages or weaken the economy. They can use phishing attacks or spyware and malware attacks to gather information or obtain money.

Typical methods of cyber attack to energy system are: malicious software (Malware) viruses, Trojan horses, worms, spyware, hacking, phishing, denial of service (DoS), IP spoofing, replay attack, man in the middle attack. However, during recent years there appeared a new type of dangerous attacks - bot installation. They are launched by a new type of hackers – bot-network operators that invade and take over multiple systems to coordinate and distribute attacks, or use the invaded and remotely controlled computers as illegal storage and processing devices.[21] The following is a detailed description of these methods.

4.1 Social engineering

Social engineering is a technique used by attackers to gain system access or information by exploiting the basic human instinct to be helpful. In most cases, social engineering is successful since the penetrated utility personnel are not aware enough of security-related duties and responsibilities. As a result cyber attacks based on information gained by social engineering can steal personal data (e.g., passwords, logins), enter a SCADA database, and made undesirable data manipulation and remote control operations.[22]

4.2 Malware: viruses, Trojan horses, worms, spyware

Malware is a short for malicious software, and covers files and programs installed without owner's knowledge and permission to infiltrate a computer system and gather information such as passwords, scan drives, upload and download data. Malware spread by email, some websites, by CD, DVD, or USB drive or from infected computers also to whole network. Typical examples of malware are viruses, Trojan horses, worms, and spyware.

4.3 Viruses

A Virus is a malicious code that can copy itself into a host computer system. More specifically, it replicates itself into operating systems and programs and modifies them in a way that is harmful towards the user. When a user runs the infected host, he causes the virus code to run also, and execute its programmed mission. The virus can only spread from one computer to another in the form of an executable code. For instance, a user sends it over a network or the Internet, or carries it on a removable medium such as a floppy, CD, DVD, or USB drive.

When viruses are executed they may cause harm to computer system's hosted data (viruses in order to seek needed information almost always corrupt or modify files on a targeted computer), functional performance, or networking throughput. They can cause from minor disruption to major malfunction or service disruption, even erase everything on a hard disk. Sometimes, viruses install a backdoor on the infected system that

[21] H. Jormakka, P. Koponen, H. Pentikainen, H. Bartoszewicz-Burczy: On managing physical and cyber threats to energy system identification and countermeasure requirements" Maintenance and Reliability no 3 (47) 2010.

[22] A. Babś, H. Bartoszewicz-Burczy, J. Świderski: Guidelines to classify threats and damages (physical and cyber). Net Protection CIPS project. IEN, 2011.

allows the attacker to control the system. These attacks are very dangerous because of the impact they can produce, such as the unavailability of the HMI used by the operators to control the plant processes and the corruption of the process historian. Even more so, since all the control traffic between the network and the remote sites passes through the Intranet, all this traffic would be affected by the attack, hindering the remote maintenance and control of the plant process network.

On the other hand, viruses can attack the process network, which hosts the whole set of SCADA system, that is, the systems that control the RTU in the field network and control the entire system. These systems are communicated with the field RTU by means of protocols like ModBUS, DNP3, OPC and Profibus. Common viruses can cause the reboot of field devices using Ethernet connections or saturate the bandwidth between master and slaves of the SCADA system, de-synchronising master and slaves. Other viruses can corrupt the SCADA masters, what can take a long time to restore. A few viruses are able to directly communicate with the field devices, taking over the function of the SCADA systems. These viruses are critical, because an attacker could take the complete control of the system. Antivirus software is the most useful tool against this threat. However, even an updated antivirus can be attacked by some viruses released between the issue of the virus code and the release of the antivirus code update.

4.4 Trojan horses

Trojan horses are designed to allow hackers a remote access to target computer systems. They are computer programs that apparently have a useful function, but hide a malicious function which can avoid security mechanisms. In case a Trojan horse has been installed on a target computer system, it is possible for a hacker to access this system remotely and perform various undesired and harmful operations. The range of operations that can be performed by a hacker depend on user privileges on a target computer system and design of the Trojan horse.

Trojan horses are similar to virus, except that it does not propagate itself as a virus does.

In October 2011 Budapest University of Technology and Economics alerted on Duqu, Trojan designed to collect intelligence about its targets. Duqu has been confirmed in several countries in this in: France, Netherlands, Switzerland, Ukraine, Iran, India, United Kingdom.[23]

4.5 Computer worm

A computer worm is a malware that is a self-replicating computer programme, and it is sent out to computers on the network. The computer worm activity is carried out without any user intervention. Unlike a virus, a computer worm does not need to attach itself to an existing program. The worm uses system memory and network bandwidth, thus overloading Web servers, network servers, and individual computers and making all operation slow down. They can also delete files on a host system.

[23] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Several destructive computer viruses and worms have attacked electric system including: Slammer, Stuxnet Flamer, and others.

In 2003, the Slammer virus, attacked the MS SQL database Scada system, and stopped for five hours of safety systems of nuclear power plants David-Besse in Ohio. Slammer entered to David Besse plant through the unsecured contractor network.

The Stuxnet virus was first detected in 2010 and showed, that a cyber attack could also cause significant physical damage to a facility targets. More than one thousand devices in the Iranian plant in Natanz next to a nuclear power plant in Bushehr were destroyed. That shows that future malware, modeled on Stuxnet, could target energy infrastructure - such as power plants, sustations in Europe as well.

4.6 Spyware

Spyware is a malware that is installed on target computers in order to steal sensitive information (user ID, password), also collect information about computer users (favorite Website) as well as copying data from hard drives without their knowledge. The presence of spyware is often hidden from the user. Spyware programs not only can collect various types of personal information but can also interfere with user control of the computer in other ways.

4.7 Denial of Service (DoS)

A Denial of Service is a deliberate limit or denial of access to resources. It is a hacker attack that is aimed at disrupting computer or website normal function to make it unavailable to its intended users. In this way, the attacker can limit or deny access to specific resources, such as company Intranets or power plant networks, or public services as file transfer servers or websites. In general, DoS attacks are implemented by either forcing the targeted computer to reset (using a design or implementation flaw discovered by the attacker), or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the attacked computer so that they can no longer communicate adequately. One common method of the attack involves saturating the target computer with external communications requests, such that it cannot respond to legitimate traffic, or responds slowly making it unable to provide operation.[24]. Other possibility is discovering an implementation flaw. When the attacker sends a malicious request to the Web Service, it causes an abnormal consumption of memory, and the unavailability of the service. These attacks are dangerous because they can avoid the maintenance and operation of some facilities, which often can be made remotely using SCADA systems, a site-to-site VPN connection and a RADIUS (Remote Authentication Dial in User Service). These systems allow the remote operators to act as if they were local by downgrading. An attacker could make impossible to access to the system information, to check the state of the system and it would not be possible to operate it in case of emergency. The importance of the attack depends on the target, the duration of the attack and the minimum service requirements. It must also be considered possible domino effects with other systems and services which depend on the attacked service.

4.8 Distributed Denial of Service

A Distributed Denial of Service attack (DDoS attack) is an attack that consists of a certain number of simultaneous DoS attacks aimed at a single target computer system and performed by different computers. As a result resources of the targeted computer system can no longer be used to provide its intended service.

[24] A. Babś, H. Bartoszewicz-Burczy, J. Świderski: Guidelines to classify threats and damages (physical and cyber). Net Protection CIPS project. IEN, 2011.

4.9 Permanent Denial of Service

A Permanent Denial of Service (PDoS), also known as phlashing, is an attack that damages a computer system or computer-based device in a way that this system/device requires replacement or reinstallation of hardware. Usually PDoS attacks use secure access connections which allow remote administration of such devices as routers, printers, or other networking hardware. The attacker replaces a device's firmware with a modified, corrupted, or defective firmware image. This makes the device unusable for its original purpose until it can be repaired or replaced.

4.10 IP spoofing or stealth of Domain Credential

IP address spoofing (IP spoofing) is accomplished when a hacker uses a discovered IP address as its source address to gain access to the protected computer system. The valid IP address can be obtained by a hacker in a variety of ways including snooping and social engineering. This type of attack is most effective where trust relationships exist between machines. For example, it is common for some corporate networks to have internal systems trust one another, so that users can log in without a username or password provided they are connecting from another machine on the internal network. Creating a connection from a trusted machine, an attacker may be able to access the target machine without an authentication (undesirable remote access to substation SCADA/IDEs is possible e.g. by using r-services – remote-login (rlogin), remote-shell (rsh))[25]. Once the attacker has obtained the IP address, he can make a direct cryptanalysis and sniff the data traffic in the network. Moreover, he can reject any remote log-in request.

4.11 Replay attack

A replay attack occurs when a hacker intercepts a communication between two parties and replays the transaction. For example, a hacker might intercept a data transaction between a SCADA dispatching center and a substation SCADA. The hacker then replays the transaction in order to perform substation control or data theft.

4.12 Man in the middle

A man in the middle attack (MITM) is an attack during which the attacker makes independent connections with communicating computer systems (e.g. with SCADA at the dispatching center and with the substation SCADA) and relays messages between these systems, making them believe that they are communicating directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker could also capture messages from a system, modify its content and sent it to the receiver.

[25] A. Babś, H. Bartoszewicz-Burczy, J. Świderski: Guidelines to classify threats and damages (physical and cyber). Net Protection CIPS project. IEN, 2011.

4.13 Cross-site scripting

The attacker uses a third party authentic website, to run their program within the victim’s computer. The attacker creates a malicious website or link in a legitimate website. When the victim clicks it, the attacker can discover vulnerabilities, steal cookies (data exchanged between web servers and browsers), log into keystroke (this is, register the passwords typed by the user on his keyboard), capture screen shots, collect information and remotely access and control the machine.

4.14 Phishing attacks and local DNS poisoning

They are used to gather information from legitimate users by making them connect to a malicious website, by means of a faked e-mail or a link. The access to this website is set in such a way as to make them believe to be connected to a legitimate website. Consequently, a legitimate user could supply sensitive data or login credentials to a malicious website.

Another possibility is transparently re-routing the user to a fake server created by the attacker. In this way, the attacker can provide the operator with a false picture of the system, or obtain the operator credentials and then have direct access to the SCADA system to attack it. The best attacks re-route the user to the legitimate website after stealing the credentials. In this way, it is very difficult for the user to discover the attackers. This attack impacts directly on the maintenance and management of the system, since the attacker could use the credential of an internal user to create a big damage. He could access to protected information and learn about anomalies.

In both cases, some social engineering is needed: to send a faked e-mail and succeed in the attack, it should look like a legitimate official e-mail. In the second case, to re-route the user it is necessary to know the user´s Domain Name Servers. Besides, the target websites must be accessible to the attacker, to learn what it looks like (logos, letter font, graphical aspect) and the language. The way the user is asked to enter has to be known by the attacker, too.

Actually, these attacks cannot cause any power disturbance, but they can ease further attacks, combining physical and cyber acts, which could cause big damages. For example, the attacker could take advantage of discovering an emergency situation to carry out a bigger attack.

