Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung, Berlin

Critical Energy Infrastructure Protection in the Electricity and Gas Industries – Coping with Cyber Threats to Energy Control Centers

by Dr. Frank Umbach

The 21st Century Threat Environment for Companies and Governments

Although the worldwide energy industry and many governments have extensive experience with ensuring operational safety, managing natural catastrophes and prevention of damaging and disrupting energy flows, the increasing sophistication of global terrorism and the growing cyber warfare capabilities of private hackers, organized crime and terrorist groups represent new challenges of a rapidly changing global security environment. While the traditional security measures of "guns, gates and guard" are still needed, they are insufficient to cope with the new risks and threats stemming from a new and rapidly changing security environment.

During the last years, the vulnerabilities of digital systems and networks have grown exponentially, while the public awareness has not kept up with those new threats and vulnerabilities in cyberspace. But these threats have the potential to affect all sectors of private and public life, national and international businesses and even security policies of national states or multinational organizations like the OSCE. In the age-old struggle between attacker and defender, the attacker more than ever appear to have the advantages by being better armed, freely choosing the intensity of the attack as well as the target and being no longer constraint by any geographical distances and frontiers.

Those threats are challenging traditional assumptions and thinking of national as well as collective security. The emergence of botnets in particular - by implementing dormant virus, unnoticed by Internet users, which the attacker can activate at any time (Trojans) and at any place in the world - allow criminal or terrorist attackers to launch massive hostile operations for data espionage, falsifying, destroying or altering confidential data with extraordinary harmful effects in the industry as well as critical national infrastructures. By blurring the border between cyber crime, cyber terrorism, and private cyber attacks, new "unholy alliances" of crime syndicates, terrorists or nationalist movements and individuals have

increased the threat of a "digital Pearl Harbor" by conducting a new form of "asymmetric warfare" in the 21st century.

The EU Efforts since 2004

Since 2001 the EU has increasingly recognized the need for protection of critical infrastructure as an important and rising national as well as international security risk that needs to be addressed by its member states and collectively within the EU. But the progress has been hindered by the fact that the single member states have traditionally developed their own individual approaches, institutions and programmes to cope with this new security challenge to protect critical infrastructures, including critical information infrastructure (CII), despite the perceived common risks, threat, vulnerabilities and strategies for securing critical (information) infrastructure. Furthermore, the EU has only limited early warning and incident response capabilities – even on a national base of its member states. Equally European-wide governance and public-private partnerships (PPPs) are lacking.

Despite these shortcomings, a first step to address those common risks and vulnerabilities as well as to cope with the cross-border effects of damaged infrastructure or its disrupted processes has been made by establishing the "European Network and Information Security Agency (ENISA)" in 2004 to enhance European coordination on information security. A broader initiative has been made by the Commission of the European Communities at the end of 2005 by adopting a "Green Paper on a European Program for Critical Infrastructure Protection". In December 2006, the European Council adopted a"European Program for Critical Infrastructure Protection" (EPCIP) that has defined principles, processes and instruments for its implementation. The EPCIP has been the nucleus for the EPCIP Action Plan, the Critical Infra-structure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, CIP information sharing processes, a procedure for a common approach to the assessments of the needs to improve the protection of such infrastructures and the identification and analysis of interdependencies between very different critical infrastructures.

Against this background, the Commission has tendered a series of studies since the second half of 2007 under the EU's 7th Framework Program for the Commission's General Directorate for Justice, Liberty and Security (JLS) that includes studies on specific sectoral infrastructures and assets. The Octavio-Project, in which CESS was involved, had three major objectives: (1) to focus on structures, functionalities and security of critical assets (i.e. Control Centers) in electricity and gas supply systems; (2) to provide an accurate (risk) assessment regarding energy sector control centers in the natural gas and electricity sectors and their cyber structure requirements; and (3) to develop a comprehensive approach to improve the security of energy control centers based on establishing criteria and methodologies to assess, audit and mitigate risks for the EU's electricity and natural gas control centers and their interdependent ICT infrastructures.

In regard to critical energy infrastructure, the EU has recognized two major challenges:

- The spread of ICT highlights numerous new security implications of our dependencies on them in all areas of our daily life. Market liberalization and privatization of state-owned infrastructure operators as well as new regulations have made the private industry and government agencies increasingly dependent on external providers of goods and services, including commercial of the shelf (COTS)-products. At the same time, almost every

single service depends directly or indirectly on the secure supply of electricity. The physical, virtual or logical networks have grown in size and complexity. As the result of growing interdependencies between various critical infrastructures, those dependencies and impacts of supply shortages and disruptions are often not apparent until a crisis occurs and the connection breaks down. Even smaller outages, failures and disruptions can have dramatic consequences and non-anticipated cascading effects in ever more complex system between various critical infrastructures and beyond national borders ("vulnerability paradox").

