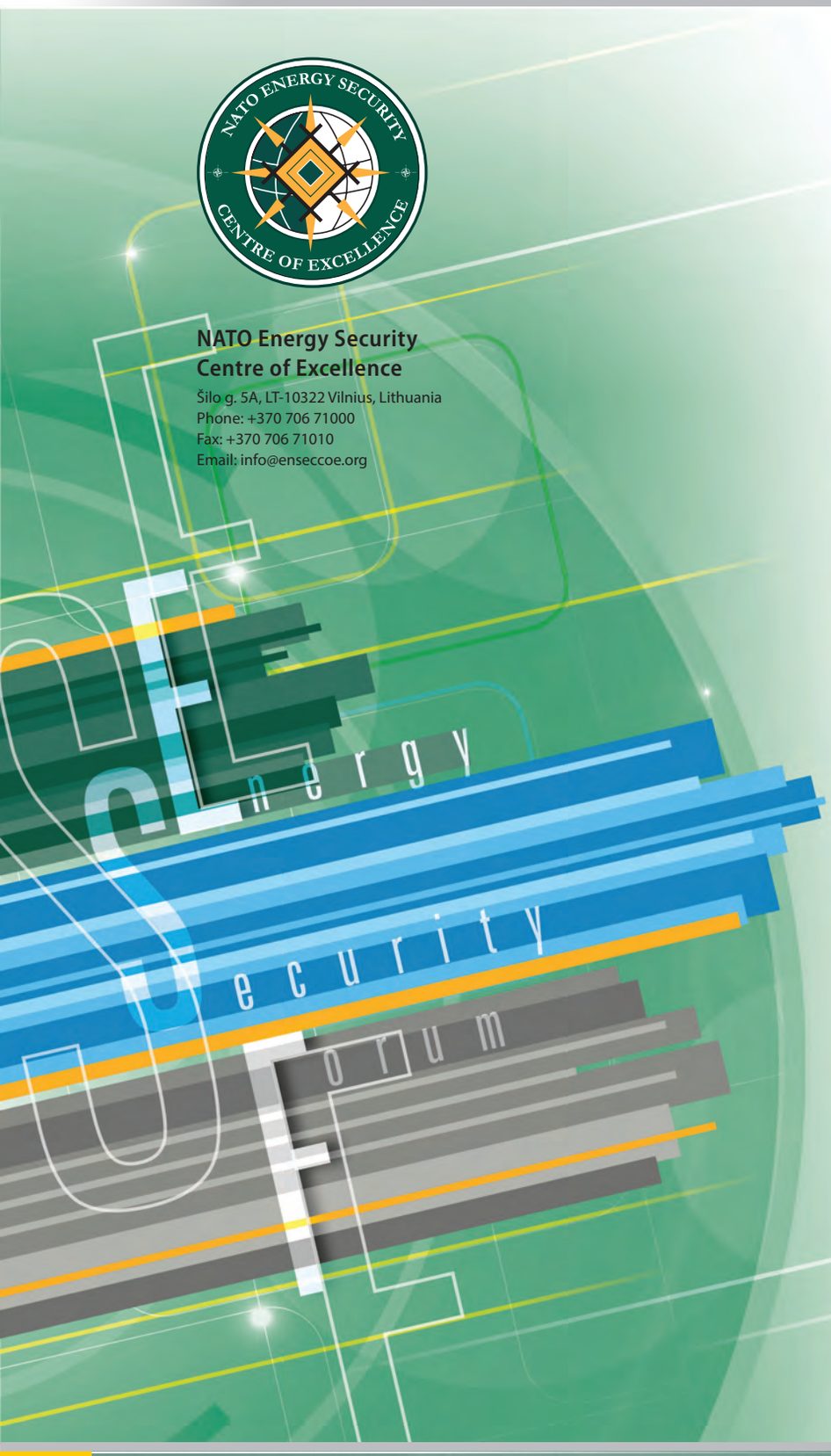
Energy Security Forum

Journal • No 8 • December 2013 ISSN 2335-2272



NATO Energy Security Centre of Excellence
Šilo g. 5A, LT-10322 Vilnius, Lithuania
Phone: +370 706 71000
Fax: +370 706 71010
Email: info@enseccoe.org

CONTENS

Editorial

Dr. Arūnas Molis

Head of Strategic analysis
and research division
NATO ENSEC COE

The topic which we have chosen for the eighth volume of the "Energy Security Forum" attracted an interest of some really recognized experts in the field. This awarded us with the possibility to publish the most extensive issue of the journal which this time includes seven articles. All of them explore one major dilemma: how to find a balance between the need to protect critical energy infrastructure objects and a fear to lose important classified information if this is done not by the owners of this infrastructure?

This question is not a trivial one. In the time then everyday life is becoming more and more complex and sophisticated, everything and everybody need power in order to work, to recharge or stay connected. And the success in securing the necessary amount of energy resources depends not only on the reliability of supplier or the costs of the raw materials. It is also influenced by availability of the properly protected energy infrastructure. Increasing amounts of human and financial resources which are invested into the protection of the critical energy infrastructure demonstrate that challenge is well understood on the both sides of Atlantic. For instance, in Presidential Directive PPD-21, the Obama administration identified energy and communications systems as uniquely critical due to the enabling function they provide across all critical infrastructure sectors. The European Program for Critical Infrastructure Protection (EPCIP) has also its main focus on energy infrastructure protection.

Major problem in this context is obvious: most of the energy infrastructure objects are owned and run by private companies, which in many cases struggle alone for the security of their property. They combat threats in order to build more resilient infrastructure defence but do it chaotically. Risks in many cases appear to be similar from one object to another; therefore joint efforts could provide much better effect. However, companies are not always keen to share information about the attacks – neither the fact that they happened nor details on what type of attack it was and how serious was the damage. In this context the added value of the public-private partnership is overlooked: despite the facts that private companies do not have enough means or resources and the governments have. Thus, potential for cooperation is there, what is needed to explore it properly?

Dr. Frank Umbach, European Center for Energy and Resource Security (EUCERS), Department of War studies, King's College, London, explains, why there's a real need to change the corporate security cultures, concerning the cyber security information sharing. He explains, how modern society, which becomes more and more reliant on electrical grid and internet connection, becomes more vulnerable from this dependence. As internet connection is reliant on electrical connection, as is the energy system reliant on communications. In last year`s we have seen dramatic increase in cyber-attacks, among others, to energy grid control system. The explanation is enforced with several stricking examples, where private companies have failed to give timely information from being attacked and breached by cyber attackers. Thus, with the encouragement from the government, the only way for the companies to survive in the new security environment, is to start collaboration among each other, and sharing their experience with the public sector.

Dr. Kevin Rosner, Institute for the Analysis of Global Security, U.S., in he's article explains the need for enhanced information sharing between private companies, but stresses that weather the information sharing between companies and public sector is mandatory or voluntary, more important is weather the companies understand the value of received information and have the capability to enforce necessary changes. He also stresses, that private companies might resist the mandatory regulations, meaning regulatory policies and enhances security measures, but as these companies are providing services, that are critical for society and essential for other infrastructures, and thus, their capability to provide these services is not only their private matter, but a public Interest. Thus, the governments must provide secure platform for information sharing in exchange to the private companies that provide the information.

Dr. Sijbren de Jong, the Hague Centre for Strategic Studies, Netherlands, takes an old and much discussed matter, witch the 2006 and 2009 Russian-Ukrainian gas dispute is, and puts it into new light. As it comes out, the stress on gas consumers would have been remarkably lighter, if the regulators would have had better overview of the gas reserves and technical parameters in European grid. Also, great benefit would have been, if the emergency plans of countries would have been better coordinated. All in all, he concludes: „if there is one thing the Russian-Ukraine crises have served to demonstrate, it is the security risks of having differing legal and regulatory standards along vital energy transit corridors".

Ernie Hayden, CISSP CEH, *Securicon* LLC, U.S. recognizes that improving information sharing is not going to be a simple remedy, as there are several obstacles to sharing, naming only few which are legal, financial, reputational and etc. But he emphasis that nevertheless the information sharing is not as effective as it should be, due to the obstacles named before, there are number of good practices already in work that have overcome these barriers and, and in future, will even more improve the situation. The main theme of his article, is that firstly, the trust should be established between the parties and secondly, make the information flow both ways.

Dr. Jennifer Giroux and Laura Melkunaite, Risk & Resilience Team in Center for Security Studies (CSS) in Zurich, Switzerland – in their article point out several new aspects to consider. Even, if the infrastructure companies are interested in information sharing, they might lack the channel to do that in secure way. It is a concern, that the level of attention given to the subject is different from country to country. While some countries have heavily invested in establishing agencies and public-private partnership platforms to exchange information, monitor and/or report incidents, other countries have yet to take these steps. To sum up, there are several good examples of Information sharing from countries, where the subject is under high attention.

Dr. Jürgo-Sören Preden, Laboratory for Proactive Technologies in Department of Computer Control, Faculty of Information Technology in Tallinn University of Technology, Estonia, – explains, how sufficient information, from all of the sectors of critical infrastructure, are needed, in order to provide adequate platform, for action for mitigating the critical situations. Considering the right of companies to their confidential information, he suggests several technologies that can be used for sharing sensitive information, without revealing unnecessary information to any of the parties. And what's more, his suggestions also provide enhanced cyber security for the information sharing platforms, in order to keep third parties, with evil intentions, away from the information.

Katerina Oskarsson, Civil-Military Fusion Centre (CFC) in NATO Allied Command Operations (ACO), Norfolk, U.S. – supports the importance of information sharing between private and public institutions, but brings out that usually private companies meet the public requirements in information sharing and protection requirements. Nevertheless, usually the private companies` unwillingness to do so is common belief, it is the public sector, that's unwillingness to share their information with the private sector, is of most concern. The majority of private companies point out, that they do not receive the information they need from the public authorities, and developing the capability of public sector in information sharing, is what we need to promote in order to enhance infrastructure protection.

Commercial Confidentiality: An Obstacle to Effective Mitigation to Cyber Attacks of Critical Energy Infrastructures?[1]

Dr. Frank Umbach

European Center for Energy and Resource Security (EUCERS), Department of War studies, King's College, London

While the present US spying efforts have caused a new transatlantic crisis and are threatening the political trust between the Transatlantic allies, the European public discussions focus on the political anger, new measures to counter US spying efforts and the need of a EU-US privacy pact for data protection as well as new ways to ensure "transparency" with the US.

The present European public discussions, however, overlook the real risks of cyber-attacks of foreign countries, terrorist groups and transnational crime groups for widespread industrial espionage. According to new estimates from anti-virus producers, McAfee and Symantec, cyber-crime victims worldwide lose between US$381–987 billion (290-750 billion euros) a year.

These discussions also ignore the rapidly changing cyber threat environment with rising cyber threats against critical (energy) infrastructures. Those targeted cyber-attacks are considered as the most dangerous because all critical infrastructures depend on a stable supply of electricity. Critical infrastructures (CI) include information systems, telecommunications, the transport and traffic sectors, energy supply, healthcare, financial services and other sensitive services. Security experts consider "critical infrastructures" to be at particular strategic risk, as these are essential for a state's survival and to sustain vital state functions.

While cyber security consciousness has grown worldwide along with the industry, the consciousness and even less the cyber security defences have still not kept pace with either the sophistication of embedded technologies or the capabilities of many attackers. The founding principles of the internet – namely interoperability, openness, and neutrality – are fast to develop, but they have become at the same time an increasing economic, political, and geostrategic risk, with an ever increasing dependence on stable and reliable electricity supplies. But without electricity, industrialised countries are thrown back into the Stone Age.