4.15Logic bombs

They are pieces of code inserted into a software system, that can start a malicious function when one or more specified conditions are fulfilled.

4.16 Passive wiretapping

Some data, such as passwords, are monitored or recorded when they are transmitted over a communications link, without changing the data.

4.17 Structured Query Language (SQL) injection

It is an attack that causes the alteration of a database search in a website. This can be used to get unauthorized access to information in a database.

4.18 War dialing and war driving

The attacker detects connections to the system by surrounding wireless-equipped computer, detecting their phone number. War driving is similar, but the attacker drives a car through cities and neighborhoods carrying a wireless-equipped computer that can find unsecured wireless networks.

4.19 Scanning

The attacker captures a message which is being sent in a wireless network, and scans the destination IP addresses. In this way, he can determine the service ports on the receiver machine that are running or in listening state to connect to access points.

4.20 Zero-day exploit

This attack takes advantage of security vulnerabilities that are unknown to the general public. Sometimes, the code is written by the discoverer of the vulnerability. It is then a potent threat because in the time interval between the first attacks and the creation of defenses there are no protections.

4.21 Password cracking

The attacker uses a program which repeatedly tries to guess the password to access to a system.

All described methods of attack can be dangerous for SCADA systems as they could allow unwanted access to systems, manipulate data as well as spread across the network.

Hardware and software components (or security subsystems) make use of security architecture:

- Firewalls, DeMilitarized Zones (DMZs) and proxy servers,
- Intrusion Detection and Prevention Systems (IDPSs),
- Cryptographic techniques including:
- Data content confidentiality,
- Data integrity, digital signatures and digital certificates,
- Authentication mechanisms,
- Anti-malware software (anti -virus, -trojan, -warm, -spyware programs)

4.22 Bot-Net

A Botnet is a network of compromised (hacked) computers (bots) with installed malicious software, which is controlled by a botnet-operator (command- and-control-server, C&C). If used for criminal purposes, the bot malicious is usually installed without the knowledge of the computer-owner.

Botnet operators are attackers, they can invade and take over multiple systems to coordinate and distribute attacks, sending spam, or use the invaded and remotely controlled computers as illegal storage and processing devices. They use C&C software, to forward repetitive operating tasks to other computers on the Internet (bots), which is independently i.e. no interaction with a computer-owner is necessary.

5 EVALUATION OF THREATS TO THE CONTROL SYSTEMS OF A POWER NETWORK

Risk assessment and management are essential to confront, minimize and prevent terrorist acts, and empower security agencies. To do this, the first step is to consider what can be threatened and must be protected. These assets are called critical infrastructures and include agriculture, banking and finance, chemical and hazardous waste, defense, etc., but one of the most important is the energy sector.

In the past, terrorists attacked mostly physical objectives and infrastructures, but nowadays it could be easier and safer for them to carry out a cyber-attack, and the damage achieved could be bigger. For instance, attacking a single bank could only cause loss of the money in the bank strongbox, but blocking the bank communication could stop all the operations which were being carried out, not only in a single bank, but also in many other offices.

In a risk assessment, the vulnerability of the infrastructures must be analyzed, critical functions and facilities identified, and their security improved. Even though it is impossible to protect every possible target, it is clear that the more difficult it is for terrorists to attack facilities, the less likely these attacks are.

Another point to be considered is that if security in the most attractive facilities makes a successful attack very difficult, terrorists could choose a nearby facility that can be less attractive, but has a higher probability of success on account of inappropriate security. In general, the probability of a terrorist attack cannot be evaluated as terrorism is random.

The evaluation of critical infrastructures and assets should be ongoing, maintaining and updating databases on critical assets and vulnerable infrastructures. Although this evaluation can seem overwhelming, it is essential to improve public safety. Assessments must be made not only as a routine but also their effectiveness against attacks should be checked.

In the next pages, the general methodology to carry out threat assessments will be commented, along with an example of a real assessment method: the National Infrastructure Protection Plan (N.I.P.P.), launched in the United States of America[26].

[26] United States Department of Homeland Security (2009). National Infrastructure Protection Plan. Partnering to enhance protection and resiliency.

Table 3: National Infrastructure Protection Plan (EEUU)

THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (N.I.P.P.)
The National Infrastructure Protection Plan (N.I.P.P.) was released in 2006 in the U.S.A., and has been updated in a new version published in 2009. The goal of this plan is to “Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation’s Critical Infrastructures and Key Resources (C.I.K.R.) and to strengthen national preparedness, timely response, and rapid recovery of C.I.K.R. in the event of an attack, natural disaster, or other emergency”. C.I.K.R.s include “systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combinations of those matters”. **Although it is not specially focused on power assets, it is a very clear framework to carry out a threat assessment. The N.I.P.P. helps administrations and private sector focus their efforts on areas where they can produce the most benefit to reduce vulnerabilities, threats and consequences of terrorist attacks. This program has been based on existing public and private sector protective programs to be cost-effective and to minimize the burden on owners and operators.** **On the one hand, this plan provides guidance to carry out risk assessments, but on the other hand it creates a framework to integrate initiatives developed by different users to create a national common strategy.**

A risk assessment and management approach consists of these steps:

1) Study and description of the system and cyber security modeling: Learn what the system is like and the way it works.

2) Criticality assessment: Identify and classify important or critical assets, and calculate criticality, or the damage that the destruction or malfunction of the asset could cause in the system.

3) Threat assessment: Identify and evaluate existing or potential threats to an asset.

4) Vulnerability assessment: Evaluate the weaknesses of an asset, or the ease to be attacked.

5) Risk calculation: Risk combines into a variable criticality, threat and vulnerability, so it is very useful to evaluate damage to the asset and probability of the attack.

Table 4: NIPP Risk Assessment methodology

N.I.P.P. RISK ASSESSMENT METHODOLOGY: STEPS
The N.I.P.P. risk assessment methodology consists of the following steps: 1) Set goals and objectives: Define the objectives and outcomes that will make up an effective risk assessment methodology. 2) Identify assets, systems and networks: Carry out an inventory of the assets, systems and networks, which are C.I.K.R.s or contribute to the critical functionality, and gather information on these assets. 3) Assess risks: Evaluate the risk, according to direct and indirect consequences of the attack, vulnerabilities to the attack and general or specific threat information. 4) Prioritize: Aggregate and compare results to get a reliable view of the importance of each asset, system or network risk, and the mission continuity if the damage finally is produced. Establish priorities according to risks, and determine appropriate protection measures to get the biggest return. 5) Implement protective programs and resiliency strategies: Select actions or programs to minimize the risk, identify and provide resources to solve priorities. 6) Measure effectiveness: Evaluate it at the appropriate sector: national, State, local, regional to measure progress and determine if the measures are effective. This process must be ongoing, so that Federal Government and users can measure progress and take corrective measures to improve the asset protection over time.

5.1. Study and description of the system and cyber security modeling:

The whole electric network must be analyzed to acquire information about the system and the way it works. Digital systems configuration and data flow must be identified and studied to create a model and establish the appropriate cyber security. As there are several systems, interacting all together, the exact location of all the systems in the site’s digital environment and interfaces with other assets should be known. In general, the following facts can be taken into account to prepare the model:

- Any redundancy could be simplified as a single system.
- One-to-one direct data communication, analog input-output and digital input-output may be simplified or excluded.
- It is necessary to know the mechanism and direction of the data transfer.
- Security controls already working, such as firewalls, intrusion prevention systems (IPS), intrusion detections systems (IDS), encryption and data flow control status must be identified.
- Possible access to the system from outside or through portable devices used for maintenance should be known.

It is necessary to identify:

- Relevant assets, ways to control the system (human workers, hardware, software and information assets, subsystems and components, interfaces).
- Data circulation between different assets or parts of the electric system.
- System operational context: different usage states, procedures and conditions.

5.2 Criticality assessment:

5.2.1) Critical infrastructure and asset list:

A criticality assessment is a systematic work to identify and evaluate important or critical assets, and the impact of an attack. It helps specialists calculate the relative importance or value of assets and divide resources up amongst the most critical assets.

It is essential to determine the results of loss or damage to important systems and assets (including loss of time), as well as the effort and control and management functions needed to solve the problem. For cyber assets, some of these damages could be loss in confidentiality, integrity or availability. Measuring criticality determines the importance of the asset. For example, damage to essential assets or loss of symbolic assets would denote a big importance.

Assessing criticality can involve some subjectivity. The energy sector is inherently vulnerable and should be considered as critical infrastructure and key assets.

To classify assets, it is necessary to evaluate if a loss of confidentiality, integrity or availability caused by cyber-attacks could reduce the security of the electric system. A useful classification could be based on the following:

- Level 3: Assets associated with safety, which should be protected from malfunction of assets of minor importance. Redundant security controls and other mitigating measures should be applied. These assets can supply information to assets in lower levels, but not receive information from them.

- Level 2: Assets which are not directly related to security, but may cause big damages or are connected to assets at level 3. These assets should not receive information from lower levels, but they can receive it from level 3 or supply it to level 1. Security controls and measures to reduce vulnerabilities can be applied.

- Level 1: Independent assets or systems which cannot impact on the safety and are not connected to any network. The need for security controls and measures to reduce vulnerabilities depends on the impact of cyber-attacks on the asset itself.

In accordance with NIPP assessment, Internet can be used as a key source of information, available for all sectors and comprising domestic and international assets within the Information and Communication technologies. D.H.S. works with the S.S.A.s and C.I.K.R. partners to develop methodologies to identify cyber assets, systems and networks that can have consequences if they are destroyed, exploited or incapacitated. In this way, the dependence of the sector on cyber assets can be assessed. If a valid cyber identification methodology has already been developed by a sector, the N.I.P.P. ensures that it follows the N.I.P.P. risk management framework.

5.2.2) Calculating criticality:

To estimate criticality, a five-point scale is used based on impact, damages and properties, interruption of the use of the facility or asset, or gain obtained by an attacker. This scale is as follows:

- **Extreme (5)**: Important damages or irreparable, permanent or prohibitive costly repair of a facility. Most items and assets are lost or destroyed and they are impossible to repair. The damage and loss of the system would provide the attacker with a big advantage: press coverage, political or tactical advantages.

- **High (4)**: Serious or costly damage to the assets is made, or a big advantage is got by the attacker. Some items cannot be repaired, but others remain intact.

- **Medium (3):** The facility operations are disrupted for a moderate period of time. Repairs can be costly, but not result in significant loss of capability.

- **Low (2):** There are minor damages to operations or facility capabilities, but they do not advantage the attacker.

- **Negligible (1):** Insignificant loss or damage to facilities or operations.

The most important are extreme and high criticality, especially when they appear along with a high threat and high vulnerability.

5.3 Threat assessment:

A threat assessment is defined by the United States Department of Homeland Security (D.H.S.)[27] as "a systematic effort to identify and evaluate existing or potential terrorist threats to a jurisdiction and its target assets. Due to the difficulty in accurately assessing terrorist capabilities, intentions and tactics, threat assessments may yield only general information about potential risks."

