ISTOCK

THE CYBER SECURITY DIMENSION OF CRITICAL ENERGY INFRASTRUCTURE

By **Vytautas Butrimas**, Chief Advisor for Cyber Security, Lithuanian Ministry of National Defense, and **Audrius Brūzga**, Director of the Energy Security Center, Lithuanian Ministry of Foreign Affairs

AMB. BRŪZGA AND MR. BUTRIMAS ARE BOTH GRADUATES OF A MARSHALL CENTER SENIOR EXECUTIVE SEMINAR. THEY HAVE JOINED FORCES TO CREATE THIS ARTICLE ABOUT ENERGY SECURITY. AMB. BRŪZGA'S WORK HAS BEEN PIVOTAL IN THE CREATION OF A NEW NATO CENTER OF EXCELLENCE IN LITHUANIA, AND MR. BUTRIMAS WAS INSTRUMENTAL IN THE PROCESS THAT LED TO THE ESTABLISHMENT OF A COMPUTER EMERGENCY RESPONSE TEAM (CERT) AT THE LITHUANIAN MINISTRY OF NATIONAL DEFENSE (MOND). HE CHAIRED THE MOND TASK FORCE THAT PREPARED THE FIRST MOND CYBER SECURITY STRATEGY IN 2009.

March 11, 2011, was a bad day in the history of critical energy infrastructure. Many were shocked and deeply moved by the earthquake and tsunami that hit the coastline of Japan resulting in great destruction and loss of life. The magnitude-9.0 earthquake also produced a perfect storm of cascading events leading to a station blackout of the nuclear power facility at Fukushima. The facility's backup power sources, consisting of the sites' other reactors, diesel backup generators, switching and control systems, and switches to Japan's national power grid, all failed after the last on-site batteries quickly drained. Nuclear plant operators had no lights on their control panels, giving them little capability to assess the situation (examine telemetry on the state of vital equipment) or to completely execute steps to protect the plant. Sensors and their links to automated safety systems failed to react to rising reactor temperatures. No power was available to operate emergency valves or coolant pumping systems.

As Fukushima personnel worked heroically to save the plant, the first analyses of Stuxnet were coming out.[1] Something troubling had appeared in cyberspace: a new and highly sophisticated form of malware capable of operating undetected while executing targeted attacks against industrial control systems resulting in destruction of

equipment. Stuxnet was a watershed event that changed the cyber security landscape.[2] This malware was programmed specifically to destroy supervisory control and data acquisition (SCADA) and programmable logic controller systems that met certain criteria. If the criteria were met, Stuxnet would then take over industrial control systems and cause the targeted equipment to malfunction and destruct. While performing the attack, it sent incorrect data to safety sensors and automated safety systems to inform that machines were running normally when they were not. Machines were being destroyed yet monitors indicated all was normal. One could not help asking the questions: Could a Stuxnet type of attack cause similar cascading failures leading to a total plant shutdown of an energy producing facility, or even a whole sector of critical infrastructure? Is plant security or critical infrastructure security just about physical security (building thicker and higher walls, raising backup generators higher above sea level, etc.),[3] or is there a significant cyber dimension that must be taken into account? Does the energy sector form part of a nation's critical infrastructure? If so, is a cyber attack on this infrastructure also a threat to national security? This article aims to explore these questions and propose solutions to reduce the risk of a "Cyber Fukushima" event in the energy sector.

THE SHAPE OF THE CYBER THREAT

International experts[4] and opinion leaders[5] in the Industrial Control Systems (ICS) field have sought answers to these questions, along with four operators in Lithuania's energy sector (two electrical grid operators, LITGRID and LESTO, the national natural gas pipeline Lietuvos Dujos and the Center for Technology and Innovation). Regarding the question of cyber security and the appearance of Stuxnet type malware, operators responded that since their control and data networks were isolated from the Internet they did not see this as a serious or imminent threat. When it was suggested that a malware attack like Stuxnet could use internal and isolated networks (via USB sticks or maintenance/engineering personnel with laptops, not to mention disgruntled employees using insider knowledge), they paused to think. They corrected themselves by adding that attacks were possible but downplayed the threat. Preparing for such an attack would require a great deal of detailed information that energy operators do not openly make available.[6]

The next question concerned interdependence. Were their operations reliant upon the health of other national critical infrastructures? The answer was yes. Both the electrical and natural gas pipeline operators depend to some extent on the telecommunications sector for their control and data networks. A failure of telecommunications would affect their ability to control and manage systems remotely. In addition, the natural gas operator's equipment was dependent on electricity from the national and regional power grid. Electrical failure would affect pipeline operations.