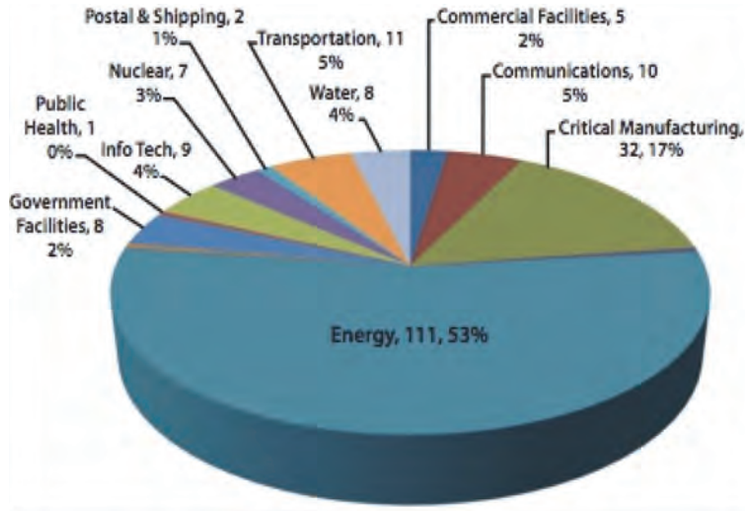


Figure: Growing Cyber Attacks on US Critical Infrastructures (First Half Year of 2013)

Source: US-Department for Homeland Security

[1] This analysis is based on a series of articles and a dossier published in the spring and summer of 2013 and being available by the Geopolitical Information Service AG (www.geopolitical-info.com) - see: Frank Umbach, Cyber Security (GIS: Liechtenstein, August 2013) as well as the author's presentation "Threats, Vulnerabilities and Building Resilience: Focus Cyber Protection of Critical Energy Infrastructures" at the NATO-Azerbaijan Expert Seminar: Energy Infrastructure Protection Informal Working Group within the Partnership Action Plan on Terrorism (PAP-T), NATO-Headquarter, Brussels, 25 June 2013.

In order to cope more successfully with the new cyber threats, the effectiveness depends on the quality of the newly created public-private partnerships (PPPs) between governmental institutions responsible for IT-security and cyber security and the private sector – in particular also industry (i.e. energy companies). These PPPs are needed as more than 80% of the CIs belong to the private sector. Within these PPPs, trust, confidence and transparency are preconditions for a close cooperation and effective mitigation strategies against the newly emerging cyber threats against critical infrastructures. But these preconditions conflict with the traditional understanding of confidentiality and corporate security cultures existing in both governmental institutions and companies.

In the EU, only 26 per cent of enterprises in the EU had a formally defined ICT security policy in January 2012. But the growing integration of national energy markets, especially for electricity, has created a whole series of new dependencies and vulnerabilities that could result in a domino effect across very larger geographical regions in the event of a major power cut.

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Figure: ENISA-Emerging Cyber Threat Landscape (2012)
Source: ENISA 2012

In response to the growing threats in cyber space, the European Commission has issued a draft directive to the 27 Member States as part of its first strategy, announced in February this year, to combat cyber threats. The aim of the directive is to establish a common level of network and information security (NIS) throughout the EU. Member countries will have 18 months to incorporate the directive into their national laws.

At the center of the internal debate within the EU on cyber-crimes is the question of whether reporting cyber-attacks should be voluntary or compulsory, particularly for CI such as transport networks, telecommunications and energy systems which are vital for the working life of developed nations. The German Ministry of the Interior, for instance, is also planning an IT Security Bill to implement a regulation requiring that significant cyber-attacks be reported by businesses, but it is based on the willingness of the corporate sector. But it is questionable whether the non-mandatory reporting will be sufficient in generating a sufficient situation picture for the EU governments and the EU Commission to cope with future cyber threats to governments and the corporate sector.

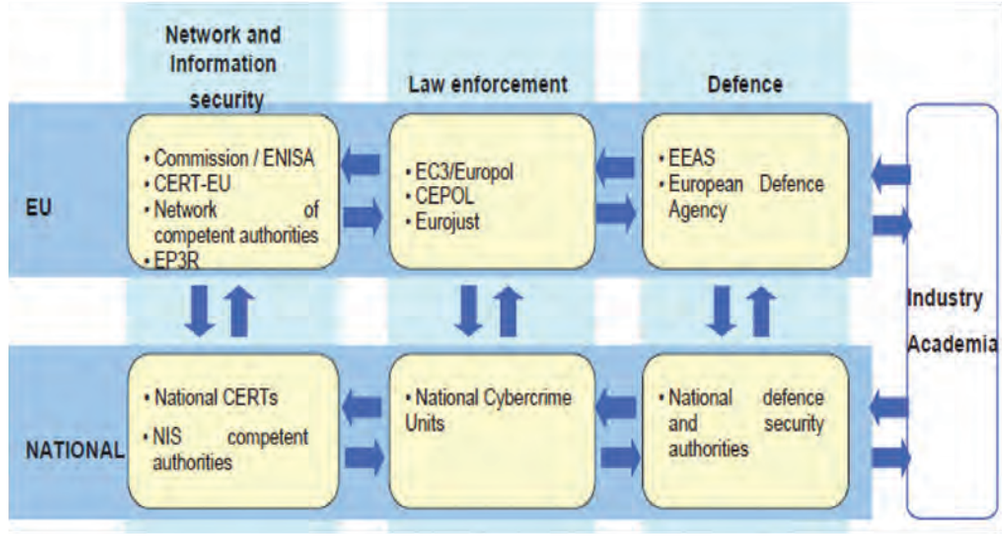


Figure: The EU's New Cyber-Security Strategy: Coordination between NIS Competent Authorities/CERTs, Law Enforcement and Defence

Source: European Commission, Cyber-Security Strategy, 2013

The Newly Emerging Cyber Threat Environment towards Critical Infrastructures

In December 2012, the German power utility 50Hertz, which specializes in the use and integration renewable energy, admitted that it had faced a serious cyber-attack two weeks prior that lasted five days. The "Denial of Service" (DOS) attack with a botnet behind it blocked the company's internet domains so that in the first hours of the attack, all email and connectivity via the internet was blocked. It was the first confirmed assault against a European grid operator. While the electricity supplies had not been affected, the company's CEO reassured, the confirmed attack comes at a very critical time of the German energy transformation.

All critical infrastructures in modern industrial societies are increasingly integrated and inter-linked by two things: electricity and the internet. Any longer term disruption to electricity and/or the internet would mean that a country could lose essential services such as energy and water supply and thus could no longer guarantee the functioning of its critical infrastructures. The more an industrialized society and its critical infrastructures are linked by the internet, the greater its vulnerability and the potential risks it faces.

A result of the growing mutual dependency between different critical infrastructures, the dependency and consequences of supply bottlenecks and disruptions are generally not obvious as long as a crisis does not hit causing a total collapse in supply. However, even smaller power fluctuations, outages and interruptions can have dramatic cascading and even transnational effects that cannot always be predicted as systems become ever more complex.

The vulnerability of the electricity sector to even large scale and transnational power cuts could further increase in the future as new security concepts and technologies to protect the power grids and to make them more robust are not being developed fast enough. The introduction of smart grid and smart metering technologies is the next major shift in energy policy, especially in the electricity sector. Smart grid technologies use intelligent electricity transmission and distribution systems to provide a constant digital exchange of energy and information. These intelligent metering systems and networks that serve as distribution and end points for communication and sensor nodes are in fact automated minicomputers. However, in Europe and the USA, today's first generation of smart grid technologies have not been developed with inherent safety and security requirements in mind. It is only now that these security standards are beginning to be defined, developed and introduced.

As a result of the introduction and proliferation of these new key technologies, the number of linkages between ever larger networks and the regular internet will increase dramatically due to the widespread introduction of wireless networks, cloud computing and the extended use of commodity IT platforms such as smart home and smart grids (intelligent networks). It could put power supply and management systems at greater risk than ever before as the increasing

number of these internet contact points will dramatically increase the system's vulnerability, but without the kind of overall system robustness and resilience that existed in the past.

In the light of this, if security is not being addressed for CEI with a sense of urgency alongside the introduction new energy technologies, an increasingly automated energy system and electricity grid in particular may turn into an invitation to disaster. But tighter regulation and compliance does not on its own lead automatically to tighter and enhanced security against cyber threats.

At the same time, extortion globally, more than espionage and sabotage, has become the most prevalent cyber threat to the global energy sector, as criminals break into utilities, gaining access to the utility's system and demand a ransom in exchange for not causing any damage. The amount of ransom has climbed to hundreds of millions of dollars. Reportedly, one in four power companies worldwide have already become victims of those extortions. In some countries, extortion attempts are even higher, with 80% in Mexico and 60% in India in analysis by IT security companies.

The threat will be even greater, as the discussion to anticipate risks and develop adequate protective measures will not have been completed, whereas the emerging threat landscape is becoming more multifaceted by causing unprecedented crises at multiple levels. The arms race between attackers and defenders has moved into a new distinct threat cycle with a shift from exploitation to disruption. They are also exposing new inbound and outbound security threats with even stealthier attacks and new methods of circumventing protection by cyber criminals, making it increasingly difficult for defenders to detect them and keep them out. Risk failures also increasingly cascade between public and private sectors. Consequently private risk failures create public disasters.

Moreover, while Advanced Persistent Threats (APTs) were largely confined to government and military targets in the past, this ultra-sophisticated threat has evolved and defused throughout critical infrastructures (CI) during the last two years. Even in the US and Europe, infrastructure operators are often at least one generation behind the attackers.

The Need to Change Corporate Security Cultures

The main security challenge facing companies and national strategies for the protection of critical infrastructures that are largely privately-owned is the need for a fundamental shift in corporate cultures. The first step is to break down the traditional habit of "keeping quiet" and to deny that the companies have been successfully attacked. Those successful attacks have increasingly led to companies being blackmailed and paying hush money to cyber criminals in order to protect their reputation in the market. Even within industry associations, companies are often reluctant to offer any transparency about cyber-attacks infiltrating their corporate networks as this could create a corporate business advantage to their competitors. Almost half of all companies surveyed by the German technology association Bitkom, for instance, admitted in 2012 they had no disaster recovery plan in the event of an attack. One in four companies even confessed they would rather not report it to the police if they were the victims of an attack or if they identified a data leak.

However, without transparency, governments have no knowledge about the quality of newly emerging cyber threats, translating into a failing or insufficient "situational awareness" of the rapidly changing cyber threat environment as a precondition for any effective counter-strategies.

It remains to be seen what benefits arise from setting up a compulsory registration office, as is the case in some countries, or from the German attempt by the "Allianz für Cybersicherheit" (Cyber Security Alliance) to set up a central, voluntary system for reporting cyber-attacks in order to encourage the anonymous exchange of information and knowledge.

The European Commission has declared that in future companies will have to take data protection more seriously and they will have a duty to disclose the extent of any cyber-attacks. The EU's new cyber-security strategy has tried to balance effective counter strategies against new cyber threats to protect individual liberties and the right to informational self-determination and democracy as a whole. Nationally, incident reporting is implemented differently in the 27 EU Member States. Each has different procedures and thresholds. But almost all national regulators

have used a common procedure, a common template and common thresholds for reporting to the European Commission and ENISA. The proposed NIS directive requires companies to report cyber incidents beyond traditionally defined CIs, such as cloud computing service providers, search engines, e-commerce platform providers, social network providers, music and video sharing services, major online computer games, and application stores.

The new cyber strategy has been adopted in the light of recent experiences that more than ever before, the private and public sector will have to "think the unthinkable" when analyzing future cyber security challenges. They will also have to abandon well-trodden avenues, strategies and traditional organizational structures. The qualitatively new cyber security threats demand completely new security reassessments and redefined corporate security cultures based on a different security consciousness and newly designed comprehensive security architectures.

Managers and military leaders often think too much in traditional security lanes of continuity and thus are increasingly blindsided, whereas the new emerging risk landscape has been described "as a superhighway where risks can come from ahead, behind, or from either side". The new risk frontiers of cyber-attacks are cross-cutting, unpredictable, and potentially highly disruptive. Risk failures also increasingly cascade between public, private and military sectors. Consequently private, corporate and military cyber risk failures may create public disasters and threaten the overall national security.

A number of EU Member States have started to recognize the need to create more transparency on cyber security incidents through voluntary or mandatory reporting schemes to prevent incidents. Even European industries and businesses want at least voluntary reporting schemes because they fear an overregulation, the loss of reputation and liability.