Thus, a threat assessment implies doing a survey about attackers who can threat the energy sector in order to know who they are, their origin, how they are organized, their intention and reasons to carry out the attack, likely targets and moments to attack, planning activities they can do, the way they will attack and their capability to do it.

The intelligence process is the basis of threat assessment, since the crime-related information can be used to evaluate and analyze terrorism and terrorist groups. Intelligence efforts can answer questions about the who, where, what, how and when of terrorism and terrorist groups.

[27] https://www.ncjrs.gov/pdffiles1/bja/210680.pdf

This assessment needs an extensive and rigorous research and analysis, using information from police forces, country, local and private organizations and agencies, health services and emergency management organizations. For example, the crime rates in the surrounding area can be used as a measure of the type of criminal activity that may threaten the assets. The assessment must result in a high level of awareness and understanding of the changing threats. It should not be forgotten that threats are motivated by a variety of political and economic reasons.

To carry out such an assessment, essential data to collect before doing it would include:

- **Classification of the attacker:** Activist, terrorist, employee, hacker, etc.
- **Category of attacker**: Foreign or domestic; terrorist or criminal; insider and/or outsider of the organization.
- **Purpose of the attacker:** Theft, sabotage, mass destruction, sociopolitical objectives, etc.
- **Number of attackers for each category**: Individual hacker, "cells" of operatives/terrorists, organized criminals, etc.
- **Target chosen by adversaries:** Power stations, distribution lines, etc.
- **Type of planning activities needed to succeed in the attack**: Long term "casing", photography, monitoring police and security patrol patterns, etc.
- **Most likely or most damaging moment an attacker could attack**: When more people are working in the facility, at rush hour, at night, when more people are using electricity, etc.
- **Range of attacker tactics**: Stealth of credentials, virus infection, deceit, combination, etc.
- **Capabilities of attacker**: Knowledge, motivation, skills, weapons and tools.

Once these data have been collected, threat levels can be estimated based on a combination of the following factors:

- **Existence**: A terrorist group or attacker is present or can access to a locality.
- **Capability**: The capability of the terrorist group or attacker to attack has been demonstrated.
- **Intention**: There is evidence of terrorist group or attacker activity, like stated or assessed intent to carry out terrorist activities, or attacks.
- **History**: There has been terrorist activity in the past, or attacks.
- **Targeting**: There is credible information or activity that shows preparations for attacks or terrorist operations (collection of information on likely objectives, preparation of destructive devices, etc.)

- **Security environment**: It indicates if and how the security and political measures affect the attackers or terrorists' capabilities to attack.

Similarly to criticality, threat is evaluated using a five-point scale:

- **Critical (5):** Existence, capability and targeting are demonstrated, even if history and intentions are not.
- **High (4):** Existence, capability, history and intentions are demonstrated, but not targeting.
- **Medium (3):** Existence, capability and history are demonstrated, but not targeting or intentions.
- **Low (2):** Existence and capability are demonstrated, but not history, targeting or intentions.
- **Negligible (1):** Only existence or capability has been demonstrated, if the rest have not.

Identifying a threat is very complex and difficult, and this process is often not understood or seen as unreachable. However, there are many resources within and outside the police forces, which should be correctly used.

5.4 Vulnerability assessment:

Vulnerability can be defined as "the identification of weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists"[28]. In this way, it is possible to evaluate the ease to attack the facility, because of good accessibility, good ways to get the location, bad protection of the site and lack of response forces or security measures. Another important factor will be the interest of attacking the system to a terrorist. Vulnerability assessment should be based on the system architecture, network design and system requirements. This includes all the computers, software platforms, networks, protocols and other resources required to control the grid and monitor its functions. Security features that are not present in the system, but should exist should be taken into account. Vulnerability can be difficult to be measured, but the following factors must be taken into account:

- **Location**: Location of targets and facilities, ways to get in and out (public websites, company network).
- **Accessibility**: How accessible a target is to the attacker, the ease of entrance, operation, information collection and response forces evasion.
- **Adequacy**: Protection of storage facilities, effective denial of access to valuable or sensitive assets such as control systems and SCADAs which could be used to cause harm.
- **Availability**: Availability of equipment, adequacy of response forces and of physical security measures.

[28] D.H.S. (United States Department of Homeland Security), https://www.ncjrs.gov/pdffiles1/bja/210680.pdf

The vulnerability is estimated using a five-point scale based on the protection and accessibility to the facilities:

- Very highly vulnerable (5): There is a combination of two or more of the following:
  - Direct or easy access to the asset or facility. There are not passwords, or existence of a guess account which allows free access.
  - Asset or facility is open or uncontrolled, so attackers can collect information, operate and avoid responses. Access controls are easily avoided or provide incomplete coverage.
  - Response units cannot effectively counteract an experienced threat.
  - It is a very attractive target for potential terrorists.
- Highly vulnerable (4): A combination of two or more of the following:
  - Easy access to the asset or facility. There exists a factory default password, what makes it easy to break it using social engineering.
  - Asset or facility is open or uncontrolled.
  - Response units cannot effectively counteract an experienced threat.
  - It is an attractive target for terrorists, with a big importance regionally or moderate importance globally.
- Moderately vulnerable (3): A combination of two of the below:
  - Moderately difficult access to the asset or facility. There exists a short password, which is easy to guess, and password is valid for a long time.
  - Asset or facility is open or uncontrolled, but attackers can be detected, or find some resistance. Access to information and operation are hindered, but firewall systems, user authentication and Digital Certificates can be avoided or provide incomplete coverage.
  - Response units can counteract effectively an experienced level attack.
  - It is a moderately attractive target for terrorists, not well known outside the local area.
- Lowly vulnerable (1): A combination of two or more of the below:
  - Very difficult access to asset or facility. It is not possible to change old passwords. They have a length bigger than 8 characters, combining 4 different categories. Passwords are changed at least each 3 months. There could be biometric identification.
  - Asset or facility is well controlled. There are Firewall systems, user authentication, user rights and privileges, and Digital Certificates for authentication of higher level users.
  - Adequate safeguards are taken to prevent and hinder access to sensitive materials.
  - Response units can answer an attack with suitable personnel, equipment and time.
  - It is not an attractive target for terrorists.

5.5 Risk calculation:

Risk can be defined as the extent to which an asset is exposed to a hazard or danger. It will be the ultimate measure of the importance of an asset or facility, as it groups not only the probability to be attacked but also the damage or loss an attack would produce.

This calculation combines into one the three assessed variables: criticality, threat and vulnerability, to determine the risk of an asset, facility or group of assets. There are several techniques to evaluate risk, from qualitative to quantitative formulas. The most used method is based on the next equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Criticality}$$

Where:

- Criticality: Measures the importance of an asset by calculating the impact if the asset is lost or harmed.
- Threat: Measures the likelihood of an attack, based on the existence, capabilities and intention to attack of the terrorists and the ability to counteract them.
- Vulnerability: Measures the weaknesses of the objectives, which the attacker could profit from.

Threat times vulnerability can be seen as the probability of the attack, and criticality is related to the consequence of loss or damage to the critical asset.

Using this method with a numerical scale can lead to a conclusion about the risk of the asset and the measures to be taken. The following is the most used method to classify assets. It is called Table Analysis.

Firstly, three square matrix (5x5) are drawn, each showing the relation between two of the variables criticality, threat and vulnerability.

	Threat				
Vulnerability	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

	Criticality				
Vulnerability	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

	Threat				
Criticality	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Figure 3: Square matrixes showing relation between criticality, threat and vulnerability

Each color represents a different risk:

- 🟥 represents a very high risk (between 20 and 25). Countermeasures to mitigate the risk should be adopted immediately.

- 🟧 represents a high risk (between 15 and 19). Countermeasures to mitigate the risk should be adopted as soon as possible.

- 🟨 and 🟩 represent a moderate risk (in yellow for values between 10 and 14, and green for values between 5 and 9, the first considerably higher than the latter. Countermeasures to mitigate the risk should be planned in the near future.

- 🟦represents a low risk (between 1 and 4). Countermeasures to mitigate the risk would increase security, but this risk is not as urgent as others.

Combining the three variables, a cube can be drawn, with values ranging between 1 and 125. This cube is shown in the next figure.

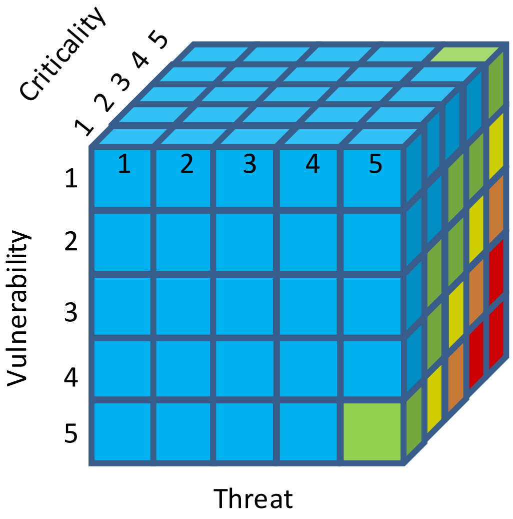

Figure 4. Cube representing the risk due to criticality, threat and vulnerability

This cube consists of 125 smaller cubes, each with a value ranging between 1 and 125. The color code has been changed to show the new value range. Scales for x-axis, y-axis and z-axis are shown, and the origin for the numeration is the left front vertex, whose cube has a value of 1.

Each color represents a different risk:

- 🟥 represents a very high risk (between 100 and 125). Countermeasures to mitigate the risk should be adopted immediately.

- 🟧 represents a high risk (between 75 and 99). Countermeasures to mitigate the risk should be adopted as soon as possible.
- 🟨 and 🟩 represent a moderate risk (in yellow for values between 50 and 74, and green for values between 25 and 49), the first considerably higher than the latter. Countermeasures to mitigate the risk should be planned in the near future.
- 🟦 represents a low risk (between 1 and 24). Countermeasures to mitigate the risk would increase security, but this risk is not as urgent as others.

6 Define attack cases for modelling and the required performance vectors (high level) to react against attack situations

6.1. Define scope of the analysis

A case study is an exhaustive analysis of an individual example to better understand a complex process, system or methodology, or to verify something already known. In a case study, a limited number of conditions and their relationships are chosen and studied. In this way, a phenomenon can be examined in its context, when the boundaries between phenomena are not clear, and different sources of information are studied.

Even when some people state that case studies are not reliable as they are focused only on a small number of cases, and that this method cannot be generalised, in fact researchers use case studies frequently as a research method very successfully, in many disciplines.

In this report, case study method will be applied to help understand attacks to networks. Two cases will be chosen: Poland and Italy. The effects of a cyber-attack, a human failure or hardware breakdown on Polish and Italian electric networks will be studied.

6.2. Requirements to estimate cost/consequence estimates

The most used method to carry out a risk assessment implies determining, for each different failure or attack, three variables: criticality, threat and vulnerability.

