Cybersecurity Strategies for Smart Grids

Sergiu Conovalu[1], Joon S. Park[2*]
[1] Maxwell School of Citizenship and Public Affairs, Syracuse University, Syracuse, NY 13244, USA.
[2] School of Information Studies, Syracuse University, Syracuse, NY 13244, USA.

* Corresponding author. Email: jspark@syr.edu
Manuscript submitted May 26, 2015; accepted November 3, 2015.
doi: 10.17706/jcp.11.4.300-309

Abstract: Today, the development of information and communications technologies have changed the utility landscape dramatically. In particular, electricity distribution networks rely heavily on a multitude of intelligent systems and devices that communicate among each other in much more advanced ways than in the past. As the Smart Grid is becoming nowadays a critical component in the electricity delivery system, it is important to make sure the grid is equipped with adequate security mechanisms that are able to guarantee its reliable operation and real-time information exchange within the power infrastructure. Therefore, in this paper we analyze critical cybersecurity aspects associated with smart grid services, including previous cyber-attack cases on smart grids, potential vulnerabilities/threats, and advanced cybersecurity strategies for smart grids with technical and management measures. Ultimately, while the service providers should continuously enhance the traditional security measures such as authentication, access control, authorization, data encryption, public key infrastructure (PKI), firewalls, log analysis, intrusion detection systems, and network security protocols, we propose that the advanced technical measures should 1) make smart grids survivable even under cyber attacks and internal failures; 2) employ a defense-in-depth approach; 3) employ a defense-in-depth approach; and 4) provide more scalable security measures. Furthermore, we also propose that the advanced management measures should 1) establish a cybersecurity governance strategy; 2) develop a strong incident response plan; 3) cultivate a culture of security; 4) employ a public-private partnership approach; and 5) comply with widely recognized security standards.

Key words: Critical infrastructure protection, smart grid, cybersecurity.

1. Introduction

As our world becomes "smarter" and increasingly dependent on information and communications technologies, we more and more hear about the vital necessity of critical infrastructure protection [1]-[3], many of which are not under direct control of national authorities. While this phenomenon enables new capabilities and improvements, the widespread interconnectivity entails additional risks to the operations of the national critical assets, which lately became enticing targets for cyber assaults. Various reports indicate that the intrusion and hacking tools have proliferated recently, being openly available and easy to use throughout the Internet [4]. Furthermore, communications speed and accessibility makes malevolent individuals more eager to exploit organizations' vulnerabilities and developed malicious attacks to compromise the critical infrastructure systems [5]. This aspect requires higher attention from the government and industry leaders, while potential devastating effects from individuals or groups with

mischievous purposes increasingly threaten the vital national interests.

Among the main critical infrastructures that rely heavily on automated control systems, the electric grid deserves closer attention [6]-[8]. Due to its ubiquitousness, it is spanning across all the sectors of theeconomy, including water supply, health care, transportation, emergency services, and so on, enabling them to effectively function. Therefore, as a serious damage on the electric infrastructure can have long-lasting effects and significant financial implications, it requires even more extensive security.

It is important to note that these infrastructures were not always designed with security in mind, which makes them increasingly vulnerable to malicious attacks, fraud, unauthorized access, and disruption of operations. Moreover, recent developments in the field of information and communications technologies have revolutionized the way the main utilities are managed and supplied to society. The Smart Grid paradigm, for example, has transformed the electric systems to a two-way flow of electricity and information for controlling equipment and for distributing energy [9]-[11]. In this way, the electricity supplier is able to monitor and control the electricity distribution more efficiently. Nevertheless, as many companies are very eager to adopt new technologies, security in these technologies is not always a priority for the designers [12], [13]. Yet most cybersecurity incidents remain unreported due to reputational concerns of the utility companies [14]. However, the nature of a cyber attack on the electric power grid can take various forms, from a disgruntled employee or anonymous malicious intruder to terrorist groups or even a hostile government.

Therefore, in this paper we analyze critical cybersecurity aspects associated with smart grid services, including previous cyber-attack cases on smart grids, potential vulnerabilities/threats, and advanced cybersecurity strategies for smart grids with technical and management measures.