It also slowly became clear that the information technology and ICS worlds looked at cyber security differently. For example, an IT security person believes in strong password policies. Passwords must be complex, securely protected from disclosure and changed periodically. The goal is to ensure confidentiality, integrity and availability of information. ICS security priorities are nearly the opposite. Availability is the top priority, followed by integrity and confidentiality. ICS need to be available, reliable and safe. The priority for ICS was availability of critical processes and services. In an emergency, a critical infrastructure operator needs to respond quickly to ensure that critical processes and vital services continue without interruption or damage and loss of life. Default passwords are often used and they are even hard-wired into the system. In the ICS world, an operator trying to access a particular black box (program logic controller that is part of a very large SCADA system) does not, in a moment of crisis – if telemetry tells the operator that pressure, temperature or spin rates are beyond accepted norms – have time to waste searching for a password. ICS systems were not initially designed with the kind of security that IT security practitioners have in mind. They were designed with minimal hardware requirements (weak CPU's, low memory, and low bandwidth, simpler protocols) to safely and reliably perform simple automated tasks. Few ICS designers assumed that one day the networked Wintel (Microsoft Windows/Intel based computers) world of IT security specialists and the bad guys, who try to attack them, would someday enter their "world."

Furthermore, unintentional incidents can occur from poorly thought out applications of IT security policies on ICS.[7] Such applications can actually cause denial of services or damage to critical systems because of a lack of advanced testing and understanding of the effects of implementing IT security policies on very large and complex systems. In fact, it may be that in the ICS world there are more unintentional or accidental cyber incidents than intentional ones. This is a very complex and difficult issue to understand and address if one relies solely on IT specialist expertise without consulting ICS specialists.[8] One must remember, regardless of how these incidents happen, a potential attacker can use this knowledge with the intention of preparing and executing an attack.

THE EU PERSPECTIVE

As can be seen by visits to Lithuanian electrical and natural gas pipeline operators, a clear need to address the cyber dimension of critical energy infrastructure (CEI) protection has emerged. If European Union member states are to become more widely interconnected through increased market liberalization (particularly in the electricity and gas sectors), privatization of state-owned infrastructure operators and the emergence of new regulations, their critical energy infrastructures must be able to continue to function under severe conditions, since their breakdown could have catastrophic consequences for other EU nations. The November 4, 2006, electricity blackout in Germany provides an illustration. The blackout started in Germany but ended up affecting 11 countries, including Austria, Belgium, France, the Netherlands, Portugal, Spain and Morocco. In total, 15 million people were affected for three days. If the

potential problem is ignored, a cyber-caused, Fukushima-like disaster affecting various countries in Europe and its neighborhood is possible. It has become clear that increased European interdependency, resulting from cross-linking energy networks and infrastructure, has inevitably led to higher vulnerability for the entire energy system. And given the high dependence on the telecommunications sector for operational processes, control, data and security, the growing cyber dimension of CEI must be given priority.

CEI broadly includes the production, storage, refining, processing and distribution of fossil fuels. But what exactly constitutes critical energy infrastructure in the EU? Although it varies within different member states and its protection falls under national jurisdictions, the European Commission (EC) has defined critical infrastructure as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[9] If the disruption or destruction of this kind of critical infrastructure would have a significant impact on at least two member states, it is referred to as "European critical infrastructure."[10] The EC Directive that includes these definitions specifically concentrates on the energy and transport sectors, the former addressing the extraction, storage, pipelines and dispatching centers associated with gas and oil, as well as power plants, transmission and distribution networks, dispatching centers, nuclear fuel cycles and hydroelectric power associated with electricity generation and transmission.

NATURAL GAS

But most vulnerable to cyber threats is the European natural gas supply chain, since it is overwhelmingly based on inflexible pipeline systems (which create dependencies, risks and vulnerabilities as seen during the Ukrainian gas crises of 2006 and 2009, the last of which affected 18 European countries).[11] The increasing number of gas interconnection systems, and their dependence on ICT systems to support control centers, compressor stations, storage sites, metering stations, pressure control systems and export stations, makes them especially vulnerable. To quote Frank Umbach and Uwe Nerlich on gas supplies: "asset security in pipeline systems is an important requirement, in many cases much more so than protection of pipes themselves [...] effective control centers and other critical assets remain an indispensable means of crisis management."[12]