Firstly, the electric network and its components must be studied. This involves knowing the systems and assets which make up the network, as well as their connections and the way data are transmitted from a part to another. The exact location of all parts and interfaces with other components must be discovered.

Once all assets and their connections are studied, criticality will be examined. Criticality can be defined as the importance of each asset, this is, the consequences (in time, money) of the loss or damage to the asset. To calculate criticality, the following aspects will be considered:

- Cost of needed repairs, if possible. If not, cost of replacement of the facility.
- Loss of time and money derived of the impossibility to use the facilities. These issues can be very important, if the attack produces a blackout.
- Advantages to the attacker: press coverage, political or tactical advantages.

The next variable is threat. It is a measure of the danger of a terrorist attack. To determine threat, police forces, public and private organizations and agencies, health services and emergency organizations can provide important data related to crime in an area. The next subjects must be evaluated:

- Type of attacker: Hacktivist, terrorist, employee, hacker, etc.
- Category of attacker: Terrorist or criminal, insider and/ or outsider of the organization, foreign or domestic.
- Objective of the attacker: Sabotage, sociopolitical objectives, theft, etc.
- Number of adversaries: Individual suicide bomber, individual activist, group of hackers, gangs, “cells” of terrorists, etc.
- Target selected by adversaries: Power stations, nuclear power plants, transformers, distribution lines, etc.
- Type of planning activities needed to attack: Photography, monitoring police and security patrol patterns, fishing, social engineering, etc.
- Most likely or “worst case” time to attack: Rush hour, at night, when more people are using electricity (a very cold day in winter, when an important football match is going to be broadcast).
- Range of attacker tactics: deceit, force, stealth, combination, etc.
- Capabilities of attacker: Knowledge, skills, motivation, weapons and tools.

Finally, for each facility, vulnerability must be assessed. It determines the weakness of the asset, the ease to be attacked. In this case, the factors to consider are:

- Location: Geographic location, routes to get to the facility entry (ease to enter the facility is measured by “accessibility”). Vulnerability measures difficulty to access the public or private website or computer system.
- Accessibility: Unlike location, it measures the ease to enter, that is, the measures to close the facility and avoid access to attackers. Vulnerability measures difficulty to access the software and programs which control processes.
- Adequacy: Protection of facilities, or difficult access to files or programs that can be used to cause harm.
- Availability: Effective protection measures to counteract an attack.

6.3. A case study method approach

As commented next, there is a wide variety of methods to study the impact of a cyber-attack on the electric system. Some of them are: table analysis, algorithmic analysis, threat trees, bar charts, Pareto diagrams, etc. In other cases, meetings, interviews or presentations can be carried out to gather or transmit information to one or more professionals.

Nevertheless, one of the simpler and at the same time more effective methods is table analysis. This is the method will be used to carry out the case studies.

In table analysis, the next steps shall be followed:

1) Gather information on the electric system: Components and their connections, transmission of data.

2) Identify critical assets: Determine which assets are more important, this is, assets which will cause the biggest damages to assets (especially if they are symbolic assets) or people, or losses of money or time.

3) Determine criticality: Estimate, for all assets, but especially critical assets, the impact of the loss or damage to the asset. This is, carrying out an economic impact analysis to determine cost of repair or replacement, cost of the lost time and other losses due to unavailability of the assets, and damage to people.

4) Identify threats: Measure the risk of a terrorist attack. This implies investigate about the existence of terrorist, their motivation and intention, capability to attack, type, number and organization of terrorists along with targets and ways to attack.

5) Identify vulnerability: This means determining the protection of the asset, how easy it is for terrorists to attack the objective. It is necessary to assess the place where the asset is, the access to the site, the protection of the files or documents in this site, and the existence and effectiveness of protection measures.

6) Combining and weighting criticality, threat and vulnerability, the risk can be calculated. In this way, assets can be classified according to a combination of the probability to be attacked and the damage an attack would produce.

7) Reviewing standards, it is possible to select some countermeasures to try reducing the risk of assets, especially more critical ones, or those which are at high risk.

8) Cost analysis of the implementation of the countermeasures: It is necessary to compare the known cost of the damage or destruction of an asset (not only money, but also lost time) with the estimated cost of implementing the solutions needed. If, taking into account all the damages and costs together the sum is smaller than the cost of the solution, this will not be implemented.

6.4. Attack cases

Electric systems are becoming more dependent on the Internet and computers. This implies a vast amount of advantages, such as real-time information on the system, to detect problems or ensure that it is working correctly. Besides, the Internet allows controlling the system and communicating with it from anywhere using SCADAs.

However, this ease of access to systems can pose an important threat: individuals and organisations can attack systems from remote locations and in a secure manner as it is difficult to identify and arrest them.

There is a big variety of ways to attack power systems, as explained before in part 4 of this Document. However, from the point of view of the electric network, it is more important to identify the effects of the attack on the system than their origin or source. These effects are the following:

6.4.1. Steal of confidential information

Some attacks are intended for getting some confidential information, such as passwords or logins. Sometimes, passwords are used to enter the system and cause further damages, such as loss or change of information or loss of control of the system. In these cases, this attack is only a way to get the real objective of the attacker.

However, stolen information can be used directly to cause damage. Attackers can steal confidential information on a company to steal money, to impersonate the company, to commit fraud or forgery, or simply blackmailing the company by threating it to make public confidential or sensitive information if the company does not pay a ransom or take an action.

6.4.2 Manipulation and remote control of the system

When the attacker takes over the system, he can cause big damages. He could control and hinder communications with the system, and make it uncontrollable for legitimate users. It is easy to imagine the damages an attacker could cause: get information on the system and data on people, hinder maintenance and operation activities, disturb power supply, cause blackouts, slow down control in emergency situations and even destroy the system (and related assets).

6.4.3 Change or loss of information: Modify, erase or corrupt files

Viruses and other types of attacks can change historic or current data, corrupt or erase files, or all the hard disk. Maybe change of information can be more dangerous, as it is more difficult to detect, unless somebody looked into data and discovered changes. Another option would be controlling communication between parties by means of changing messages they receive and send (this attack can be used to steal information too).

6.4.4 Hindering or slowing down of operations

Some attacks are intended to disrupt communications and avoid control of the system or exchange of information between people. This can be done in order to control or manipulate the system, but sometimes, the objective of the attacker is simply avoid communications or make operators lose control of their systems. In these cases, the system operation is not controlled, and possible breakdowns, accidents and emergencies (not directly caused by the attacker) would not be discovered.

A typical way to get this is a Denial of Service (DoS). The attacker prevents legitimate users from entering the systems using a variety of methods: forcing repeatedly the system to reset or saturating the computer with external communication requests in such a way that it cannot respond legitimate requests. Other possibility would be using programming flaws which, if activated, consume large amounts of memory.

7. OTHER METHODS TO EVALUATE THREATS

The information to build the following methods has been gathered from MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos). This methodology, which has been developed by the Spanish Government (Ministry of Finance and Public Administration), is defined as a formal method to look into the risk in the I.T. systems, used to recommend suitable measures to control these risks. MAGERIT methodology consists of three documents or "books". In the first book, called "MAGERIT-Libro 1-Metodología"[29], the general risk assessment method is explained, along to some advices to develop a security plan for I.T. assets. The second document, "MAGERIT-Libro 2-Catálogo de Elementos"[30] describes existing I.T. assets, an asset value assessment methodology, a threat classification and finally safeguards. Finally, the third document, "MAGERIT-Libro 3-Técnicas"[31] is a compilation of threat evaluation methods, which will be explained below.

7.1. Algorithmic analysis

In general, an analysis is a study carried out to split something into all its parts or elements, to know these elemental parts. In a **qualitative analysis**, only the relative importance of the assets will be known, this is, assets will be ordered according to their value, but values will not be known. On the contrary, in a **quantitative analysis**, values will be exactly calculated.

[29] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1-Método. Madrid. http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

[30] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October, 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2-Catálogo de Elementos. Madrid. http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

[31] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October, 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 3-Guía de Técnicas. Madrid. http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

7.1.1 Qualitative analysis

In this kind of analysis, the objective is to know the different elements that make up an asset, and their relative importance, without knowing their exact value. The next steps shall be followed:

- **Value of assets:** It is necessary to assign a relative (not real) value to the assets to assess them. Different scales can be used, but all of them will look like this:

  $$V= (0,.., v_0,v_{1,}\dots, v_i,\dots)$$

  The value 0 means that the asset has no value, it can be lost without any damage or loss. Value should include not only the mere value of the asset (if it has to be replaced) or the reparation (if it can be repaired) but also loss of time and money.

- **Dependences between assets**: It is important to know if the asset A can affect or depends on an asset B. In this way, graphs showing dependences between different assets can be drawn:

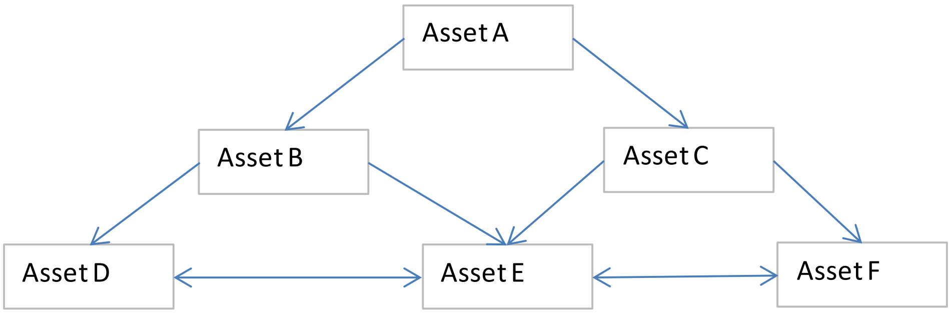

Figure 5: example of assets dependency diagram

- **Cumulative value of an asset A:** It is the sum of the values of the asset A plus all the other assets which depend on asset A, and which would be damaged if A suffered an attack.

- **Loss of value of an asset**: If an asset suffers an attack, part of its value is lost. It is represented as “d”, whose value can vary between 0 (total loss of value) and 1 (no loss of value). Thus, the new value of the asset would be:

  New value= $d.v_i$

- **Loss of value of an asset related to threats to other assets:** If an asset B depends on an asset A, and asset A suffers an attack which makes him lose its value to “$d.v_A$”, then asset B would lose value as well. The new value of B will be “$d.v_B$”.

- **Probability of the attack**: A probability will be assigned to each attack. A scale will be used, like this:

  $$P= (0, p_1, p_2,., p_i,\dots)$$

It is possible, but not compulsory, to use a scale between 0 and 1. Probabilities are related to a certain period of time: they will be different if probability of an attack is measured for a month or for a year.

- **Risk**: It depends on impact (loss of value of assets) and probability. Generally, this function is defined as follows:

  R = Probability x Loss of value of the asset

  Minimum risk will be 0.

- **Cumulative risk:** It is calculated like risk, but using cumulative loss of value.

- **Safeguard packet:** To counteract a threat, some protection measures will be employed. Its efficacy, ”e” will vary between 0 and 1.