But a lack of transparency and lack of information on the corporate side makes it very difficult, if not impossible, for policy makers to understand the root causes and possible cascading interdependencies between affected sectors and the impact of cyber-crimes across borders. As a consequence, political decision-makers, businesses, industries and private consumers are left in the dark about the frequency and dangers of cyber-attacks, its impacts and what needs to be done to prevent them.

The European Commission, for instance, was particularly alarmed by the case of the Dutch certification company, DigiNotar, in the summer of 2011, when the company not only failed to report that its systems had been hacked but did not revoke the digital certificates which were issued fraudulently over the internet during the attack. The result was a large number of invalid certificates circulating online which compromised internet security services. The Dutch Government has since prepared a new system of mandatory security breach notifications for relevant critical infrastructure and national services.

In addressing these new emerging cyber security threats, security concepts have been broadened to become more comprehensive, deepened and integrated. Accordingly, security concepts such as "resilience", once being only reactive, have increasingly become more pro-active by preencountering anticipation of the emerging threats.

Furthermore, the imposition of regulatory performance standards often does not solve the inherent problems because of the slow moving bureaucratic processes. Traditional regulatory models are seen by industrial experts rather an antithesis of the innovation the private sector and those who built, operate and use the cyber space need. In their view, those traditional regulatory models also lead to uneconomic requirements for universal service, non-commercial viable investments to secure CI and may even have even unintended consequences of enhancing robust cyber security defences. Also, regardless of the quality of the European security and defence system against newly emerging cyber threats, both cyber-terrorism and cyber-crime can only be confronted at a global level as they know no national borders and are restricted by geographical distance.

Is Information Sharing a Help or Hindrance to Critical Energy Infrastructure Protection?

Dr. Kevin Rosner

Institute for the Analysis of Global Security, U.S.

Information sharing occurs every day by collective means to protect against contemporary risks to critical energy infrastructure (CEI). Often however precautionary critical energy infrastructure protection (CEIP) measures taken may not be readily and explicitly recognized as such. Weather services around the world track storms, cyclones, and hurricanes that can destroy refineries, swamp storage facilities, and take down electricity transmission towers. Meteorological organizations track seismic activity to warn human populations about dangers to themselves, their homes and their communities from pending or actual earthquake activity. The US Department of State and Foreign Ministries around the world warn their citizens travelling abroad of terrorist threats, political violence, or other instabilities that could put them in harm's way. Cyber-minded government institutions, associations, and private industry publically warn of cyber-attacks and viruses as they spread across the net. Collective means to disseminate information critical to protecting life and property are already routinely employed to these ends.

Threats vary

When it comes to describing and defining threats to critical energy infrastructure, the startling diversity of threats quickly indicates that there is no 'one size fits all' solutions package. Having said this, a requisite first step for categorizing the most common threats to CEI can be accomplished which helps determine whether a prevention, mitigation, or response mechanism should be individual or collective in nature. In all cases, future preventative measures are improved through lessons learned via information sharing but the ultimate litmus test is whether the owners/operators of CEI take these lessons to heart and act upon them.

Weather and cyber threats have already been mentioned as two threat categories that already benefit from collective means of information sharing. There are also threat categories such as technological breakdowns, industrial accidents, employee or complicit insider catalyzed actions that can undermine CEI. In the case of a technological breakdown, product manufacturers and service providers can benefit from information sharing particularly if the casual factor for the breakdown is linked back to an engineering or production failure. Broken or defective valves, a software glitch in a SCADA system deployed across a range of network systems can be identified and corrected once the hardware/software problem has been identified.

The best industrial example of such corrective action is in the transportation sector when product advisories are released, and vehicles recalled, when a manufacturing or process control problem has been identified. Industrial accidents, in terms of the drawing up of de facto future preventive measures, can also benefit from information sharing without divulging (in most cases) proprietary commercial information, although the companies that experience these accidents are often loathe to share information once an accident has occurred for reputational, financial, and prosecutorial reasons. A prime example of this can be drawn directly from the Deepwater Horizon oil spill in April 2010 and the blame game that ensued between British Petroleum, rig operator Transocean and con-tractor Halliburton.

Finally, even in the case of an attempt by an employee of a firm operating a piece of critical infrastructure (water sanitation, electricity transmission, power generation and oil and gas distribution, et al) going rogue, CEI operators can benefit ex post facto by establishing due diligence and heightened vetting and security procedures to prevent future incidents from occurring across similar networked systems based on information sharing and lessons learned. Steps taken as simple as preventing employees from entering USB keys into proprietary networked computers, islanding SCADA systems from the internet, or by preventing third party access to sensitive or critical instrumentation can help mitigate but certainly not prevent cyber intrusion and crime from either stealing or divulging commercially sensitive information. The same case can be made for government as exemplified by the breach of top secret data in the case of Edward Snowden a contractor to the US National Security Agency.

CEI, Commercial Confidentiality, and Unwelcome Information Sharing

There is no question that private companies have the right to protect their commercially confidential information but the fact is that this data and information is increasingly difficult to protect from cyber-crime and espionage. Robert Muller, Head of the US FBI said in a 2012 speech that, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." This of course doesn't mean that critical information regarding a company's commercial secrets or physical assets are impossible to protect but that contrary to our sensibilities perhaps information sharing is one of the best ways to protect these assets.

In 2012 a US News and World Report article quoted the director of the National Security Agency, Gen. Keith Alexander, [who] called cyber-crime "the greatest transfer of wealth in history." The price tag for intellectual property theft from US companies is at least $250 billion a year. That's far more than what businesses pay in federal corporate income taxes. The US *Government Accounting Office*, according to its own report, found that in 2012 federal agencies reported 46,562 cyber security incidents up from 5,503 incidents in 2006. Of course, all of this has hinged on the explosion and development of the internet, data mining by all sorts of operatives, and those looking to exploit and potentially destroy critical assets to national infrastructure.

No amount of denial is going to make threats conducted through the internet or make the internet itself go away. Secondly, as noted commercial espionage is already rampant with malevolent hackers trying to stay one step ahead of authorities so there is no way of putting that genie back in the bottle. Finally, commercial enterprises in a country like the US already own and operate the vast majority of the nation's CEI, and even if asset ownership reverted to public authorities, the government itself is a preferred target of cyber stealth in which to steal all kinds of sensitive information. So what can be done?

By way of example, the US Department of Homeland Security (DHS) *works* with a networked alliance of partners to enable informed decisions and timely actions among the 16 sectors it has identified as critical to the nation. In short, it has decided that a collective path (a network of partners) that drives information sharing forward is preferable to a piece-meal approach. They argue that this allows for information sharing for informed action on three levels:

- **Strategic planning and investment** to inform effective risk management decisions;
- **Situational awareness** in steady state (normal) operations and during a crisis or event, including suspicious activity reporting, incident analysis, and recommended protective actions; and
- **Operational and tactical planning and execution**

Outside the framework of an individual nation, information sharing can serve the same ends, although in this case a strict adherence to the concept of criticality is necessary. Here the *European Union* has made some notable progress of defining what it terms 'European' critical infrastructure. The short version of this definition reads, "European critical infrastructure" or "ECI" means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure." Interestingly, the Commission may participate in discussions between two or more Member States that share ECI but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

Returning to the DHS for a moment it maintains that infrastructure protection based on information sharing provides for:

- **Alerts, threats, and warnings** – Immediate transmission catalyzes action.
- **Effective risk management programmes** – Informs private sector investment decisions and government analysis and planning.
- **Collaboration and coordination** – Supports the development of plans, strategies, protective measures, preparedness, risk mitigation, and response and recovery efforts.

Information shared within a structured and secure information sharing environment helps critical infrastructure owners and operators guide investments, implement protective programmes, and ensure effective response to infrastructure threats as they arise. Similarly, the EU has developed a Critical Infrastructure Warning Information Network (CIWIN) for use by Member States and the respective owner/operators of ECI to be advised of alerts, threats and warnings to their assets.

Private sector role

In a recent *Forbes* article an IT security consultant summarized the value added by information sharing, collected and disseminated in this case by private IT security contractors, when he wrote, "Information sharing is an effective way to get ahead of the bad guys. It increases their expense by making them shift their ground. They cannot target many organizations from the same compromised server because the first one detects it and the rest block subsequent attacks." Where collective means to protect CEI are concerned already in many jurisdictions departments responsible for national security, defence, justice, treasury are joining forces in an attempt to protect and thwart either kinetic or cyber-attacks from bringing down the systems on which modern nations depend. Information sharing is at the forefront of successful efforts as was attested to earlier in 2013 within the framework of a US House of Representatives Subcommittee *hearing* on what capabilities the US government, lead by DHS, has in protecting these assets. The following incident was communicated as part of the written testimony submitted and serves as an example of how information sharing can lead to coordination, cooperation, and action in the field of CEIP.

In March 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December 2011. The attacks were highly targeted, tightly focused and well crafted. Stolen information could provide an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems. While there is no evidence that anyone has tried to subvert the operation of these industrial control systems, the intent of the attacker remains unknown. DHS immediately began an action campaign to alert the oil and natural gas pipeline sector community of the threat and offered to provide assistance. Industry partners have been responsive to these threats, and in May and June 2012, DHS deployed onsite assistance to two of the organizations targeted in this campaign: an energy company that operates a gas pipeline in the U.S. and a manufacturing company who specializes in producing materials specific to pipeline construction. DHS also partnered with the Department of Energy and others to conduct briefings across the country. Over 500 private sector individuals attended the classified briefings and hundreds more received unclassified briefings providing warnings and mitigation strategies.

In considering the potential launch of collective efforts aimed at protecting CEI on a transnational basis, particularly within a potentially new organizational framework, a healthy dose of scepticism can be expected from private owners/operators of these assets. First, in spite of the fact that commercially confidential information is already being mined by operatives with increasing frequency, push-back can be expected in at least two areas, from this community: mandatory regulatory policies and mandated enhanced security measures. The argument that needs to be made however, is that these infrastructure assets, identified as critical to either national or collective (two states or more) security, provide public goods in the form of water, power, communications, health and human services go beyond the prevue of owners/operators themselves. Second, ownership and trust must be present in the organization newly charged with information sharing for CEIP purposes, and protocols established to ensure as best as possible, no haemorrhage of private and confidential information into the public space. Fortunately, no trend or precedent has been set thus far to lead one to this negative conclusion. Finally, the private sector itself needs to accept that the success of any collective means to lean from the past and protect in the future depends (1) on their willingness to share past experience, (2) alert authorities of present and ongoing threats, and (3) to individually introduce prudent but well-qualified risk management measures on the grounds that these measures are for the good of their own enterprise and for the collective good of the nation or nations involved.

Confidentiality of Commercial Information and Collective Action in the Case of Energy Security Threats

Dr. Sijbren de Jong

The Hague Center for Strategic Studies, Netherlands

Introduction

In January 2009, natural gas deliveries from Russia through Ukraine were halted owing to a commercial pricing dispute between the two countries. What followed were reported shortages and a cut in supplies to other European countries (most of whom are NATO members), notably in South-eastern Europe. During two weeks, in one of the coldest winters in decades, the EU experienced the largest interruption to its natural gas supply to date.[1]

Several years before, in January 2006, a similar crisis between the two countries had resulted in falling pressures and non-delivery of gas reports by European companies. This unprecedented event prompted a rethink of existing energy security arrangements, including a proposal by Poland to commit NATO and EU Members to act in concert in the event of an energy disruption, either by natural disasters or political decisions by suppliers.[2] In the end, the Polish proposal never materialized. However, in 2009 proper contingency plans of a non-military nature for dealing with such a major disruption were (still) not in place, as industry had thought an event on this scale to be impossible.

A factor often mentioned in analyses of the event is that the January 2009 crisis proved particularly difficult to solve in light of the limited access to important technical information on the gas system and gas flows at the national and EU level.[3] Adequate crisis prevention and management of a collective nature depends on having such information available and updated on a permanent basis.

This article takes a closer look at the role played by confidential commercial information in contemporary risks to critical energy infrastructure. Taking the January 2009 Russian-Ukrainian gas crisis as the basis, an analysis has been made as to whether this should be viewed as an obstacle, an issue or a challenge to effective crisis mitigation by collective means which relies on information sharing.