The EU has taken some steps at the national and EU-level to protect CEI. The first legal instrument on the subject of critical infrastructure protection was the 2008 European Council Directive on the identification and designation of European critical infrastructure and the assessment of the need to improve its protection. The European Commission Directorate-General for Energy also established a network of critical energy infrastructure operators from the electricity, gas and oil sectors (the TNCEIP Network) to exchange experience on security-related issues. The most significant effort in CEI protection, however, has been the 2006 European Commission Program for Critical Infrastructure Protection, which established the framework for protecting critical infrastructure – be it national or European – in the EU, and led to the 2008 directive. The overall challenges to critical infrastructure in the EU are identified as:[13] The growing links between critical infrastructures (namely energy infrastructure and information and communication infrastructure), which can lead to dependencies and risks that might not be apparent until a crisis occurs; and the expansion of regional networks across national boundaries, which leads to increased vulnerabilities of the entire system.

NATO

NATO Secretary-General Anders Fogh Rasmussen meets with President of Lithuania Dalia Grybauskaite in January 2012. Vilnius, Lithuania, will be the site of new NATO Energy Security Centre of Excellence.

THE SCOPE OF THE THREAT

Is there a credible cyber threat to energy infrastructure? Though rare, and even more rarely publicized for obvious reasons, incidents of cyber attacks on energy infrastructure have occurred.[14] Russian hackers apparently attacked a nuclear power plant near St. Petersburg in May 2008. Although plant operations were unaffected, its website was taken offline inhibiting communication between the plant and Rosatom (the state nuclear corporation) for several hours. Simultaneously, rumors of "radioactive emissions" were circulated, causing panic among nearby residents. There is also evidence of a concerted attack by Russian hackers on Georgian government websites in August of 2008, accompanying the military attacks that followed. The cyber attacks infiltrated the Baku-Tbilisi-Ceyhan pipeline, but did not disrupt the flow of gas. They did, however, signal Russian willingness to use cyber warfare to achieve its goals. The CIA has numerous reports of incidents that have been attributed to cyber attacks. Although these reports do not name any specific countries, the power outages in Brazil in 2005, 2007 and 2009 seem to point to disruptions in SCADA systems achieved through hostile intrusion via the Internet.

THE ASSOCIATED PRESS

A view of the No. 4 reactor building at the Fukushima nuclear power plant in May 2012

Furthermore, evidence of cyber spies infiltrating U.S. electrical grids has surfaced. In theory, the software left behind in the process could disrupt the flow of electricity.

To fight cyber security threats, it is necessary to evaluate the threat level, possible losses, chances of a breach and other parameters crucial to preventative or response measures. Furthermore, operative security of any activity – including that of critical energy infrastructure – depends on information and cyber security. On the national level, the U.S. has paid an increasing amount of attention to neutralizing cyber threats and has employed rather effective response mechanisms to do so. In 2009, the U.S. Cyber Command was created; its mission to defend the information security environment and protect the country from external cyber attacks. The U.S. Center for Strategic and International Studies has also established a Commission on Cyber Security to advise the president on the creation and maintenance of a comprehensive cyber security strategy. Furthermore, the White House has assigned an official to the National Security Council responsible for coordinating the country's activities in the field of cyber security.

NATO'S VIEWS

In NATO, cyber defense and energy security both belong to the Emerging Security Challenges Division. During the recent Chicago Summit, NATO reaffirmed its commitments to the cyber defense initiatives it agreed to at the Lisbon Summit – namely, the Cyber Defense Concept, Policy, and Action Plan. NATO has also undertaken steps to provide the required resources and reforms necessary to bring all the critical elements of NATO bodies under centralized cyber protection. Along these lines, the NATO Computer Incident Response Capability Full Operational Capability, including protection of most sites and users, should be in place by the end of 2012. NATO has also set out to develop its ability to prevent, detect, defend against and recover from cyber attacks by "further [integrating] cyber defense measures into Alliance structures and procedures and, as individual nations, [remaining] committed to identifying and delivering national cyber defense capabilities that strengthen Alliance collaboration and interoperability, including through NATO defense planning processes."[15] Along with the EU, the Council of Europe, the UN, and the Organization for Security and Co-operation in Europe, the Cooperative Cyber Defense Centre of Excellence in Estonia is listed as a relevant partner in addressing growing cyber security threats.