- **Residual loss of value of an asset**: As defined before, loss of value is defined as “d”, and the new value is “d.v”. If protection measures are applied, new loss of value will be “dr”, and the new value will be “dr.v”. “dr” will vary between 0 and “d”, being 0 if protection measures are totally effective, and “d” if there are no protection measures, or they are totally useless.

  Residual loss of value = dr.v_i

- **Residual probability of the attack**: If countermeasures are employed, the probability of an attack will be reduced from “p” to “pr”. “pr” will vary between 0, if the protection is perfect, and “p” if the protection in totally useless.

- **Residual risk**: It is defined as risk, but using residual probability and residual loss of value.

  Residual risk = Residual probability x Residual loss of value of the asset

In this qualitative analysis, asset value “v_i”, probability “p_i” and risk “R_i” are measured relatively to other assets. This is, used values are not real, but they show the importance of an asset compared to the others.

7.1.2 Quantitative analysis

This analysis is similar to the qualitative analysis, but the objective is to know the real value and importance of the asset, and the exact damages and losses related to an attack to this asset. Thus, this model does not use a discrete scale, but real positive numbers.

- **Value of assets:** The value of an asset is a real number equal or bigger than 0. “v_0” represents the limit between relevant and negligible values.

- **Dependences between assets:** It is important to know if an asset depends on other or not, and this dependence is evaluated by a coefficient that varies between 0 (independent assets) and 1 (total dependence).

- **Cumulative value of asset A**: If some assets B, C, D… depends on an asset A with certain coefficients, the cumulative value of the asset A is the sum of the value of A plus the values of B, C, D… each one multiplied by the respective coefficient.

$$\text{Cumulative value of asset A} = \text{Value (A)} + \Sigma_i(\text{value (X) x coefficient (X)})$$

- **Loss of value of an asset**: When the asset is attacked, its value is reduced. The loss is represented as “d”, similarly to the qualitative case. “d” varies between 0 and 1. Thus, the value of the asset will be:

$$\text{New value} = d.vi$$

- **Loss of value of an asset related to threats to other assets:** If an asset A depends on B, the damage suffered by B is transmitted, to some extent, to A. If v_A is the value of A, d is the loss of value of B, and “c_{A-B}” is a coefficient that represents the relation between the values of A and B, the new value of A will be:

$$\text{New } v_A = d \text{ x } v_A \text{ x } c_{A-B}$$

It is important to notice that, in this formula, the value of the asset B is not used.

- **Probability of the attack (p)**: The probability will be the ARO, or Annual Rate of Occurrence if it is referred to 1 year. It will vary between 0 (impossible attack) and 1 (certain attack). Sometimes, if probability is smaller than a value p_0, it is not considered.

- **Risk**: It is calculated in a similar way than in qualitative analysis:

$$R = \text{Probability x Loss of value of the asset}$$

- **Cumulative risk**: It is calculated like risk, but using cumulative loss of value.

- **Safeguard packet**: Some protection measures are used to fight a threat. Its efficacy, ”e” will vary between 0 (the measures do not protect) and 1 (the measures protect totally). It is possible to distinguish between an efficacy against frequency, “e^f” and efficacy against loss of value, “e^i”. Total efficacy can be defined using this formula:

$$(1-e^i) \text{ x } (1-e^f) = 1-e$$

- **Residual loss of value of an asset:** If “d.vi” is the new value of the asset after a totally effective attack, “dr” will define the loss of value when protective measures are applied. “dr” will be 0, and there will not exist any impact if the effectiveness of measures is total, this is, $e^i=1$. “dr” will be “d” if the measures do not protect and $e^i=0$. “dr” will take intermediate values for e^i ranging 0 and 1.

$$\text{Residual value} = \text{dr.vi}$$

- **Residual probability of the attack:** If the protection is totally effective (e^f=1), probability will be 0, and if protection are useless (e^f=0), probability will be "p", the probability before applying protection. For other values of e^f, p_r will take intermediate values.

- **Residual risk**: It is defined as risk, but using residual probability and residual loss of value.

$$\text{Residual risk} = \text{Residual probability} \times \text{Residual loss of value of the asset}$$

In quantitative analysis, all variables are real numbers, greater than or equal to 0.

7.2. Threat trees

Threat trees are used to represent all the possible ways to attack an objective. This objective is the "root" of the tree. Iteratively, different "branches" are drawn, representing ways to attack the objective. It is possible to draw intermediate nodes representing steps to be reached when following a way to attack (or a "branch"). If there is more than one objective or asset, each one will have its tree, so it will be necessary to draw what is called a "threat forest".

Threat trees allow understanding graphically and quickly different ways to attack an asset, and designing protections. Besides, the objectives of an attacker can be analysed, along with the knowledge, abilities, information, etc. which he would need.

Generally, it is possible to follow several alternative ways to reach an objective. Then, the node is called OR node. If there are activities that must be carried out simultaneously to success in the attack, the node is an AND node.

Nodes or steps to reach an objective can be completed with information about the attack: knowledge required (somebody with no experience, with some experience, a professional hacker, etc.), investment (amount of money and time needed to reach the objective) and risk (consequences to the attacker if he is arrested).

Once this information has been assigned to each node, it is possible to determine the most likely attack, by finding the way that requires the less knowledge and investment. If the attacker profile is known, the branch chosen will be that which requires the less expenses given the attacker knowledge.

On the other hand, if protection measures are applied, their effects can be:

- Increasing the required knowledge and abilities of the attacker to succeed in the attack. Ideally, the attack should be impossible no matter the knowledge.

- Increasing the required money to succeed in the attack. Ideally, the cost of the attack should be bigger than the potential gains.

Ideally, protection measures should eliminate all the branches, but normally security levels only have to reach a certain level.

To draw the tree, it is necessary to know where the biggest value of the asset is, along with attackers' objectives. Ideally, all possible branches should be drawn, but it depends on the imagination and knowledge of the analyst. The more experience is got from successful or detected attacks, the more the system can be improved. Some ideas to get this experience are the following:

- Gather experience from the company, or other companies.
- Brain storming meetings, where some people suggest, in an informal way, possible ideas of attackers. In this way, it is possible to get ideas, which must be ordered and carefully analysed.
- Tools suggesting attacks based on the nature of the assets.

The algorithmic analysis, explained formerly, can be used to determine the nature of the assets and relations between them. In this way, assets which can be used as a way to more important assets are defined.

In conclusion, threat trees are very useful to determine threats and prevention. They help to think like the attacker, foreseeing their actions. Threat trees are very difficult to build if no or little information can be gathered, but when there is some experience available, they can use it effectively.

On the other hand, they must be carefully protected from attackers, because they can be a very useful tool to succeed in the attack. Besides, to analyse all possible threats to a complex system, it is necessary to build a great amount of very complex trees.

7.3. Graphic methods

Sometimes, representing risks (determined using algorithmic analysis or table analysis) in a graph can help to make decissions or understand risks. There are a variety of methods to represent risks:

7.3.1 Line graph

It is the most clasical graph. X and Y axes are used, representing in the abcissa axis the threat and in the ordinate axis the risk. Ordinate axis can be linear or logarithmic. Linear scale can be used when risks do not vary very much, and logarithmic must be used when they are very different.

On the other hand, linear scale can show absolute difference between two values:

$$x_i-x_j$$

while logarithmic scale shows relative difference:

$$\underline{x_i-x_j}$$

x_i

Risks can be drawn as points, or link the points using lines. Sometimes horizontal lines can be used to show thresholds (minimum or maximum values to make a decision). The following is an example of these graphs.

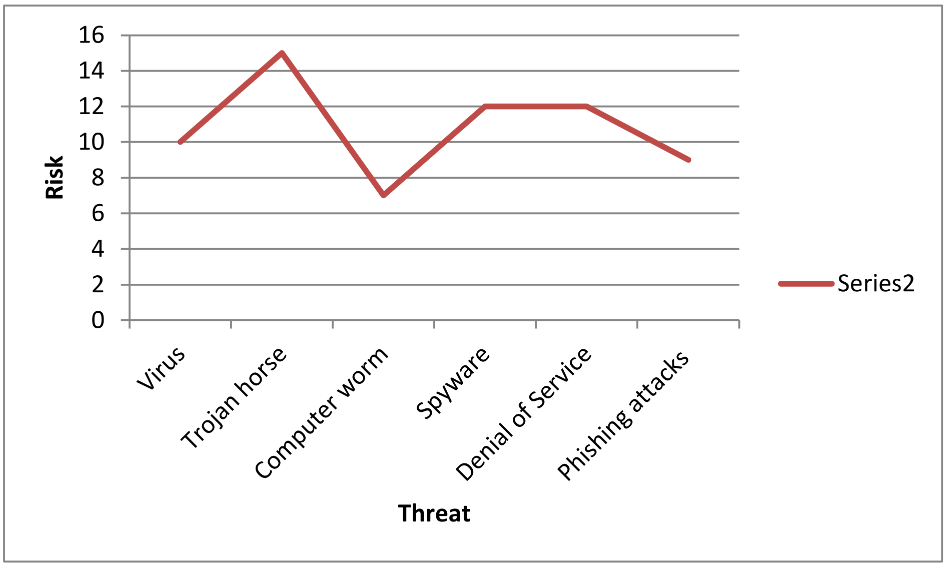

Figure 6: Example of linear graph

7.3.2 Bar chart

In a bar chart, data are ordered in X and Y axes: in the abscissa axis the threat and in the ordinate axis the risk. They are similar to line graphs, but they can show less data (as bars take up more space than points and lines). Similarly to line graphs, Y axis can be logarithmic (if data vary very much) or linear (if data are similar). Horizontal lines can be drawn to show minimum or maximum thresholds.

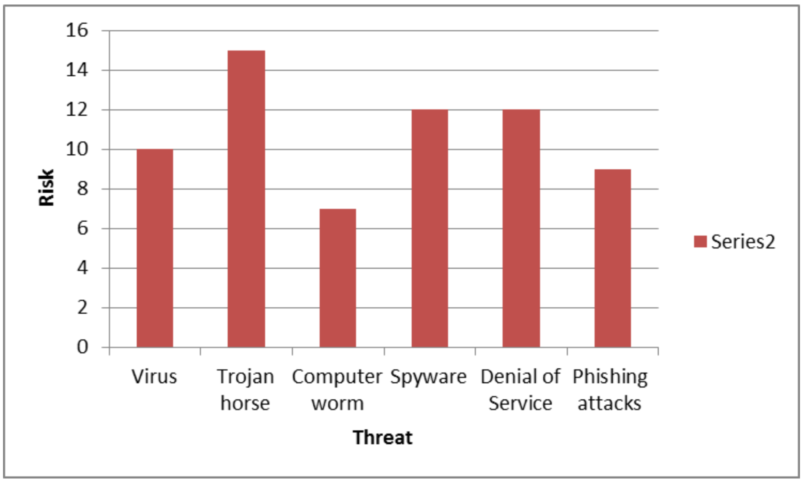

Figure 7: Example of bar chart representation

7.3.3 Radar chart

These graphs show all the variables in semi-axes or radii which radiate from the centre of the log. Each radius represents a variable, and they are graduated to show levels and thresholds in linear or logarithmic scale. The value of each variable is marked in its radius (the centre is the value 0 for all variables). All the marks are linked by segments, resulting in an irregular star-shape polygon called radar chart.