The January 2009 Crisis and the Role of Commercially Sensitive Information

Although by late December 2008 there were some signs of impending difficulties with respect to the transit of natural gas through Ukraine, there was no indication that supplies to and through Ukraine would in fact be completely shut off.[4]

In anticipation of difficulties however, the European Commission called a meeting of the Gas Coordination Group – a body which facilitates the coordination of security of supply measures by the Union in the event of a major supply interruption – for 9 January 2009.[5] Following this meeting, the Czech EU Presidency and the European Commission intensified their lobbying efforts to facilitate a solution, which resulted in a monitoring agreement between Ukraine, Russia

1 "The Russo- Ukrainian Gas Dispute of January 2009: A Comprehensive Assessment" (Oxford Institute for Energy Studies, February 2009).

2 S. Haghighi, Energy Security: The External Legal Relations of the European Union with Major Oil and Gas Supplying Countries, vol. 16, Modern Studies in European Law (Oxford and Portland, Oregon: Hart Publishing, 2007), 357.

3 "COMMISSION STAFF WORKING DOCUMENT - THE JANUARY 2009 GAS SUPPLY DISRUPTION TO THE EU: AN ASSESSMENT" (European Commission, July 16, 2009), 5, http://ec.europa.eu/energy/strategies/2009/doc/sec_2009_0977.pdf.

4 "Russia-Ukraine Gas Row Heats up," BBC, December 31, 2008, sec. Business, http://news.bbc.co.uk/2/hi/7805770.stm.

5 "Measures Discussed at the Gas Coordination Group MEMO/09/4," Europa.eu, January 9, 2009, http://europa.eu/rapid/press-release_MEMO-09-4_en.htm.

and the EU on 9 January 2009. The agreement provided for independent monitors from all the involved parties to oversee gas transit on both Russian and Ukrainian soil.[6] Meanwhile, the Gas Coordination Group raised production in several EU Member States, increased withdrawal from storage to maximum capacity in the most affected areas, limited consumption for industry in Bulgaria, Slovakia and temporarily for large consumers in Hungary, and arranged for increased imports from sources both inside and outside the EU.[7]

Although the initial EU response was swift, it is reported that Norwegian supplies could not reach Eastern Europe due to a lack of interconnections, as well as different standards of gas.[8] At this point during the crisis it became apparent that reliable aggregate level information about demand patterns, gas flows, how much gas was in the system and in storage proved hard to come by. Limitations on consistent information and exchange of data between gas companies were all obstacles in making the most of the available market potential. Put differently, the EU was aware of the shutdowns of gas supply that were causing major difficulties for industrial and household consumers, but did not have adequate access to information about the flows of gas which were contracted commercially for distribution to its customers.[9]

This view is supported by various actors. Gas Infrastructure Europe (GIE)[10] in its April 2009 assessment, claimed constraints that arose from the confidentiality of data limited information exchanges between traders/suppliers and operators on the availability of natural gas. This prevented the actors from putting information on capacity and commodity together and undermined arriving at a satisfactory solution to the crisis. The Council of European Energy Regulators[11] advised that, in order to improve transparency, a harmonized minimum level of information – whilst respecting existing confidentiality agreements – should be made available to the market, especially in crisis situations. The European Commission arrived at a similar conclusion advising that comprehensive market data needs to be available, without restriction, on a daily basis, bearing in mind the possible need of recipient bodies to respect the standard commercial confidentiality requirements.[12]

Policy Measures in the Wake of the Crisis

Numerous policy measures were tabled in the wake of the crisis. In assessing these initiatives, it is important to point to some limitations on the ability of the EU to address the issue posed by commercially sensitive information on natural gas flows and contracts.

Under the Treaty of Lisbon, EU energy policy has remained an area of shared legal competence between the Union and its Member States. Perhaps most important in this regard is Article 194(2), second paragraph of the Treaty on the Functioning of the European Union (TFEU) which states that measures necessary to achieve the objectives of Article 194(1) TFEU

> "[…] shall not affect a Member State's right to determine the conditions for exploiting its energy resources, its choice between different energy sources and the general structure of its energy supply [….]".[13]

Put differently, the EU cannot legally oblige its Member States to disclose commercially sensitive information if it thinks this will improve its crisis mitigation capacity. Therefore, improving collective action crisis management should be attained through other means, notably enhanced coordination.

6 "Monitoring Team Starts Work in Kiev and Gas Coordination Group Urges Naftogaz and Gazprom to Resume Gas Deliveries Immediately IP/09/24," Europa.eu, January 9, 2009, http://europa.eu/rapid/press-release_IP-09-24_en.htm.

7 S. de Jong, J. Wouters, and S. Sterkx, "The 2009 Russian-Ukrainian Gas Dispute: Lessons for European Energy Crisis Management after Lisbon," European Foreign Affairs Review 15, no. 4 (2010): 522.

8 "European Regulators Group for Electricity and Gas (ERGEG) Advice on Russia-Ukraine Gas Dispute," February 10, 2009, http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Gas/2009/LM_Piebalgs_090210.pdf.

9 "COMMISSION STAFF WORKING DOCUMENT - THE JANUARY 2009 GAS SUPPLY DISRUPTION TO THE EU: AN ASSESSMENT," 6.

10 "GIE Views Regarding the Prevention and the Management of Gas Crises Ref: 09GIE130" (Gas Infrastructure Europe, April 30, 2009), 2–4

11 "European Regulators Group for Electricity and Gas (ERGEG) Advice on Russia-Ukraine Gas Dispute," point 5.

12 "COMMISSION STAFF WORKING DOCUMENT - THE JANUARY 2009 GAS SUPPLY DISRUPTION TO THE EU: AN ASSESSMENT," 6.

13 Art. 194(2)(2) TFEU, OJ C 326/134 of 26 October 2012.

To that effect, the February 2009 EU Energy Council concluded that transparency and reliability should be increased through meaningful exchange of information between the Commission and Member States level on energy relations, including long term supply arrangements, with third countries while preserving commercially-sensitive information.[14]

This call resulted in the revision of the Security of Gas Supply Regulation, which was adopted on 20 October 2010. The regulation provides for the establishment of preventive action plans and emergency plans at the national level with coordination of the plans by the European Commission and the Gas Coordination Group.[15] This addresses one of the key-problems encountered in the January 2009 crisis, namely the limited coordination of emergency plans. Although, the regulation does *not* specifically address the issues posed by commercially sensitive information, the prominent role assigned to the Gas Coordination Group does go a long way into enhancing coordination of emergency measures.

Another noteworthy policy initiative was the decision to establish an information exchange mechanism between EU Member States and the European Commission with regard to intergovernmental agreements in the field of energy, with the aim of optimizing the functioning of the internal energy market.[16] The mechanism obliges EU Member States to inform the Commission of intergovernmental agreements in the field of energy in so far as they contain elements which have an impact on the functioning of the internal energy market or on the security of energy supply in the Union. However, under the Decision, the initial assessment as to whether an intergovernmental agreement, or another text to which an intergovernmental agreement refers explicitly, has an impact on the internal energy market or the security of energy supply in the Union, should be the responsibility of Member States. Moreover, under Article 4 of the Decision, Member States retain the right to indicate whether any part of the information – be it commercial or other information the disclosure of which could harm the activities of the parties involved – is to be regarded as confidential and whether the information provided can be shared with other Member States. The Commission is obliged to respect those indications.

The above observations point to important limitations in the ability of the EU to tackle the issue posed by commercially sensitive information in crisis situations. This raises the question whether the EU should *at all* focus its attention on this issue from the perspective of collective action in the case of energy security threats, and whether commercially sensitive information is the real issue at hand.

A specific type of geopolitical risk affecting natural gas markets are the differences between legal and regulatory regimes to which a pipeline is subjected when it crosses the territory of multiple states.[17] When attempting to address a supply disruption, having similar legal and regulatory standards on either side of the EU border facilitates the flow of information as the parties affected are under similar disclosure obligations. The limited availability of important technical information on the gas system and gas flows at the national and EU level during the January 2009 crisis thus seems to have been primarily due to differing legal and regulatory standards in Ukraine, rather than because of the legal right for commercial entities to shield commercially sensitive information.

It is in this respect that I believe the EU should instead base its efforts on addressing some of the root causes of inadequate energy crisis response based on a domain in which it has a stronger legal competence, namely the internal energy market.

[14] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning Measures to Safeguard Security of Gas Supply and Repealing Directive 2004/67/EC" (European Commission, July 16, 2009), 9.

[15] "REGULATION (EU) No. 994/2010 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 October 2010 Concerning Measures to Safeguard Security of Gas Supply and Repealing Council Directive 2004/67/EC OJ L 295/1," November 12, 2010.

[16] "DECISION No. 994/2012/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 Establishing an Information Exchange Mechanism with Regard to Intergovernmental Agreements between Member States and Third Countries in the Field of Energy" (Official Journal of the European Communities, October 25, 2012).

[17] Ernest Moniz et al., The Future of Natural Gas - An Interdisciplinary MIT Study (Cambridge, Massachusets: Massachusets Institute of Technology (MIT), 2011), 147.

Expand the Energy Community Treaty

The added value of having legal and regulatory regimes on energy in non-EU states of comparable or equal strength as the EU's own energy *acquis communautaire* was recognized well before the Russia-Ukraine crises began. In October 2005, the decision was taken to establish the Energy Community Treaty. The Treaty extends the EU internal energy policy to South East Europe and the Black Sea region on the grounds of a legally binding framework. The overall objective is to create a stable regulatory and market framework. Ukraine became a contracting party to the Treaty as of 1 February 2011. Crises comparable to the January 2006 and 2009 gas interruptions between Russia and Ukraine have not occurred since.

The Energy Community represents a unique international body which not only unites all EU Member States, but also key-transit states in its neighbourhood, notably Ukraine and all the states from former Yugoslavia. In light of the ongoing efforts in Europe to diversify the supply of natural gas by increasing the volumes of gas contracted from the Caspian Sea region, the roles played by energy transit countries such as Turkey and Georgia are set to become even greater in the near future.

Currently, both Turkey and Georgia are observers to the Energy Community. Membership negotiations with Turkey were initiated in September 2009 and Georgia applied for full membership in January 2013.[18] Although negotiations with Turkey are said to be progressing, it remains an open-ended question when the country will join the Energy Community as a full member. The October 2013 Energy Community Ministerial Council called on the European Commission and Georgia to start negotiations early enough so that an Accession Protocol could be signed at the October 2014 Ministerial Council Meeting.[19]

Given the growing energy partnership between the EU, Georgia and Turkey and the decision by Turkey and Azerbaijan to construct an essential pipeline along the 'Caspian route' themselves, it is strongly encouraged that negotiations are finished sooner, rather than later.[20] For, if there is one thing the Russian-Ukraine crises have served to demonstrate, it is the security risks of having differing legal and regulatory standards along vital energy transit corridors.

[18] "EU-Backed Nabucco Project 'over' after Rival Pipeline Wins Azeri Gas Bid," EurActiv.com, accessed November 1, 2013, http://www.euractiv.com/energy/eu-favoured-nabucco-project-hist-news-528919.

[19] "11th Energy Community Ministerial Council - Meeting Conclusions" (Energy Community, October 24, 2013).

[20] "What Is TANAP | TANAP – Trans Anadolu Doğal Gaz Boru Hattı Projesi," TANAP.com, 2013, http://www.tanap.com/en/what-is-tanap.

Barriers to Information Sharing Negatively Impact Critical Energy Infrastructure Protection

Ernie Hayden

CESSP CEH, *Securicon* LLC, U.S.

Attention to critical infrastructure in the world continues to expand – especially following the events of Super Storm Sandy, the Philippine typhoon, and so forth. The energy infrastructure continues to receive increased attention globally due to its importance to our society and national defence. Fortunately, due to increased awareness and attention by government agencies and energy company management the security of these systems is improving; however, there continue to be substantial challenges in information sharing between the energy companies and the government and its regulators and vice versa.