In terms of energy security, NATO noted in its Chicago Summit Declaration that, while issues pertaining to this sector are primarily the responsibility of national governments and international organizations, NATO will continue to "integrate, as appropriate, energy security considerations in NATO's policies and activities." The Alliance expressed support for the establishment of a NATO-accredited Energy Security Centre of Excellence in Lithuania, reflecting the growing importance of the field. The fact that both the NATO Energy Security Centre and the Cooperative Cyber Defense Centre of Excellence are located in the Baltic Sea region points towards the emergence of regional expertise. The contribution of the Baltic states to training and education could be instrumental in addressing the growing cyber dimension of critical energy infrastructure protection in Europe and employing the idea behind NATO's Smart Defense concept. These centers could develop best practices by providing doctrines and

THE ASSOCIATED PRESS

The 1999 Olympic Pipeline accident in the United States was caused in part by misapplication of IT security on an Industrial Control System.

concepts for the Alliance in this emerging field; hosting and conducting training for NATO countries, courses, and exercises; conducting research and development activities; studying past or ongoing attacks and drawing up lessons learned; and providing advice during ongoing attacks.[16]

NATO's Industrial Resources and Communication Services Group (IRCSG) has also carried out reports on the protection of critical energy infrastructure in electricity, gas and oil sectors and offered best practices and recommendations. A Draft Concept Paper on Energy CIP was created in 2011.

CONCLUSIONS

Cyber attacks or unintentional incidents inside CEI, while difficult to diagnose and expose, are likely to have been visible and consequential. One can conclude that cyber threats are an issue for ICS, on whose foundations rest our critical energy infrastructures. A cyber security incident can occur unintentionally[17] because of a lack of information about the system and the unintended consequences of initiating a new process or implementing poorly thought out IT security policy. Knowledgeable attackers can intentionally cause the same to occur. Both possibilities can lead to major cascading failures in critical infrastructure resulting in danger to national security.

What can be done to reduce the risks of cyber incidents or cyber attacks on CEI? First, attention to physical security of sites and equipment is not enough. A Fukushima disaster variant could have been achieved with a Stuxnet style attack, yet in preliminary reports about Fukushima there is little mention of any cyber security recommendations.[18] Second, risk needs to be understood with an appreciation for the peculiarities in security practices found in the IT and ICS realms. IT and ICS security practitioners need to formulate policies to address risks and threats and those policies must be approved by management. The bottom line is that time and effort must be dedicated to training system designers in IT, cyber security and engineering.

At the national level, IT and ICS security professionals and operators (both public and private) need to start discussing the way ahead. Vulnerabilities need to be understood, dependencies recognized and effective measures developed to reduce the risk of accidental and intentional actions leading to major failures in critical infrastructures.[19] Few incidents are analyzed and made public. Awareness should be increased and a better business case built to encourage security professionals to take steps to secure ICS. In addition to Computer Emergency Response Teams (CERT) for the IT world, there also needs to be a CERT for the ICS[20] world that would collect (with confidentiality assured) information about incidents and distribute analyses and data to ICS managers. With this information, a business case for investing in training and security equipment designed for the particular requirements of ICS can be made.

International cooperation is key to reducing risks from cyber threats. Much attention is being given to combating cyber crime and terrorists' use of the Internet. However, very little has been accomplished in restraining states from taking advantage of the "cloak of invisibility" cyberspace provides for engaging in malicious cyber activities against critical infrastructures of other states. There is no room in this article to discuss how these activities could affect international relations.[21] However, states should consider taking action on concerns in their common interest:

- Agreements to refrain from directing malicious cyber activities (MCA) at CEI[22] of other states.
- Agreements for states to take some responsibility for acting on reported MCAs in their cyber jurisdictions.
- Agreements to set up a coalition of willing institutions and experts to monitor, analyze and report on violations of the first two agreements.

The importance of exercises to test procedures, resilience and robustness of systems cannot be overstated. In recognition of the cyber threat to critical infrastructure, NATO for the first time will combine its traditional crisis management exercise (CMX 12) with its cyber exercise (Cyber Coalition 12). One of the scenarios will be a cyber attack against critical infrastructure. In addition to international exercises, it may be even more important for nations to conduct national exercises to discover capabilities and shortcomings.[23]

In trying to comprehend cyberspace, several models or paradigms have been used. At first (late 1980s and late 1990s), medicine and history seemed to be a good model (viruses and use of anti-virus software to ensure immunity from Trojan horses). Later (early 2000s), horror movie terminology was popular. New words appeared such as "zombie" computer and robot networks, or "botnets." In 2007, military terminology entered the vocabulary. During a NATO meeting,[24] an Estonian announced to the audience that his country was under [cyber] "attack." The arrival of Stuxnet took the military tack further with talk of cyber "weapons." Today, this issue is even more complicated and

REUTERS

A view of the Gazelle high-pressure pipeline station in Brandov, Czech Republic, which helps diversify Europe's natural gas supply

perhaps "religion" could be of help. Speakers at cyber security conferences have introduced themselves as cyber security "evangelists." There are cyber war "true believers" and cyber war "skeptics." There are even different "doctrines" of thought, especially regarding "attribution" and the usefulness of treaties. Sometimes, when one speaks about cyber security to an audience, one can appreciate what it must have been like to have been a Christian missionary speaking to a pagan audience about why it should take this new "unseen power" seriously.