This graph helps to study globally the risks, showing their features, trends and relations between risks.

Once the risks are calculated, to get the chart the first step is drawing the centre and radii. Scales are drawn in the radii, drawing a circle (or regular polygon) with all the radii inside it. It is important that the angles between consecutive semi-axes are always the same. Sometimes circles or polygons are drawn representing minimum or maximum thresholds.

These diagrams are useful to show graphically balance or unbalance in the axes, to show maximum and minimum profiles and to show evolution.

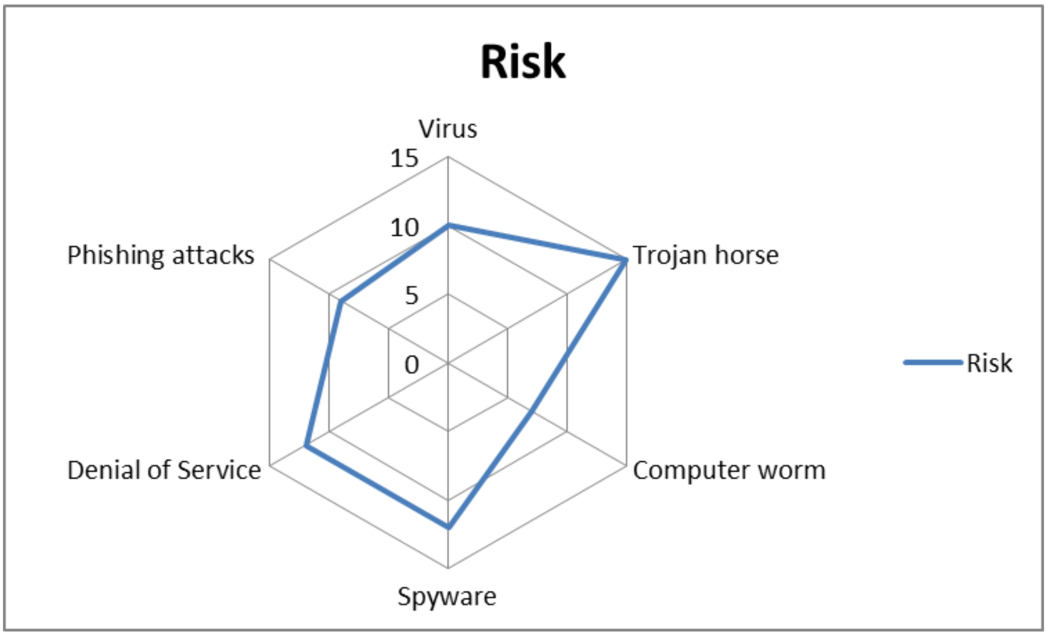

Figure 8: example of radar chart

7.3.4Pareto diagram

Vilfredo Pareto (1848-1923) was an Italian sociologist who studied the income distribution. He discovered that 80% of wealth belongs to 20% of the population, and 80% of the population owns the 20% of the wealth, in all societies throughout history. This was called Pareto principle or 80-20 rule.

This law has also been applied to quality and business management, where it can be summed up as: “if a problem has several causes, 20% of them cause the 80% of the problem, while solving the remaining 80% of the causes will only solve 20% of the problem”.

Pareto diagrams are used to graphically separate the few and very important aspects and the many and irrelevant aspects. In this way, it is possible to focus on important aspects, solving most of the problem.

This graph shows in the abscissa axis the problems, and in ordinate axis the cost of the cause. The different causes are represented in decreasing order: the few important causes in the left and the many irrelevant in the right. It is possible to show, at the same time, the aggregate risk in percentage.

Using this graph, it is possible to analyse the risk according to the assets, determining the assets that cause most problems. Besides, they are useful to detect which threats are more dangerous. The following graph is an example of Pareto diagram.

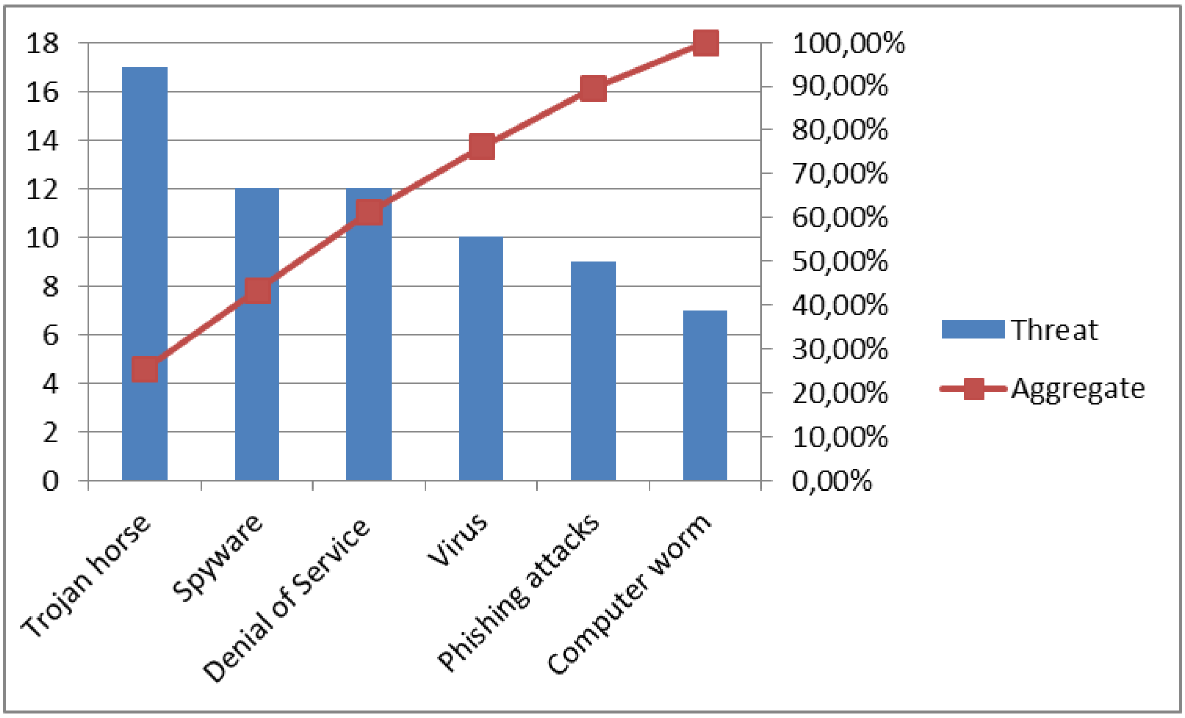

Figure 9: example of pareto diagram

7.3.5Pie chart

These diagrams show data as circle sectors, each sector covering an angle proportional to its value. Together, the sectors make up a full circle, this is, 360º. Generally, these graphs use linear scale.

Commonly, data are ordered decreasingly, as in Pareto diagrams. Pie charts are used to show graphically the contribution of all parts to the total, but they are not suitable to represent very much data.

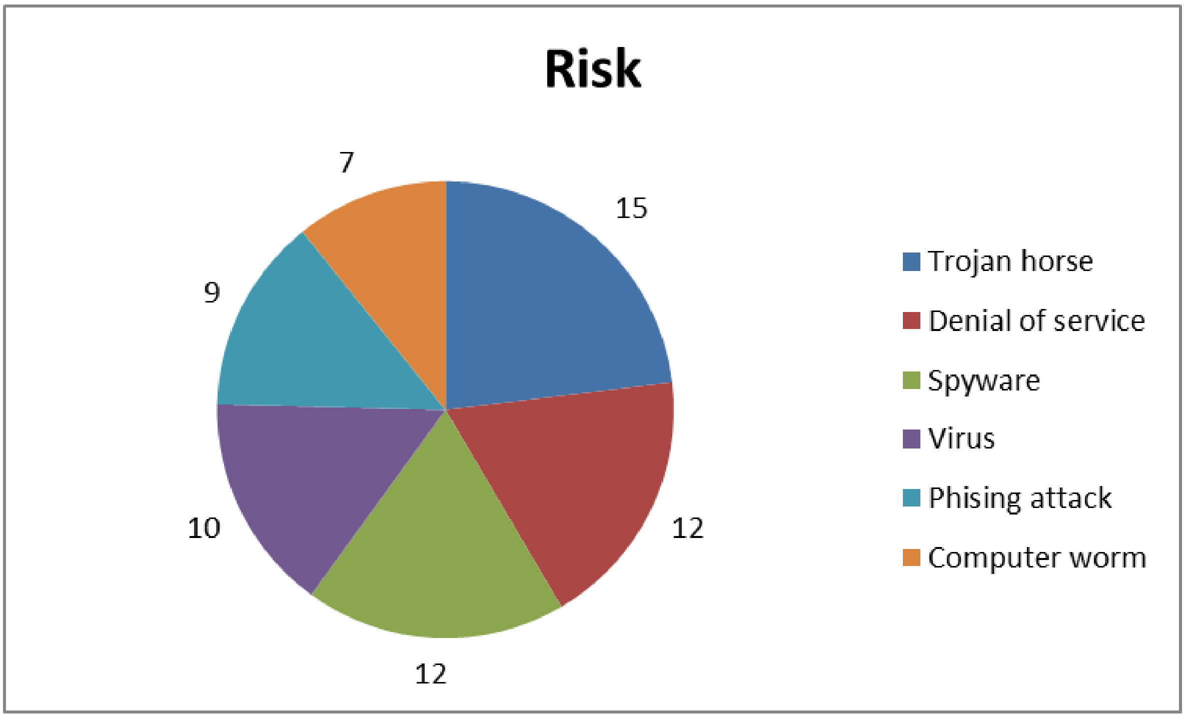

Figure 10: example of pie chart

7.4. Working sessions

Working sessions can be used to gather information, communicate results, save time, ease users and managers' participation or increase quality. According to participants, objective and how they are conducted, they are divided into interviews, meetings and presentations.

7.4.1 Interviews

Interviews are working sessions aimed at getting information from people individually or in groups. They can be structured when there is a set of planned questions without improvising or non-structured when there is no rigid questionnaire.

In general, these interviews are semi-structured: there is a set of questions, but the interviewee can answer in a different order, or expand on some points. It is very important that no useful information is hidden or forgotten, and, at the same time, to gather only useful information, without excessive details.

The following people within an organisation must be interviewed:

- Managers: They know the consequences of attacks for the organisation.
- Service team: They know the services provided, and the consequences of no providing them.
- Data team: They know used data, their value and the consequences of attacks on them.
- Information Systems and Operation teams: They know the systems, their history, the consequences of an incident, protection measures and new activities related to security.

7.4.2 Meetings

Meetings are aimed at gathering information from different people, making strategic decisions, communicating ideas and results and analysing needs for information.