Why is this so? Why hasn't this problem been solved in light of the numerous news reports of cyber hacktivism against these various utilities and energy companies? This discussion will summarize some of the actions taken to date to encourage and facilitate improved information sharing and some of the barriers to this process will be reviewed. Finally some possible solutions to this dilemma will be highlighted.

History of Information Sharing

Intelligence sharing between the energy critical infrastructure owners/operators and the government agencies has been limited and hindered by a variety of factors to be discussed later. Similarly, but slightly less hindered, there has been some intelligence sharing between the energy infrastructure owners/operators and their peers. However, in both instances the sharing is restricted and often only one way – especially when dealing with the government.

In the US in 1998 an emphasis on preventing physical and cyber-attacks against critical infrastructure by sharing information between public and private sectors was begun. President Bill Clinton signed the Presidential Decision Directive 63[1] (PDD 63) thus creating the concept of the Information Sharing and Analysis Centres – otherwise referred to as ISACs – for industries related to critical infrastructure. The PDD continues to note *"…Such a centre could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and to the (government)…" The PDD continues that "While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchange between companies and the government."*

The concept of the ISAC is fundamentally a good one and since then some excellent models of improved communication have surfaced, such as the Financial Services ISAC[2] and the Research and Education Network ISAC (REN-ISAC)[3]. Other approaches to improving two-way communication have also surfaced in the US, such as the Federal Bureau of Investigation starting the Infragard[4] chapters and the establishment of the US-Computer Emergency Response Team (USCERT)[5] and the US Industrial Controls Systems CERT (ICS-CERT)[6].

However, even 15 years later there is continued criticism and public-private demand for improved information sharing with the goal of protecting critical infrastructure from attack.

[1] https://www.fas.org/irp/offdocs/pdd/pdd-63.pdf
[2] https://www.fsisac.com/
[3] http://www.ren-isac.net/
[4] https://www.infragard.org/
[5] http://www.us-cert.gov/
[6] http://ics-cert.us-cert.gov/

Barriers to Sharing

Conceptually, the idea of sharing information between you and your fellow citizens for everyone's protection makes complete sense. However, such approaches to protecting critical infrastructure are stymied by a variety of issues ranging from legal to financial to political. Key aspects of these barriers can be summarized as follows:

Legal Barriers: Probably the most frequently cited causes of constrained communications are the legal aspects. For instance a corporation could be held liable for damages caused should it share information that can be viewed as a reckless release of information or opinion. Also, there are concerns over anti-trust issues whereby sharing information to your competitors could be legally challenged as contrary to open and fair competition. On the government side, the law enforcement entities may be concerned about sharing information because it could jeopardize their ability to prosecute the attacker. And finally, some information is legally classified by the government agencies and sharing such information could violate laws designed to protect classified information.

- **Financial Barriers:** Some organizations are fearful of sharing information because it could lead to negative impacts to the organization's stock price (if appropriate) or to investor's willingness to direct money to the company. For instance, if a company raises the spectre of a current or potential attack this may cause investors to take their money and move it to other "more perceptually secure" companies thus lowering the actual and perceived value of the company and its assets.
- **Public Reputation:** Sharing information on possible vulnerabilities, potential attacks or even current attacks can still result in negative impacts on the public view of the organization and its ability to securely run the critical infrastructure. This can be due to the way and means of delivering the information and it can also be how the media – including social networks – could construe the news. Raising concerns about the weakness of the organization's management or systems will both lower the public reputation for the organization and may even draw the attention of other potential attackers.
- **Denial, Ignorance and Lack of Inclusion:** Some entities will deny that they are a potential target for attackers and as such simply step away from responsible information sharing. Some entities are simply unaware that they are under attack and should report the event. And some organizations don't feel like they are being included in "the club" such as an ISAC and as such they don't have a sense of obligation to report their issues, events and concerns.
- **Lack of Value:** In order to encourage an effective two-way system for information sharing it is critical that both parties get a sense that their participation is valuable. Not only are their contributions viewed as important and useful but also the return information is useful and usable. Unfortunately this particular point is probably one of the biggest reasons why information sharing for critical infrastructure protection is ineffective in the US. In particular the participating entities in such organizations as Infragard or some ISACs feel that the information flow is in only one direction – to the government and that there is no value to being in the association.
- **Lack of Mutual Trust:** This is by far the biggest reason why information sharing is simply not effective. There is concern by the government that sharing secrets with the organizations may result in leaks and possibly cause investigations to collapse. Similarly, there are concerns that sharing the information with the government or regulator may lead to future problems and possibly penalties or fines that are contrary to the primary intent of sharing information to protect the critical assets.

Overall, there may be more barriers to information sharing than those summarized above; however, it is recognized that improving information sharing is not going to be a simple remedy.

Possible Solutions to Improve Information Sharing

As noted in the commentary above, there continues to be recognition that information sharing between the critical infrastructure owners/operators – especially those in the public sector – and the government and regulatory agencies is not in place, that it is not effective and it needs substantial improvement. From before 1998 to today it is easy to find commentaries and editorials about how all parties need to improve information sharing for the benefit or our collective protection and defence.

So, what is happening today and what other ways and means are there to improve the situation?

- **Executive Order:** The highest profile initiative is President Obama's Presidential Decision Directive, *Improving Critical Infrastructure Cybersecurity*, which he signed on 12 February 2013. The President's order specifically denotes:

  It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with US private sector entities so that these entities may better protect and defend themselves against cyber threats.

  The order also goes on to ensure the timely production of unclassified reports of cyber threats to the US that identify a specific target entity and that classified reports would be disseminated to critical infrastructure entities authorized to receive them. Hence, there will be increased emphasis on processing security clearances for appropriate personnel employed by critical infrastructure owners/operators. Similarly, there will be expanded use of programmes that bring private sector subject matter experts into US Government service on a temporary basis to have them provide advice regarding the content, structure and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

- **Cybersecurity Framework:** As an outcome of the Obama Executive Order the US National Institute of Standards and Technology (NIST)[7] has been charged with working with US critical infrastructure owners/operators and developing a cybersecurity framework[8] for reducing cyber risks to critical infrastructure. The framework will consist of standards, guidelines, and best practices to promote the protection of critical infrastructure.

  A preliminary cybersecurity framework has been published on the web.[9] In several instances the framework draft reinforces the need to share information to help protect critical infrastructure.

- **Information Sharing and Analysis Centres (ISACs) Continue to Expand and Evolve:** The ISACs are still in play and in a few instances expanding. For instance, the Industrial Control Systems (ICS) ISAC[10] was formed and is continuing to expand with new members focused on sharing information to help protect industrial controls systems used in critical infrastructure.

- **Private Information Sharing Groups Formed:** Because of the concern over trusted transfer of information, frustrations over the tendency of the government to be very ungenerous with sharing intelligence and a need to assure that all parties are included and feel that they are gaining value for their physical and monetary contributions, some private organizations are surfacing to fill this void.

  A collective of visionaries in the US electrical energy industry formed a voluntary group called EnergySec.[11] EnergySec's mission is to drive security excellence among participants through collaboration and careful analysis of security issues. In some respects, EnergySec may have been formed to fill the trust voids between the electric industry and the Electric Sector ISAC (ES-ISAC)[12] which is run in conjunction with NERC.

  In other critical infrastructure industry verticals – such as health care and financial services – groups have been formed to allow for increased sharing without concerns that the information would be released to the government. One such group is the Payments Processing Information Sharing Council (PPISC)[13] and another is the Health Information Trust Alliance (HITRUST)[14].

[7] www.nist.gov
[8] http://www.nist.gov/itl/cyberframework.cfm
[9] http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
[10] http://ics-isac.org/
[11] http://www.energysec.org/
[12] http://www.esisac.com/SitePages/Home.aspx
[13] http://www.ppisc.com/
[14] http://www.hitrustalliance.net/

A final example of an information sharing organization at a local level is the AGORA in the Seattle area. The AGORA was founded over 15 years ago in the Seattle area by the then Chief Information Security Officer of the City of Seattle. His vision was to bring together interested and concerned individuals in the Seattle metropolitan area to share ideas and experiences about cyber and physical security threats to their companies and the region's infrastructure. The AGORA is not affiliated with any government agency and is operated at a very low cost.

Recommendations

The biggest challenges to effectively overcoming the complications with information sharing in the area of critical infrastructure are two-fold. First, repair and correct the trust issues. Secondly, ensure that the information flow is two-way. Without these fundamental elements being addressed and corrected through laws and supervisory emphasis the problems with information sharing will probably remain.

Promulgating guidelines regarding information sharing will not be adequate. Overall, there needs to be some sort of emphasis – especially to the government agencies – that sharing information is in everyone's best interest. Hence, there may be a need to substantially increase the number of personnel with security clearances at the various energy infrastructure owner/operators in order to give the government adequate "trust" that the recipient can use the threat/attack data responsibly and not leak it to the public.

Conclusions

The lack of effective information sharing between the owner/operators of critical infrastructure and the government is not a new issue. It has been happening for many years and was even recognized in 1998 by the Clinton Administration with the establishment of the ISACs. Unfortunately the problem still continues due to legal, financial, and reputational barriers with the penultimate barrier being lack of trust by all parties in the dialogue. As such, until trust and the effective establishment of a true two-way communications flow are foundationally established, the problem with information sharing to protect critical infrastructure will remain.

Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges

Dr. Jennifer Giroux

Risk & Resilience Team in Center for Security Studies (CSS) in Zurich, Switzerland

Laura Melkunaite

Risk & Resilience Team in Center for Security Studies (CSS) in Zurich, Switzerland

During fieldwork carried out in Nigeria in 2012, one informant from a large oil company expressed [to this author] the challenges and difficulties that arise not only from operating in high-risk environments but also within an industry characterized by interdependencies and partnerships. These challenges were often compounded, he explained, by the lack of consistent information sharing practices. Though domestic and sector-specific information sharing networks exist, albeit informal in nature, the reality is that most company information sharing policies include issues of confidentiality that prevent critical risk information from being shared immediately or at all. To illustrate, he referred to an incident that involved unconfirmed information of a criminal attack aimed at a competitor's offshore assets. Given that both companies operate in the same space, there was a need for this information to be verified and shared throughout the industry so that other companies could take the necessary precautions. The reality, however, is that there were no mechanisms or agreements in place to enable this exchange. In fact, due to issues of confidentiality, the company did not release information of the incident until many days after the attack.

Of course, while Nigeria is a unique context, the issues that this individual expressed share some similarities with other cases across the globe. Despite shared interests, getting people (or by extension organizations) to share information (whether it's over the telephone, through an online forum, or face-to-face in a meeting) about threats or breaches in security is incredibly challenging and complex. On the one hand, in today's world, threats are unbounded, complex, and exhibit non-linear forces that come from all directions. In fact, the very nature of the contemporary risk environment demands information sharing as one of the mitigation tools. On the other hand, critical infrastructures are embedded in this threat landscape through complex interconnections between the public and private actors and technical linkages as well as interdependencies across sectors and interests. The information or virtual systems that play such a prominent role in today's world now serve as the underbelly of critical (physical) infrastructures and thus create new and often hidden points of vulnerability. These factors alone necessitate the sharing of information between owners and operators of critical infrastructures, particularly in the energy sector where physical and cyber-attacks aimed at energy infrastructures are on the rise. And yet issues of confidentiality and competition or even punishment limit the type of robust and rapid exchanges needed to mitigate risks in today's volatile terrain.

Platforms for Information Sharing

Any discussion on information sharing in critical energy infrastructure protection (CEIP) first warrants an explanation of the types of information sharing networks and public-private partnerships (PPP) in particular. Simply, PPPs are platforms for collaboration and information sharing between state and non-state actors that have a shared interest in the delivery of critical services, such as electricity, to the public. As the owners and operators of critical infrastructures are increasingly from the private sector, states have been confronted with a new reality where they are no longer capable of providing the security for public services. PPPs have thus grown in importance as a type of network approach to modern governance. Given that information on security breaches and threats is dispersed across a network of authority, knowledge and influence, PPPs have become a mechanism and a function of risk management.[1]

The rapid exchange of information is a key part of any partnership network. While this includes the already discussed PPPs, there are 2 other types of information sharing partnerships (Figure 1). For example, information sharing partnerships can be designed to serve only the public sector.