- In previous times, the energy supply system was decentralized with a power plant for each region and a local distribution network, which connected the producer with the consumers. If the power plant failed, the whole region was without energy. When the regional networks were interconnected by transmission networks, security of supply was enhanced by the possibility to exchange energy between the regional networks. It also saved financial resources particularly on the side of producers. Today those regional networks have been expanded across national states, connecting individual EU member states with the perspective of creating a common, liberalized energy market in the entire EU. Whereas this is true for both electricity and gas supplies, the European pipeline-based gas supply system, perceived as the "Achilles heel" of the EU's energy supply security, covers a much wider geographical area by long distance gas pipelines, connecting producer, transit and consumer countries.

The Functionalities of Energy Control Centers and its Vulnerabilities

The operational processes of the electricity and natural gas supply chains as well as its security and control are highly dependent on the ICT infrastructure. Energy Control Centers control the operation of power plants as well as of networks. The operation of huge cross-border electricity and gas networks requires a network management and a control center hierarchy (Main, Regional and District Control Centers) to ensure security of electricity and gas supplies. The efficiency of control centers by applying methods of data handling and processing is closely linked with the development and application of ICT. Their task is:

- Measurement and information gathering by sensors – incl. satellite based surveillance and control of pipeline systems, power plants, pump stations, storage sites and networks;
- Acquisition: transmission of necessary information from the network to the Control Center transmission of commands from Command Centers to "operational" components like substations;
- Processing, display and archiving of information from the network, generation of control information.

In contrast to the former auxiliary function for the control of operations of plants and networks, meanwhile it has been transferred into a centralized complex instrument with the central function in energy supply. Without this central function, any operation within the energy and gas supply chains ranging from production to distribution and supply would be impossible. The efficiency and reliability of those Control Centers, in particular the System or Central Command and Network Control Centers, is essential and the biggest threat in case of physical and electronic attacks. They could have extensive consequences on other critical infrastructures and could also lead to heavy losses of companies at the stock exchange and ten thousands of consumers.

Acquisition and processing tasks are elements of SCADA (Supervisory Control and Data Acquisition) System. With SCADA, control centers are able to identify and repair interferences, to take the necessary measures of repair centrally and to acquire data relevant for planning and further action. Originally, each power plant had its own Control Center linked with others a part of a hierarchy of networks. The development of ICT enhanced the capability to combine not only the different tasks of command structure for the hierarchy of net-works, but also for different media, such as electricity, gas, water or district heating in a Central Command Center. The latter have extended their capabilities by using Geographical Information Systems (GIS) to provide geo-referencing information of facilities, networks, vehicles and geographical or political details. Modern SCADA systems use standard inter-faces and standard components (of computers operating under UNIX or Windows). It has improved system interconnection and efficiency, but has also increased significantly the system vulnerability to outside electronic attacks.

Outlook

In addition to the new forms of terrorist attacks, private hackers and (transnational) criminal organizations, the vulnerability of the different sectoral infrastructures have also increased because they are much more linked with each other in some way due to the rapid spread of information technologies. ICT infrastructures in the energy, transport, banking and financing sectors have become the nervous system of our modern information societies. Disruptions of ICT can multiply in other locations, branches or sectors, with an impact that extends far beyond the original area of damage as well as across the state-border of an EU-member state. Their security and resilience cannot be ensured and enhanced by purely national and uncoordinated strategies. Furthermore, market forces do not provide sufficient incentives to private operators for investing to protect critical infrastructures. The fundamental and still underestimated problem is that the low level of protection in some member states can increase the vulnerability of others, whereas, in parallel, the insufficient systematic interstate cooperation in Europe substantially reduces the effectiveness of preventive and timely countermeasures. While the Octavio project had primarily to identify the physical and cyber threats to and vulnerabilities of the energy control centers as well as other infrastructures in the electricity and gas supply chains, the presently conducted INSPIRE-project of the EU goes a step further: it aims to mitigate the threats and to improve robustness as well as resiliency of energy control centers and other Large Complex Critical Infrastructures (LCCI) by increasing safety and security of the LCCI's control systems.

When the financial and personnel resources available to operators protect their infrastructure systems are limited, both the energy industry and their governments need to use all available resources efficiently by assessing risks and setting priorities for an adequate risk management. While it is impossible to protect a utility 100% from a physical or cyber attack on a utility's facilities and infrastructure, those threats can be minimized without compromising their productivity and day-to-day operations. A professional security and risk assessment needs in a systemic perspective to address physical and cyber security, SCADA and distributed control systems (DCS), communications security, grid security, distribution security, generation security, and biological/chemical issues in new holistically integrated security concepts.

***

Remarks: Opinions expressed in this contribution are those of the author.

This analysis was published originally in: OSCE-CTN Newsletter, Special Bulletin: "Protecting Critical Energy Infrastructure from Terrorist Attacks", Vienna, January 2010, page 25 - 28. http://www.osce.org/documents/atu/2010/02/42569_en.pdf

Frank Umbach

Dr. Frank Umbach is Senior Associate for International Energy Security, Centre for European Security Strategies (CESS), Munich-Berlin

Phone: +49 173 9349189
E-Mail: umbach@cess-net.eu