To call a meeting, it is necessary to:

- Prepare the meeting: agenda, attendants, place, objectives, material, available time.
- Send attendants the call containing the agenda, date, start time, end time, place and attendants.
- In the beginning of the meeting, it is important to do a summary of the agenda, the objectives, and the method.
- In the end, conclusions should be drawn, agreements made and pending points determined. A date for next meeting should be set.
- The secretary, who takes notes in the meeting, should draft minutes and send them to attendants.

7.4.3 Presentations

Presentations are used by a working team to communicate advances, conclusions and results to attendants. They can be made to inform about the progress of a project, or final results.

The first step is determining the objective of the presentation, and the information to communicate. Then, it is important to decide who the lecturer is, what matter he will explain, what the duration, place and tools will be and who the audience will be.

Next, the message has to be structured to make it clear and well organised. The approach will be chosen according to the audience. Normally, the presentation is divided into introduction, background, core, review and final conclusion.

It is important to carefully select the tools: statistic data, visual tools, etc. There should not be too much, because if they are, public will not pay attention to what is said, and technic problems are more likely. Before the beginning of the presentation, all tools should be checked.

The lecturer should speak clearly and correctly, paying attention to formal aspects. Besides, he should be open to questions and comments from audience.

7.5. Delphi assessment

Delphi assessment was developed by the RAND (Research ANd Development) Corporation and used firstly for military purposes. It is a structured communication technique, based on the answers of a pannel of experts to some questionnaires, in two or more rounds. After each questionnaire, the experts' opinions and explanations are summarized in a document which is sent to all experts. In this way, they can revise their own answers after reading other opinions. The process is stopped after a pre-defined number of rounds, when a consensus is reached or when answers do not differ substantially. The average scores will be the final conclusions. This method is suitable for this analysis for these reasons:

- It is a good methodology to study, qualitatively, very complex problems.
- Experts in the subject will give their opinions on it, so the best ideas and opinions will be gathered.
- It is based on an initial scenario, which help to identify the existing situation and problems.
- It is a better methodology than simply collect individual opinions, since these opinions are confronted and a more better solution can be reached.
- As expert answers questionnaires, it is not possible that some opinions prevail over other on account of simply the expert power of persuasion or reputation.

A Delphi assessment consists of the following steps:

a) Prepare a questionnaire.

b) Deliver the questionnaire to a panel of experts in the studied subject.

c) When answers are received, a statistic study (e.g. histogram) is carried out to determine how many experts choose each option.

d) If experts choose clearly an option, this will be the solution and the process ends.

e) If there are clear differences between opinions, the same questionnaire will be sent again, along with the histogram. Experts are asked if they want to change answers or not.

f) If the results of the second round are again unclear, new questionnaires can be sent, or a meeting can be called to reach a consensus. A second round is commonly necessary, and more rounds can better solutions reached, but experts can get tired of the process. Anyway, if answers are very different, it is important to review if the question has been clearly posed, or new questions or experts should be included in the study.

Generally, a panel of experts should consist of among 15 and 35 people. More people will be called if the subject is general. The Delphi methodology has the following advantages:

- If experts think about the subject alone, it is possible that total number of ideas will be bigger than in a meeting.
- As all experts have to write answers, they think better them than if they simply talk.
- Experts answer individually, so their opinion is not influenced by other opinions (for example, experts who take an excessive leading role).
- Answers are anonymous, so experts can answer freely and do not tend to adhere to the majority opinion.
- Experts can be in different places and answer questionnaires from their workplaces.
- Experts can change or improve their views in a feedback process achieved using questionnaires.
- Experts give informed opinion, which can be different from common opinion in society.

BIBLIOGRAPHY

Johns, Lionel S. et al. (June 1990): Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage OTA Project Staff, Report OTAE-453. Washington, D.C.
www.ota.fas.org/reports/9034

Council common position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP). Official Journal of the European Communities L 344/93, 28.12.2001

Council regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.

A secure Europe in a better world European security strategy
Brussels, 12 December 2003

Dotzek, Nikolai (2003): An updated estimate of tornado occurrence in Europe. Atmospheric Research. Volumes 67-68, July-September 2003, pages 153-161. Elsevier.

Scheffers, Anja; Kelletat, Dieter (2003): Sedimentologic and geomorphologic tsunami imprints worldwide - a review. Earth-Science Reviews. Volume 63, issues1-2, October 2003, pages 83-92. Elsevier.

Farzan, F.; Mohajerani, Z.; Jafari, M.A; Wei, D.; Lu, Y. (2003). Cyber-related Risk Assessment and Critical Asset Identification within Power Grid.
http://ie.rutgers.edu/resource/research_paper/paper_11-003.pdf

Taylor, Coral; Oman, Paul; Krings, Axel (2003). Assessing Power Substation Network Security and Survivability: A Work in Progress Report. Computer Science Department, University of Idaho, Moscow, Idaho 83844.
http://cs-snake.cs.uidaho.edu/~krings/publications/SAM03.pdf

Zimmerman, Rae; Restrepo, Carlos; Dooskin, Nicole; Fraissinet, Jeremy; Hartwell, Ray; Miller, Justin, Remington, Wendy (2005): Diagnostic tools to estimate consequences of terrorism attacks against critical infrastructure. Center for Rik and Economic Analysis of Terrorism Events, University of Southern California, LA, California, draft report #05-014, May 31, 2005. pp. 66.
www.icisnyu.org/assets/.../Diagnostic_Tools_Estimate_Consequences.pdf

Green Paper of 17 November 2005 on a European Programme for Critical Infrastructure Protection
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

Leson, Joel. (September, 2005). Assessing and Managing the Terrorism Threat. Bureau of Justice Assisstance, Office of Justice Programs, U.S. Department of Justice.
https://www.ncjrs.gov/pdffiles1/bja/210680.pdf

Hołyst B., Terroryści–samobójcy, Praca przeglądowa, Uniwersytet Łódzki.

Security Guidelines for the Electricity Sector: Physical Response, NERC standard, ver. 3.0, November 2005.
www.nerc.com/files/Physical-Response.pdf

Stouffer, Keith; Falco, Joe; Kent, Karen, (September, 2006). NIST (National Institute of Standards and Technology) Special Publication 800-82 – Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security. Recommendations of the National Institute of Standards and Technology
www.cyber.st.dhs.gov/.../NIST%20Guide%20to%20Supervisory%20and

Katastrofy naturalne i cywilizacyjne. Terroryzm współczesny. Aspekty polityczne, społeczne i ekonomiczne. Pod red. M. Zuber, Wrocław 2006.
http://www.dbc.wroc.pl/dlibra/doccontent?id=3312&from=PIONIER%20DLF

Bagby, John W. (May 2006). Invited paper, The Emerging Standards War in Cyberspace Security. Financial Information Systems and Cyber Security: A Public Policy Perspective (Forum), Smith School of Business, Univ. of Maryland, College Park MD, May 24, 2006.
http://faculty.ist.psu.edu/bagby/SIG/EmergingCyberspaceSecurityStandardsWar.pdf

Wolf, Yuval; Frankel, Ofir (2007): Terrorism: Toward an overarched account and prevention with a special reference to pendulum interplay between both parties. Aggression and Violent Behaviour. Volume 12, Issue 3, May-June 2007, pages 259-279. Elsevier.

Security Guidelines for the Electricity Sector: Physical Security, NERC standard, ver. 2.0, May 2007.
www.nerc.com/files/Physical-Security.pdf

Greenberg, Michael; Mantell, Nancy; Lahr, Michael; Felder, Frank; Zimmerman, Rae (2007): Short and intermediate economic impacts of a terrorist-initiated loss of electric power: Case study of New Jersey. Energy Policy, 2007. Volume 35, issue 1, pages 722-733. Elsevier.
www.research.create.usc.edu/cgi/viewcontent.cgi?article=1079&context

Defining Terrorism, Transnational terrorism, security and the rule of the low. October 1, 2008, European Commission under the Sixth Framework Programme
www.transnationalterrorism.eu/tekst/publications/WP3%20Del%204.pdf

Dondossola, Giovanna; Szanto, Judit; Masera Marcelo; Fovino Igor Nai. (2008).Effects of Intentional Threats to Power Substation Control Systems. Int. J. Critical Infrastructures, Vol.4, Nos.1/2.

http://www.cert.fi/attachments/hvk-materiaali/automaatio/5llzxzj69/effects_of_intentional_threats _to_ power_substation.pdf

4th Benchmarking Report, on Quality of Electricity Supply 2008, Council of the European Energy Regulators, December 2008, pp. 177.
www.energy-regulator.eu

Ten, Chee-Wooi; Liu, Chen-Ching; Govindarasu, Manimaran (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. Electrical and Computer Engineering Department, Iowa State University of Science and Technology, Ames, USA.
http://vulcan.ee.iastate.edu/~gmani/personal/papers/journals/IEEE-PS-08.pdf

Bompard, Ettore; Napoli, Roberto; Xue, Fei (2009). Analysis of structural vulnerabilities in power transmission grids. International Journal of Critical Infrastructure Protection. Volume 2, Issues 1-2, May 2009, pages 5-12. Elsevier.

Jormakka ,Henryka; Koponen, Pekka; Pentikäinen, Heimo; Bartoszewicz-Burczy, Hanna (2009): Control Systems of Critical Infrastructures, Security Analysis, Energetyka, no. 4, pp. 229-236.
www.elektroenergetyka.pl/upload/file/.../elektroenergetyka_nr_09_04_3.pdf
Structure of Energy Sector Control Centers: Analysis of the Different Levels and Uses of Control Centers in the Energy System (Electricity and Natural Gas), Octavio (March 2009): Energy System Control Centers Security, an EU Approach.

Woo, Gordon (Risk Management Solutions, London, UK) (Spring 2009). Terrorism Threat Assessment and Management. Defence Against Terrorism Review. Vol.2, No. 1, pp.101-116.
http://www.coedat.nato.int/publications/datr3/06_Gordon%20Woo.pdf

Council regulation (EC) No 501/2009 of 15 June 2009 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing
Decision 2009/62/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:151:0014:0016:EN:PDF

Hoon Oh, Chang; Reuveny, Rafael (2009): Climatic natural disasters, political risk, and international trade. Faculty of Business, Brock University, Canada, Indiana University, USA. Global Environmental Change. Volume 20, Issue 2, May 2010, pages 243-254. Elsevier.

Luallen, Matt. (October, 2009). Securing a Smarter Grid: Risk Management in Power Utility Networks. SANS, sponsored by NitroSecurity.
http://www.sans.org/reading_room/analysts_program/NitroSecurity_Securing_Smarter_Grid.pdf

Akinci, Aybige; Malagnini, Luca; Sabetta, Fabio (2009): Characteristics of the strong ground motions from the 6 April 2009 L'Aquila earthquake, Italy. Soil Dynamics and Earthquake Engineering. Volume 30, Issue 5, May 2010, pages 320-335. Elsevier.