[1] Giroux, Jennifer (2013). Early Warning & Information Sharing In Critical Infrastructure Protection (CIP). Centre for Security Studies, ETH Zurich.

This could either include sharing within a specific government (e.g. across different agencies or departments) or between governments (e.g. intergovernmental cooperation for early warning and rapid response to transnational threats). There are also partnerships that encourage sharing within or between the private sector, such as those operating in a specific industry. In this case, as with PPPs in general, not only can information sharing provide an avenue for an entire sector to see the threat landscape but it can also provide decisive advantage by creating a mechanism for early warning by allowing stakeholders to quickly identify, respond, diffuse and prepare for threats.

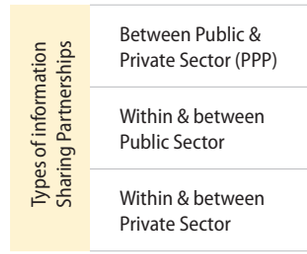


Figure 1: The types of information sharing in CIP

Key Challenges

Recalling the Nigeria example, for operators in this region being immediately informed of incidents can help the entire energy sector network track the movement patterns of threats and quickly adapt security postures. However the lack of strong formal or informal sharing mechanisms or platforms means that information is not always provided to the network. This case draws out one of the key challenges of information in CEIP: even though the opportunities and benefits of information sharing are well known and documented, limitations arise due to respective interests, policies, etc. to not disclose sensitive information, particularly to competitors. For intrusions to information infrastructure, such as those aimed at supervisory control and data acquisition (SCADA) systems like the infamous Stuxnet worm, the issue of guarding or not releasing information about security breaches is particularly pronounced.

These challenges arise out of the various ways that stakeholders view and prioritize CIP and CEIP more specifically. On one end of the spectrum, privately owned CI operators prioritize innovation and company growth above other obligations, such as regulatory.[2] According to McCrohan, the security goals of the private sector aim for "maximum protection for minimum cost, consummate with the threat."[3] On the other end of the spectrum, a state's primary interest is the delivery of public goods and maintaining the smooth functioning of critical services, thus making protection and security of infrastructures a primary goal. Therefore, the aspect of diverse interests within PPP might cause some imbalances.

Another issue is one of confidentiality. To note, placing private companies in information sharing networks with state or private actors, the latter of which consists of competitors, raises a number of considerations that limit sharing, especially if trust within the network is low. Low trust typically translates in companies guarding information out of fear that government partners may not respect the issue of confidentiality or that sensitive information may fall into the hands of competitors and thus cause reputational damage or impact competitive edge. This aspect is particularly relevant within the cyber realm where incidents are not as evident as physical intrusions and therefore easier to keep quiet (that is unless it is a major attack resulting in clear disruptions, such as e.g. power outages). In addition, the private sector also fears an increase in exposure to liability due to the disclosure of critical infrastructure information (CII). Of course, governments also face risks related to information confidentiality and disclosure. Accidental or intentional exposé of classified intelligence can seriously jeopardize the activities of intelligence services and other institutions[4]. Additionally, governments often withhold information related to current vulnerabilities of CEI and methods employed to rectify those vulnerabilities as a form of protection.[5]

Information Sharing & Early Warning

Despite the aforementioned challenges – particularly in terms of confidentiality issues – CEI information sharing networks are valuable. One discernible trend is the way in which some of the platforms can create a space and mechanisms for early warning (EW), which is defined as the advanced warning of threats. Here we note two distinctions. The first is pre-event early warning, which seeks to prevent an event from happening. This implies that authorities communicate threat/risk information to partners who then enhance protection and preparedness efforts.[6] The second is EW during the event. In this case, when a member of a network reports an event, other

[2] Ibid

[3] McCrohan, Kevin (2010). Information Sharing: Lessons from the Post 9/11 Environment. GMU Centre for Infrastructure Protection and Homeland Security, the CIP Report, 8(11), pp. 7-10. Accessed: 31.11.2013. http://cip.gmu.edu/archive/CIPHS_TheCIPReport_May2010_InformationSharing.pdf.

[4] Dunn Cavelty, Myriam & Suter, Manuel (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure protection. International Journal of Critical Infrastructure Protection, Vol. 2(4), P. 3.

[5] Gallagher, Sean & Neugebauer, Michael. Critical Infrastructure Information Sharing. Accessed: 30.10.2013. http://www1.maxwell.syr.edu/uploadedFiles/campbell/events/GallagherNeugebauer.pdf.

[6] Giroux (2013), p.3-4.

stakeholders are immediately notified so that they can take measures bolster security, contain the threat, and take appropriate measures to prevent disruptions or at least mitigate the effects.[7] In the Nigeria case this would have meant that the attack would trigger an alert that would be sent to other operators in the area so that they could respond and adapt accordingly.

In Practice

Information sharing in CEIP occurs through a number of formal and informal mechanisms; however processes and practices differ from country to country. While some countries have heavily invested in establishing agencies and public-private partnership platforms to exchange information, monitor and/or report incidents, other countries have yet to take these steps.

At an inter-governmental level, some notable examples of information sharing within CEIP include efforts at the OSCE, EU & European Commission, and NATO. All of these entities provide either some type of platform – some of which could be classified as pre-event early warning – to bring public and private actors together to exchange information and/or carry out more specific tasks such as identifying best practices to mitigate threats to CEI. For example, though the European programme for critical infrastructure protection (EPCIP) is a legislative effort, one of its aims is to create boards on Critical Infrastructure Protection (CIP) at the European Union level. This, in turn, facilitates information sharing about CIP issues, of which the energy sector is included. The EPCIP has also facilitated the implementation of a warning system on critical infrastructures (CIWIN), which is also another mechanism for sharing information. Outside of the realm of government, the European energy sector has also established a network of CEI operators to share information on various risks.

At a domestic level, the US Department of Homeland Security, through its National Infrastructure Protection Plan (NIPP) and Information Sharing Environment, has created various mechanisms and pathways for public and private actors in the energy sector, amongst other critical infrastructure sectors, to share information. However, it bears mentioning that this is a highly regulated endeavour, one that is directed by frameworks and guidelines that clarify roles and responsibilities.

For more sector-specific, cyber-related incidents, the private sector can participate in CERT/CSIRT which are information sharing platforms that serve as an EW mechanism in the pre-event and event phase, thus leading to better preparation and reaction/response to incidents. By participating, owners and operators gain a comprehensive risk picture. In many cases, CERT/CSIRT have been able to mitigate issues of confidentiality – though they still persist – and be a rather effective mechanism. Another, and more recent information sharing network, is the Energy Sector Security Consortium, or EnergySec[8], which brings together a number of the owners/operators of the power sector [in the US] to share information *about threats to the information (or cyber) assets of critical energy infrastructures*. This consortium has had some success in creating a collaborative network and one that also benefits from the analysis that EnergySec performs on cyber threats. Uniquely, this network was born out of very informal meetings amongst energy professionals in the US and then developed organically into an organization with a more formal structure and mandate.

Final Remarks

Overcoming the challenges of confidentiality and other information sharing issues that surface across a diverse network of partners and competitors is not an insurmountable task. However, cultivating a space of trust and meaningful interaction is a necessary ingredient to any successful information sharing endeavour. This is typically accomplished through a combination of having a coordinating or initiating body that can push forward and promote a culture of information sharing as well as a network of actors that sees (and experiences) the value of the exchange. In many cases this is a government actor however in such cases it is important that both state and non-state actors provide a mutual exchange of information. Many complaints from the private (energy) sector regarding PPPs is that state partners do not reciprocate with information sharing due to their own limitations releasing confidential or classified information. However, given the numerous and myriad threats that confront the energy sector – coming from both the physical and cyber realm – as well as the network approach to modern governance, actors need to develop a contemporary understanding of the value of exchanging actionable and timely information as well as additional modes of trusted sharing pathways that can mitigate today's challenges.

[7] Ibid p.4.

[8] http://www.energysec.org/

Sharing confidential commercial information for ensuring availability of critical infrastructure: technology opportunities and perspectives

Dr. Jürgo-Sören Preden

Laboratory for Proactive Technologies in Department of Computer Control, Faculty of Information Technology in Tallinn Univerity of Technology, Estonia

The modern world presents our societies with new threats, which although comparable to conventional threats, are more difficult to mitigate and require new approaches for maintaining national security. Current and future conflicts are characterized by asymmetry – the offensive actions are not only targeted against military assets and personnel. Instead, untraditional tactics and weapons are used in unexpected locations, including actions against civilian infrastructure. In order to effectively tackle these new threats but also the threats arising from accidents and natural disasters society must adapt and consider new ways of utilizing and adapting the technology we have at our disposal for mitigating threats and also for disaster recovery. As our societies rely on critical infrastructure for keeping the society operational, the critical infrastructure owners and providers of critical services (e.g. power, telecommunications, banking, rescue services, and transportation) must all collaborate in mitigating threats and dealing with the consequences of crises.

Handling Critical Situations

Most critical services are interdependent in various ways and in many cases do not depend only on the situation and decisions taken within a single domain, region or a country. Power plant failure in one country may immediately increase the expectations towards imported energy from neighbouring countries, a great number of people gathering at a public event may create chaos if a heavy storm hits the area and communication services are not available. There are hundreds of examples of how the limited availability of critical services can disrupt our economy and the daily life of citizens. In the highly dynamic modern world situations can change fast. The reasons for the change of the situation stem from a range of sources, from climate conditions to manmade events. Most of the emerging situations require timely response from the authorities to prevent undesired results. To be able to respond to the developing situations, the authorities and people responsible for maintaining overall civil protection resilience (including combating terrorism, protecting law and order, supporting rescue activities, protecting the environment – as a whole, ensuring the health and well-being of population) must have up-to-date information on the current situation. Maintaining situational awareness is required both for prevention of unwanted consequences as well as for dealing with the results if the unwanted events cannot be avoided. With no objective information in advance of the incident or during the incident, the possibility of adequate reaction is minimal. Therefore, it is critical to provide the information necessary for achieving and maintaining adequate situational awareness on any ongoing event (and to provide means for predicting possible future scenarios (modelling) to the responsible authorities not only for responding to any threats in a timely manner, but also for planning proactive measures.

Providing the Right Information to Decision-makers

Discussing the information needs of a decision-maker responsible for maintaining availability of critical services, one should not only consider the correctness of the information but also the data requirements – what is the right information needed. In case of a crisis or a potentially developing crisis the decision-makers must take proactive and reactive measures to avoid the development of a crisis or to reduce the effects of a crisis. The decision-makers in this context are not only the state authorities responsible for the security of citizens, but also the people working the organizations that are responsible for providing critical services.

Clearly the decision-makers must have a high level of experience, be able to take into account the factors relevant in a specific situation and also be able to predict the future scenarios that may develop from the current situation. However, in order to be able to make adequate decisions the decision-makers must be provided with up-to-date and relevant situational information to develop the level of situation awareness needed. Situation awareness is the perception of elements in the environment, their comprehension and projection to the future[1]. In order to have adequate situational awareness the individual decision-makers must be provided with the data they need, in the form that they need it and when they need it. The information needs to vary between individual decision-makers both in the type and granularity of information. The source information elements needed by individual decision-makers may be similar but the information elements and their effects are interpreted differently – from the energy supply perspective the number of people in a specific area translates to energy needs, from a rescue perspective it may translate to the number of rescue vehicles needed for evacuation.

The situational information needed for deciding on effective actions is much broader than just the information from a single organization or even a domain (such as the energy domain) as there is a clear interdependence between services, for example banking or communication services are only available if energy services are available. As information relevant for adequate decision-making also includes commercial information from companies from all the domains providing critical services (among many other information sources and types), this type of information must be exchanged as well. However, for resolving or avoiding a crisis the detailed commercial information need not be made available to all parties, only the information relevant for the individual decision-makers needs to be exchanged. Furthermore, the information that is made available to the decision-makers does not have to be the original source information but instead it can be higher level situational information necessary for decision-making (energy shortfall in a specific area or the number of days for which food supplies in stores will last in a specific area).