Regardless of terminology, this is a critical time for leaders and citizens to reach an understanding of the threats emerging in cyberspace, for the threat to critical energy infrastructure concerns us all. We need to understand this if we are to make any headway in fostering consensus among ourselves and nations for reducing threats represented by this new unsettling trend. □

1. For a more detailed analysis of STUXNET see: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html
2. "An Unsettling Trend," *per Concordiam*, Vol. 2, Issue 2; pp. 10-15.
3. Steps suggested after early analysis of Fukushima disaster by TEPCO: http://www.tepco.co.jp/en/press/corp-com/release/betu11_e/images/111202e13.pdf
4. Special thanks to the ICS industry professionals and readers of the SCADSEC newsletter. For more information on this and other critical infrastructure newsletters see: http://news.infracritical.com/mailman/listinfo or specifically about SCADASEC see: http://news.infracritical.com/mailman/listinfo/scadasec
5. Special thanks to Joseph Weiss (for graciously answering a phone call from Vilnius nine time zones away), Jacob Brodsky, Bob Radvanovsky and Joe St. Sauver.
6. Much industrial control system information such as the default passwords of equipment is available online. Even the US-CERT working to protect these systems publishes this information. Look at: http://www.kb.cert.org/vuls/id/889195 or http://arstechnica.com/business/news/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems.ars
7. A good report to read on the San Diego blackout of 2011 http://www.ferc.gov/D791C849-C62F-495A-90B2-2B63F0D10C78/ForceRequestingFullContent/D791C849-C62F-495A-90B2-2B63F0D10C78/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf
8. See Joseph Weiss's book, *Protecting Industrial Control Systems from Electronic Threats*, 2010, Momentum Press at http://www.momentumpress.net/authors/joe-weiss
9. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
10. Ibid.
11. http://www.reuters.com/article/2009/01/07/uk-russia-ukraine-gas-factbox-idUKTRE5062Q520090107?sp=true
12. Umbach, Frank and Uwe Nerlich. "Asset Criticality in European Gas Pipeline Systems – Increasing Challenges for NATO, its Member States and Industrial Protection of Critical Energy Infrastructure" in *Energy Security: International and Local Issues, Theoretical Perspectives, and Critical Energy Infrastructures (NATO Science for Peace and Security Series C: Environmental Security)*.
13. Ibid.
14. All examples are listed in the SAFE Intelligence Report of January 2010. http://www.secureenergy.org/sites/default/files/1111_SAFEIntelligenceReport3120100120.pdf
15. Chicago Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. Press Release (2012) 062, Issued on 20 May 2012.
16. Based on Lord Jopling's recommendations: 157 CDS 08 E rev 1 - Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures. http://www.nato-pa.int/default.asp?SHORTCUT=1478
17. Human errors in following procedures, lack of training, poorly programed automated safety equipment, and not looking at the control panels at the right time led to a major power failure in the US in September 2011. http://www.nytimes.com/2012/05/02/science/earth/power-failure-in-west-is-tied-to-combination-of-errors.html?_r=1
18. For example, no mention of cyber precautions in TEPCO interim report https://netfiles.uiuc.edu/mragheb/www/NPRE%20402%20ME%20405%20Nuclear%20Power%20Engineering/Fukushima%20Earthquake%20and%20Tsunami%20Station%20Blackout%20Accident.pdf and http://www.tepco.co.jp/en/press/corp-com/release/betu11_e/images/111202e13.pdf
19. Two excellent works on this topic are Joseph Weiss's *Protecting Industrial Control Systems from Electronic Threats* and Ralph Langner's *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*.
20. The US has already done this http://www.us-cert.gov/control_systems/ics-cert/
21. Discussed in depth at http://www.ted.com/talks/guy_philippe_goldstein_how_cyber-attacks_threaten_real_world_peace.html
22. Worth to consider adding to the list to include not only CEI but financial and telecommunications infrastructures.
23. If anything, exercises should point out who is in charge, who do you call, and who needs to participate in responding.
24. Witnessed this myself at a NATO Cybersecurity Workshop held at Microsoft in Redmond, Washington, late April 2007 – V.Butrimas.