Hines, Paul; Apt, Jay; Talukdar, Salosh (2009): Large blackouts in North America: Historical trends and policy implications. Energy Policy. Volume 37, pages 5249-5259. Carnegie Mellon Electricity Industry Center.

United States Department of Homeland Security (2009). National Infrastructure Protection Plan. Partnering to enhance protection and resiliency.
www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Topft, Peter, Duero, Arash.; Bieliauskas, Arunas (2010): Terrorists targeting and energy security. Institute of Energy, JRC of EC, Petten,.Elsevier
http://ipac.kacst.edu.sa/eDoc/2010/190257_1.pdf.

Fovino, Igor Nai; Guidi, Luca; Masera, Marcelo; Stefanini, Alberto (2010): Cyber security assessment of a power plant. Electric Power System Research. Volume 81, Issue 2, February 2011, pages 518-526. Elsevier.

Protecting Against Terrorism Third Edition. Third Edition (2010). The Centre for the Protection of National Infrastructure (CPNI).
www.cpni.gov.uk/.../2010002-protecting_against_terrorism_3rd_edition

Patel, Sandip; Zaveri, Jigish (Department of Information Science & Systems, Morgan State University, Baltimore). (March 2010) A Risk-Assessment Model for Cyber Attacks on Information Systems. Journal of Computers, Vol. 5, No. 3, March 2010, pp. 352-359.
www.academypublisher.com/ojs/index.php/jcp/article/.../1591

Kim Jeong, Won; Jeong, Ok-Rang.; Kim, Chulyun; So, Jungmin (2010): The dark side of the Internet: Attacks, costs and responses. Information Systems. Volume 36, pages 675-705. Elsevier.

Jormakka, Henryka; Koponen, Pekka; Pentikäinen, Heimo; Bartoszewicz-Burczy, Hanna (2010): On managing physical and cyber threats to energy system identification and countermeasure requirements. Maintenance and Reliability no 3 (47) 2010, ISSN 1507-2711.

Gayà, Miquel (2010): Tornadoes and severe storms in Spain. Atmospheric Research. Volume 100, Issue 4, June 2011, pages 334-343. Elsevier.

Babś A., Bartoszewicz-Burczy H., Świderski J. (2011): Guidelines to classify threats and damages (physical and cyber). Net Protection CIPS project. IEN.

Renfroe, Nancy A.; Smith, Joseph L. (October, 2011). Threat Vulnerability Assessments and Risk Analysis. Applied Research Associates, Inc.
http://www.wbdg.org/resources/riskanalysis.php

Terrorism and Electric Power Delivery System (2012). National Academy of Sciences http://www.nap.edu/openbook.php?record_id=12050&page=R1

Gill, Paul (2012):Terrorist violence and the contextual, facilitative and causal qualities of group-based behaviors. Aggression and Violent Behavior. Volume 17, Issue 6, November-December 2012, pages 565-574. Elsevier.

Govindarasu, Manimaran; Hann, Adam; Sauer, Peter. (February, 2012). Cyber-Physical Systems Security for Smart Grid. Iowa State University & University of Illinois at Urbana-Champaign.
www.pserc.wisc.edu

Wilshusen, Gregory C. GAO (United States Government Accountability Office) (July, 2012). Cibersecurity Challenges in Securing the Electricity Grid.
http://www.gao.gov/assets/600/592508.pdf

Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1-Método. Madrid.
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October, 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2-Catálogo de Elementos. Madrid.
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, Secretaría de estado de Administraciones Públicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (October, 2012). MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 3-Guía de Técnicas. Madrid.
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

Mc AFFEE. (2012) Smarter Protection for the Smart Grid. Santa Clara (California).
http://www.mcafee.com/us/resources/reports/rp-smarter-protection-smart-grid.pdf

Tomaszewski, Michal; Ruszczak, Bogdan (2012): Analysis of frequency of occurrence of weather conditions favouring wet snow adhesion and accretion on overhead power lines in Poland. Cold Regions Science and Technology. Volume 85, January 2013, pages 102-108. Elsevier.

Brázdil, Rudolf.; Chromá, Kateřina; Dobrovolný, Petr; Černoch, Zbyněk (2012) : The tornado history of the Czech Lands, AD 1119–2010. Atmospheric Research. Volume 118, 15 November 2012, pages 193-204. Elsevier.

Song, Jae-Gu; Lee, Jung-Woon; Lee, Cheol-Kwon; Kwon, Kee-Choon; Lee, Dong-Young (Korea Atomic Energy Research Institute). (December 2012). A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants. Nuclear Engineering and Technology, Volume 44, No 8, December 2012, pages 919-928.
http://www.kns.org/jknsfile/v44/8_11_65.pdf?PHPSESSID=2d3b18b9d415e3c564b40853e16fe3d7

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack (Board on Energy and Environmental Systems, Division on Engineering and Physical Sciences, National Research Council of the National Academies). Terrorism and the Electric Power Delivery System. Washington D.C.2012.
http://www.nap.edu/catalog.php?record_id=12050

United States Senate Committee on Energy and Natural Resources. Full committee hearing: Cyber Security and the Grid. 2012
http://www.energy.senate.gov/public/index.cfm/2012/7/full-committee-hearing-cyber-security-and-the-grid

The Smart Grid Observer. Smart Grid Security Virtual Summit 2012. August 9, 2012
http://www.smartgridobserver.com/platform-sgs.htm

ANEX 1. LIST OF TERRORIST

Groups prepared by National Counter - terrorism Center

http://www.nctc.gov/site/other/fto.html

1. Abu Nidal Organization (ANO)
2. Abu Sayyaf Group (ASG)
3. Al-Aqsa Martyrs Brigade (AAMS)
4. Al-Shabaab
5. Ansar al-Islam (AAI)
6. Army of Islam (AOI)
7. Asbat al-Ansar
8. Aum Shinrikyo (AUM)
9. Basque Fatherland and Liberty (ETA)
10. Communist Party of the Philippines/New People's Army (CPP/NPA)
11. Continuity Irish Republican Army (CIRA)
12. Gama’a al-Islamiyya (Islamic Group)
13. HAMAS (Islamic Resistance Movement)
14. Harakat ul-Jihad-i-Islami (HUJI)
15. Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
16. Harakat ul-Mujahidin (HUM)
17. Hizballah (Party of God)
18. Islamic Jihad Group
19. Islamic Movement of Uzbekistan (IMU)
20. Jaish-e-Mohammed (JEM) (Army of Mohammed)
21. Jemaah Islamiya organization (JI)
22. Kahane Chai (Kach)
23. Kata'ib Hizballah (KH)
24. Kongra-Gel (KGK, formerly Kurdistan Workers' Party, PKK, KADEK)
25. Lashkar-e Tayyiba (LT) (Army of the Righteous)
26. Lashkar-e-Jhangvi
27. Liberation Tigers of Tamil Eelam (LTTE)
28. Libyan Islamic Fighting Group (LIFG)
29. Moroccan Islamic Combatant Group (GICM)
30. Mujahedin-e Khalq Organization (MEK)
31. National Liberation Army (ELN)
32. Palestine Liberation Front (PLF)
33. Palestinian Islamic Jihad (PIJ)
34. Popular Front for the Liberation of Palestine (PFLP)
35. PFLP-General Command (PFLP-GC)
36. Al-Qa’ida (AQ)
37. Al-Qa'ida in the Arabian Peninsula (AQAP)
38. Al-Qaida in the Islamic Maghreb (AQIM)
39. Real IRA (RIRA)

40. Revolutionary Armed Forces of Colombia (FARC)
41. Revolutionary Organization 17 November
42. Revolutionary People’s Liberation Party/Front (DHKP/C)
43. Revolutionary Struggle (RS)
44. Shining Path (Sendero Luminoso, SL)
45. Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (QJBR) (al-Qaida in Iraq) (formerly Jama'at al-Tawhid wa'al-Jihad, JTJ, al-Zarqawi Network)
46. Tehrik-e Taliban Pakistan (TTP)
47. United Self-Defense Forces of Colombia (AUC)

GROUPS AND ENTITIES from Official Journal of the European Union 16.6.2009

Source: COUNCIL REGULATION (EC) No 501/2009

1. Abu Nidal Organisation' – 'ANO' (a.k.a. 'Fatah Revolutionary Council', a.k.a. 'Arab Revolutionary Brigades', a.k.a. 'Black September', a.k.a. 'Revolutionary Organisation of Socialist Muslims')

2. Al-Aqsa Martyrs' Brigade

3. Al-Aqsa e.V.

4. Al-Takfir' and 'Al-Hijra

5. Aum Shinrikyo' (a.k.a. 'AUM', a.k.a. 'Aum Supreme Truth', a.k.a. 'Aleph')

6. Babbar Khalsa

7. Communist Party of the Philippines', including 'New People's Army' – 'NPA', Philippines, linked to SISON, Jose Maria (a.k.a Armando Liwanag, a.k.a Joma, who plays a leading role in the 'Communist Party of the Philippines', including 'NPA')

8. Gama'a al Islamiyya' (a.k.a. 'Al Gama'a al Islamiyya') ('Islamic Group' – 'IG')

9. İslami Büyük Doğu Akıncılar Cephesi' – 'IBDA C' ('Great Islamic Eastern Warriors Front')

10. Hamas', including 'Hamas Izz al Din al Qassem

11. Hizbul Mujahideen' – HM

12. Hofstadgroep

13. Holy Land Foundation for Relief and Development

14. International Sikh Youth Federation – ISYF

15. Kahane Chai' (a.k.a. 'Kach')

16. Khalistan Zindabad Force' – 'KZF'

17. Kurdistan Workers' Party – PKK, (a.k.a. 'KADEK', a.k.a. 'KONGRA GEL')

18. Liberation Tigers of Tamil Eelam – LTTE

19. Ejército de Liberación Nacional' ('National Liberation Army')

20. Palestine Liberation Front – PLF

21. Palestinian Islamic Jihad – PIJ

22. Popular Front for the Liberation of Palestine – PFLP

23. Popular Front for the Liberation of Palestine – General Command' (a.k.a. 'PFLP – General Command')

24. 'Fuerzas armadas revolucionarias de Colombia' – 'FARC' ('Revolutionary Armed Forces of Colombia')

25. 'Devrimci Halk Kurtuluş Partisi-Cephesi' – 'DHKP/C' (a.k.a. 'Devrimci Sol' ('Revolutionary Left'), a.k.a. 'Dev Sol') ('Revolutionary People's Liberation Army/Front/Party')

26. 'Sendero Luminoso' – 'SL' ('Shining Path')

27. 'Stichting Al Aqsa' (a.k.a. 'Stichting Al Aqsa Nederland', a.k.a. 'Al Aqsa Nederland')

28 'Teyrbazen Azadiya Kurdistan' – 'TAK' (a.k.a. 'Kurdistan Freedom Falcons', a.k.a. 'Kurdistan Freedom Hawks')

29. 'Autodefensas Unidas de Colombia' – 'AUC' ('United Self Defense Forces/Group of Colombia') EN L 151/16