Aspects of Confidential Information Exchange

It should be obvious that there are no alternatives to sharing confidential commercial information if we want to ensure a sustainable society. As exchange of confidential commercial information is crucial for ensuring the safety of citizens, we should not look for reasons and ways of avoiding information sharing but instead look for methods of identifying the minimum subset of required information and exchanging the information in a way where all entities concerned are satisfied with the solution. Naturally, it should be done in a way where the commercial interests of companies are not threatened by the exchange of information needed for preserving the safety of nations. As it is a citizen's responsibility towards the state to notify it of threats to society, it is also the duty of critical service providers to share information on aspects of critical service availability with the state authorities as well as with other companies affected by the critical service. The organizations that provide critical services and maintain critical infrastructure are active contributors to homeland security and they should acknowledge the responsibility.

Below some of the possible technological solutions are described that are applicable for sharing commercial information between critical service providers and state authorities without damaging the commercial interests of the parties involved.

Technologies and Solutions Supporting Sharing of Confidential Information

The objective of sharing confidential information is to provide situational information to decision-makers. Therefore, we should look at the information delivery chain from generating the information to communicating it to the information users. Sharing information does not mean that all data available at a data source is delivered to a potential user, instead only the information the user needs (and is authorized to access) at a specific moment is delivered to the user. A model of communication based on the concepts of a data producer and data consumer

[1] Endsley Mica R and Garland Daniel J, "Situation awareness analysis and measurement" - London : Lawrence Erlbum Associates, Publishers, 2000

with a data subscription based exchange method that supports information pull (as opposed to push) would be applicable in the current context. In a normal situation only a very limited amount of information is delivered. However, in the event of a crisis in a specific area, requests for more detailed data are made automatically by data consumers. In addition to reducing the exposure of confidential information such an approach also helps to mitigate the big data problem – not piling all the data to all the data consumers significantly reduces the amount of data communicated and delivered. Such a data exchange model can be facilitated by a mediated data exchange model, called the mediated interaction, which concept is explained in further detail below.

The system architecture that can facilitate this approach is a system of systems approach, where individual systems can be both information providers (i.e. information can be generated in these systems) and also information consumers (i.e. systems that use information either to compute the probability of scenarios and/or for presenting the information to the human user). However, regardless of the availability of information from other systems the individual systems can also operate autonomously.

Mediation of Information

In order to facilitate the correct exchange of information the theoretical concept of mediated interaction must be used for controlling the exchange of data between systems.

Wiederhold2 introduces the abstract concept of a data mediator as a means to tackle the issue of semantic heterogeneity in large scale information systems. Wiederhold proposes that mediators could interpose integration and abstraction services in large scale information systems, where the applications used by decision-makers require data from heterogeneous sources (Figure 1). The mediation in this context addresses the inconsistency in composition, where a large system depends on services that were developed independently. Such resources cannot be expected to be compatible in any dimension as they have not been designed as services or components. While Wiederhold addresses the semantic aspects of mediation in data processing systems, the same concepts can be also applied in more dimensions (performing online validity checks in several dimensions and also data quality evaluation) to guarantee successful exchange of information between data providers and consumers.

Figure 1: Information mediation from data sources to users by Wiederhold [8]

Mediated interaction enables smart and potentially proactive one-to-one interaction between autonomous systems, where the functionality and operation depends on situational information and on the goals of the system(s). The concept of mediated interaction enables dynamic filtering of transmitted messages, or modifying the mapping (i.e. what information is delivered to which party and in which format) carried out by interaction. The mediation can be triggered by one of the interacting partners (usually by the consumer of the messages) or by an authorized agent from the environment of interacting agents.

The drawbacks of the SoS architecture involving mediators taking care of mediated interactions are also evident – increased complexity of individual systems and also increased processing overhead required for mediation. However, in the case of a complex SoS with changing structure

[2] Wiederhold, G.; "Mediators, Concepts and Practice", Studies Information Reuse and Integration In Academia And Industry, Springer Verlag, Wien, (2012)

(which the application for ensuring availability of critical services is), involving autonomous systems that may join and leave the system dynamically, the use of the concept of mediated interactions is inevitable and the advantages of this solution clearly outweigh the drawbacks.

Using the concept of mediated interactions implemented in a proactive middleware (ProWare) for the exchange of information in a SoS[3] has been proposed by the Research Laboratory for Proactive Technologies at Tallinn University of Technology. This approach makes it possible to separate the information processing from the communication (which is handled by active mediators), thus making it possible to enforce data exchange rules and security policies independently of the computation. Naturally, the semantic mediation of data is handled by the same mediators, if needed. Building on this theoretical foundation a SoS architecture has been designed and implemented, where the mediation of data is a distinct operation, which can be controlled separately from the computation. The data needs of every data consumer are described in a high level (this description can be also changed at run time).

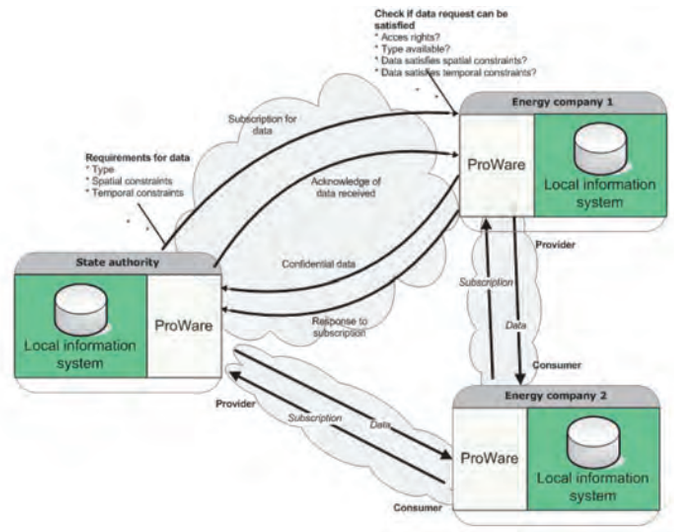


Figure 2: Data exchange controlled by ProWare

In Figure 2 the operation of the middleware is depicted in the context of energy security. The grey clouds identify individual partnerships between information providers and consumers. Any node can be an information provider or consumer. For the top left partnership between *State authority* and *Energy company 1* the interaction steps are described one by one, the explanatory texts on both ends of the *Subscription for data* message explaining what are the operations and checks performed by the consumer and the provider before data exchange can go ahead. Every data consumer discovers the appropriate data providers and requests data in the form of a subscription. After the data provider mediator has validated that the requester is authorized to have access to the requested data and that the data provider is able to provide the requested data (satisfying the specified constraints) the subscription contract is executed. The mediators take care of delivering the right information to the data consumer, while ensuring the correctness of data and enforcing access rights. This ensures that only the minimum set of data is communicated within the system and that the authorized parties are able to view the information they have been authorized to view.

Secure Multi-party Computation

If the information required for decision-making is too sensitive to be exchanged between parties also an alternative solution can be used to preserve privacy of confidential information, which is the Secure Multi-party Computation (SMC). SMC offers methods that enable autonomous parties to jointly aggregate data (compute a function over the data each party owns), while not delivering

[3] Motus, L.; Meriste, M.; Preden, J.; Pahtma, R., "Self-aware Architecture to Support Partial Control of Emergent Behavior", 7th International Conference on System of Systems Engineering, Genoa, Italy, (2012)

data to the other party, thus preserving privacy of information. One example of a practical SMC solution is the Sharemind system[4], which makes it possible to perform computations without sharing confidential information[5]. See Figure 3.

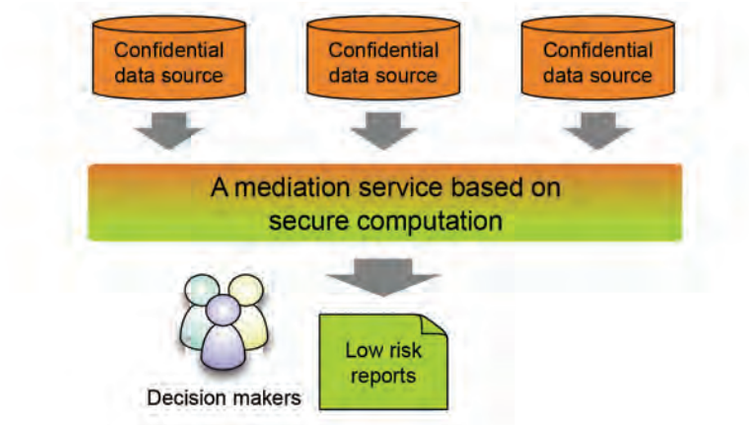


Figure 3: Secure mediation with secure computation

SMC solutions, such as Sharemind are being considered for both civil and defence use. Sharemind has been successfully used in practice for developing financial reporting services[6], public sector data analysis[7] and various prototype applications. This can be applied in the analysis of economic trends from national databases, developing better cures from data in several hospitals[8] and protecting the secrets collected from businesses and individuals.

However, also the US Defence Advanced Research Projects Agency (DARPA) implemented the Programming Computation on Encrypted Data (PROCEED) program to develop new and efficient secure computing methods.

SMC is a very powerful tool for analyzing and aggregating confidential information from individual data sources or sensors. For example, using SMC governments can more easily convince individual parties to contribute their data to improving situational awareness related to energy security.

Conclusion

As existing and new threats to homeland security, including both natural and man-made phenomena, also require new approaches to ensuring homeland security. For this reason, society should review its views on how individuals and organizations can contribute to homeland security.

The sharing of confidential commercial information is required to ensure homeland security, and it is for this reason that we should not look for reasons and ways of avoiding information sharing. Instead we should look for methods to identify the minimum subset of required information and at ways of how new and emerging technology can be applied for sharing this type of information in a manner where the commercial interests of companies are not threatened and all parties involved feel comfortable about it. The paper presented some methods and tools which can be applied for that purpose, it is a question of state requirements and the willingness of the parties involved to apply these or other tools to ensure the safety of nations.

[4] The Sharemind secure computation system. http://cyber.ee/sharemind/

[5] Bogdanov, Dan. "Sharemind: programmable secure computations with practical applications" PhD thesis, University of Tartu, 2013.

[6] Bogdanov, Dan., Talviste, Riivo. Willemson, Jan. "Deploying secure multi-party computation for financial data analysis (Short Paper)" In Proceedings of the Sixteenth International Conference on Financial Cryptography and Data Security 2012, FC 2012, LNCS, vol. 7397, pp 57-64. Springer (2012).

[7] Income analysis of the Estonian public sector. https://sharemind.cyber.ee/clouddemo/

[8] Kamm, Liina., Bogdanov, Dan. Laur, Sven., Vilo, Jaak. "A new way to protect privacy in large-scale genome-wide association studies." Bioinformatics 29 (7): 886-893, 2013.

Public-Private Partnerships for Critical Energy Infrastructure Protection: Benefits and Challenges of Information Sharing

Katerina Oskarsson

Civil-Military Fusion Centre (CFC) in NATO Allied Command Operations (ACO), Norfolk, U.S.

Critical Energy Infrastructure Protection: Who Is in the Lead?

Over the past several decades, liberalization has put a large part of the energy (and other) infrastructure in many NATO member countries in the hands of the private sector. While privatization has, in many cases, increased competition and improved efficiency and productivity, it has also heightened concerns about emergency preparedness and crisis management.[1] On one hand, market forces alone do not provide sufficient incentives for private companies to provide an adequate level of security for society as a whole. On the other hand, governments are unable to provide the public good security without assistance from the private sector. As a result, the combination of governments' diminished role in the energy sector and private companies' need to minimize costs and maximize profits creates a situation in which neither the public nor private actors alone are able or willing to provide a sufficient level of security for physical and cyber domains of critical energy infrastructure.

This is a rather alarming development, considering that former US Secretary of Defence, Leon Panetta, identified a "cyber-attack perpetrated by nation states or extremist groups" as capable of being "as destructive as the terrorist attack on 9/11."[2] Echoing this warning, the US Department of Homeland Security's Industrial Control Systems Cyber Emergence Response Team (ICS-CERT) reported that attacks against the energy sector represented the greatest share, or 53 per cent, of the 200 reported incidents across all critical infrastructure sectors in the first half of the 2013 fiscal year. Furthermore, a May 2013 report on electric grid vulnerability released by the US House of Representatives revealed that more than a dozen US power utilities reported "daily," "constant," or "frequent" attempted cyber-attacks – with more than one public power provider reporting being under a "constant state of 'attack' from malware and entities seeking to gain access to internal systems."[3]

Consequently, since neither the private nor the public sector is willing or able to provide adequate security alone, information sharing and coordination between the two sectors have become imperative in developing approaches to defending against cyber and physical energy infrastructure attacks which could threaten national security. The terrorist attacks of September 11 illustrate the impor-tance of having timely information from other sources that can give prewarnings about possible threats or attacks.

More Interconnectedness Necessitates More Information Sharing

The importance of sharing information and coordinating responses to cyber threats among various stakeholders will only continue to increase as society becomes even more reliant on interconnected computer systems to support operations of critical infrastructures. Critical infrastructure interdependence magnifies this threat, since nearly every service depends directly or indirectly on the secure supply of energy (Figure 1.). Failure in one infrastructure domain, such as electricity, can cascade quickly through the others. For example, denial of service in telecommunications would affect the energy sector's monitoring and system control capabilities such as SCADA systems, gas control centres and other systems. At the same time, without electric power, telecom services including data and all the switches, routers and firewalls would be heavily impacted.[4] Moreover, future communications networks are set to become even more interconnected through physical interconnections with electricity networks; in fact, the growth of data flowing through electricity grids is expected to exceed the growth of electricity flowing through them.[5]

1 Jan Joel Andersson and Andreas Malm, "Public-Private Partnerships and the Challenge of Critical Infrastructure Protection," in the International CIIP Handbook 2006: Vol. II, *Center for Security Studies ETH*, 2006.

2 "Remarks by Secretary Panetta on Cybersecurity to the Business Executive for National Security," *U.S. Department of Defense*, October 11, 2012.

3 "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps," *US House of Representatives*, May 21, 2013.

4 Francois Gaspard and Alain Hubrecht, "Tackling Critical Energy Infrastructure Network Interdependencies," *The Journal of Energy Security*, March 2010.

5 "The Future of the Electric Grid," *MIT*, December 2011.

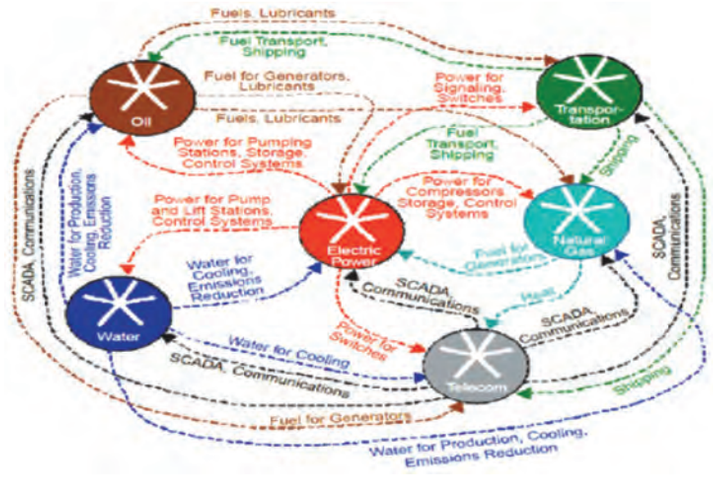


Figure 1. Interdependencies between Critical Infrastructure Sectors

Source: Rinaldi et al. (2001). Extracted from "Protecting Critical Infrastructure in the EU," Centre for European Policy Studies (CEPS), 2010.

Public-Private Partnerships (PPSs) and Information Sharing: The US Experience

For many countries, public-private partnerships (PPPs) have become the key tool to create an information-sharing framework on threats and vulnerabilities affecting the nations' critical energy and other critical infrastructures and to coordinate action between public and private stakeholders. While both the private and public sector embrace the concept of these partnerships, developing and implementing effective information sharing mechanisms has proven difficult in practice due to long-standing cultural differences between the two communities. While some PPPs have been able to establish effective information sharing relationships and coordination capabilities, others struggle to foster such partnerships due to concerns about inappropriate disclosure of information and other mismatches between private and public stakeholders' expectations and priorities. In the US the public-private partnerships for critical cyber-reliant infrastructure protection has been evolving for more than a decade, therefore providing a fertile ground to explore obstacles and best practices relevant to cyber-related information sharing between public and private stakeholders.

Generally, the main obstacle to the sharing of sensitive information between private and public stakeholders is both sectors' concern that shared information will not be protected and will subsequently be revealed. Regardless of the critical infrastructure domain, private companies are particularly worried that the sensitive information on past security incidents shared with public sector partners might not be treated with a necessary degree of confidentiality and might negatively impact their competitive advantage, reputation and the confidence of their customers if released to the public or disclosed to those companies' competitors. Some companies are also concerned about having open discussions of threats and possible litigations due to liability or other legal concerns. The risk of prosecution under antitrust regulations for sharing information with other entities constitutes another industry concern.

Information sharing is a two way street. While the private sector is often perceived as the one unwilling to share sensitive, commercial information, the public sector is equally or sometimes even more hesitant to divulge information on potential threats to the private sector since an inadvertent or intentional disclosure of classified intelligence constitutes a security risk. The energy sectors, along with information technology and financial sectors are actually quite incentivized to partner with government agencies on cyber security issues as these sector companies rely on critical electronic systems that are routinely subject to attacks by malicious actors.[6]

Private-Public Expectations Mismatch

In general, there appears to be an "expectations gap" in information sharing between the public and private sectors, with both sectors being dissatisfied with the information received from the other.[7] A GAO-conducted survey of public sector officials and 56 private sector representatives

[6] "Critical Infrastructure Partnership Strategic Assessment," *National Infrastructure Advisory Council*, October 2008.

[7] Austen D. Givens and Nathan E. Busch, "Realizing the promise of public-private partnerships in US critical infrastructure protection," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, (March 2013): 39-50.

from US cyber-reliant critical infrastructure sectors[8], including energy, reveals that private sector stakeholders participating in PPPs expect government counterparts to supply – first and foremost – usable, timely, and actionable cyber threat information and alerts, access to sensitive information, a secure platform for sharing information, security clearances, and a single centralized government source for cyber-related information that is capable of coordinating a national response and avoiding confusion.[9] Meanwhile, public partners expect their private sector counterparts to first and foremost implement plans and recommendations and supply appropriate staff and resources, in addition to providing timely and actionable cyber threat information.[10]

However, while the private sector stakeholders appear to be generally fulfilling the public sector's expectations regarding critical energy infrastructure cyber-related information sharing (Table 1), it is the less the case vice versa (Table 2).[11]

Table 1. Public Sectors' Expected vs. Obtained Services from the Private Energy Sector

Source: "Critical Infrastructure Protection," U.S. Government Accountability Office (GAO), July 2010. Modified by the author.

Services	Expected Services from the Private Sector	Extent to Which the Private Sector Provides the Expected Services
Commitment to execute plans and recommendations	Great/moderate	Great/moderate
Timely and actionable cyber threat information	Great/moderate	Great/moderate
Provide appropriate staff and resources	Great/moderate	Some
Timely and actionable cyber alerts	Great/moderate	Great/moderate
Technical expertise	Some	Some
Participation, planning for exercises and simulation	Great/moderate	Great/moderate

Specifically, although noting there are limits to the "depth and specificity" of the information supplied, the government partners reported receiving timely and actionable cyber threat and alert information from the private sector. However, as the second column of Table 2 indicates, governmental stakeholders do not necessarily meet the private actors' expectations when it comes to cyber-related information sharing. Specifically, more than 95 per cent of private sector survey respondents participating in the PPPs expect to receive timely and actionable cyber threat information and alerts from their public partners to great or moderate extent. In practice, however, only 27 per cent of them reported that they received these services to such extent.

Table 2. Private Sector' Expected vs. Obtained Services from the Public Sector

Source: "Critical Infrastructure Protection," U.S. Government Accountability Office (GAO), July 2010. Modified by the author.

Services	Expected to a Great or Moderate Extent (%)	Obtained to a Great or Moderate Extent (%)
Timely and actionable cyber threat information	98	27
Timely and actionable cyber alerts	96	27
Access to actionable classified or sensitive information	87	16
A secure information-sharing mechanism	78	21
Security clearances	74	33
Quick response to recommendations to improve partnership	69	10

Moreover, the quality of mutually provided information poses a challenge. Many business representatives view the information they obtain from the government as generic, watered-down and dated; consequently, this information is not always actionable for defending their cyber resources from advanced attacks.[12] The public sector is not able to satisfy industry stakeholders' expectations partially because of restrictions on the type of information that they can share with the private sector and because they are restricted to sharing sensitive information

[8] In addition to the energy sector, other critical infrastructure domains include (1) banking and finance, (2) communications, (3) defence industrial base (DIB), and (4) information technology (IT).

[9] "Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed," *US Government Accountability Office (GAO)*, July 2010.

[10] For the complete list of the private and public sectors' expectations see the aforementioned GAO report.

[11] Ibid.

[12] Austen D. Givens and Nathan E. Busch, "Realizing the promise of public-private partnerships in U.S. critical infrastructure protection," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, (March 2013): 39-50

only with cleared private sector actors.[13] Although the US Department of Homeland Security (DHS) and Energy (DOE) embarked on initiatives to enhance sensitive information sharing, including the opening of the 24/7 National Cybersecurity and Communications Integration Centre and efforts to increase the number of private actors from the energy industry with security clearances, it remains to be seen to what extent these initiatives address the private stakeholders' main information sharing expectations. Lastly, some industry stakeholders also felt that the government often approaches the private sector on issues that are not a priority to the private sector but are issues the government "thinks" the private sector is interested in.[14]

Best Information Sharing Practices

Although a detailed overview of best practices on information sharing is outside the scope of this paper, it suffices to highlight that the private and public organizations which succeeded in building effective information-sharing relationships pertinent to cyber threats singled out trust as the central underlying element to successful partnerships. Although there are other factors in play, the establishment of relationships based on trust that are reinforced through practice is the single most important ingredient to the willingness of private and public sector stakeholders to share sensitive and confidential information, commit resources and take rapid action when necessary. Trust can be built only over time and, first and foremost, through personal relationships.[15] As surveys indicate, trust built through regular, face-to-face meetings or forums was essential to overcome stakeholders' initial reluctance to divulge their vulnerabilities and confidential or proprietary business information. However, as a study on the effectiveness of the public-private partnership for critical infrastructure protection conducted by the U.S. National Infrastructure Advisory Council (NIAC) cautions, when trust is compromised, which the study found has been the case in several critical infrastructure sectors, it takes a long time to rebuild these relationships.[16] Illustratively, in one case, the government disclosed non-critical, but still commercially-sensitive, information to the public without first consulting the disclosure with the concerned critical infrastructure sector and without regard to the potential consequences it might have on the affected industry.[17] Lastly, the challenge of fostering trusted relationships is often compounded by reorganization and the turnover of government staff and private sector representatives.

Conclusion

Effective information sharing in the context of trusted public-private partnerships is indispensable to the protection of cyber-reliant critical energy infrastructure. Comprehensive and timely information on threats and incidents is essential to an understanding of the risks, development of preventive measures and management of a potential crisis. While each sector knows how to mitigate risks by acting on its own, the probability of serious disruptions resulting from sophisticated cyber-attacks significantly diminishes when national and international public and private stakeholders work together, communicate with one another, and share information.[18]

[13] *GAO*, July 2010.

[14] Ibid.

[15] "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection," *U.S. Government Accountability Office*, October 2001.

[16] "Critical Infrastructure Partnership Strategic Assessment," *The U.S. National Infrastructure Advisory Council*, October 2008.

[17] Ibid.

[18] "Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations, " *The National Association of Regulatory Utility Commissioners*," June 2007.

Managing editor Jonas Kukulskis
Designer Aida Janonytė

Circulation 100 units
Layout by the Publishing Section of the General
Affairs Department of the Ministry of National Defence,
Totorių str. 25/3, LT-01121 Vilnius

ISSN 2335-2272