2. An Overview of Smart Grids

The concept of Smart Grid has evolved as a necessity to modernize the electric grid due to a number of shortcomings that emerged in the power industry, such as: the challenge to match power generation toconsumer's demand; the necessity to integrate various sources of energy into the grid, like wind and solar power; and the inability for consumers to efficiently manage the use of energy for various electric appliances [4].

There is no single all-inclusive definition for what a smart grid is. However, for more clarification, the European Commission described it as *an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added* [15]. Simply put, Smart Grid integrates "smart technologies" into the electric grid to bring knowledge to power, which is capable to improve the energy efficiency through real-time exchange of information and electricity from suppliers to consumers and vice versa. Analog to the "World Wide Web", the smart grid creates a widely-distributed "Energy Web" that allows the utility to monitor and control the operation of all the interconnected elements [16].

According to the US National Institute of Standards and Technology (NIST), the Smart Grid architecture consists of seven domains (Bulk Generation, Transmission, Distribution, Customer Information and Management, Markets, Operations, and Service Provider), that are logically interconnected between each other. The conceptual model of Smart Grid is depicted in Fig. 1 [17].

In legacy power systems, electricity is generated by power plants, transmitted across the electricity grid, and distributed to residential, industrial, and commercial users. Advanced distribution technologies and broadband capabilities allow for a unified network platform by introducing three new domains: distribution, customer, and service provider [16]. Based on the Internet Protocol (IP) suite, this network provides multiple paths, from sender to receiver, to reliably connect all the devices within the electric

power infrastructure. Thus, all the interconnected elements within different domains of energy generation, distribution, and consumption are exchanging information through two-way communication channels. Price information, control commands, andmeter data are the essential information exchanged in the smart grid network, as shown in Fig. 2 [4].

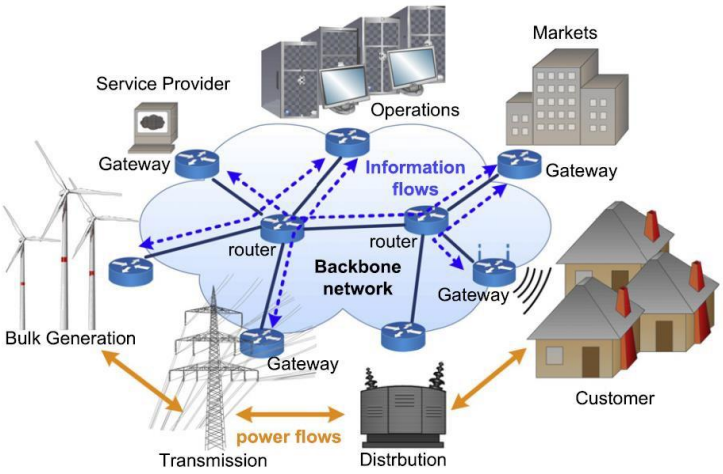

Fig. 1. NIST smart grid conceptual model.

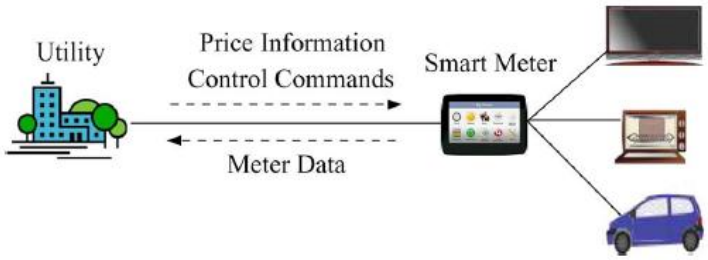

Fig. 2. Two-way information flow within a smart grid.

These improvements are designed to bring a host of benefits, both to consumers and utilities, including: better situational awareness regarding the state of the grid; predicting the level electricity demand; providing a reliable power supply, with self-healing power systems and quick recovery solutions after an outage; real-time pricing and consumption management, that allow consumers to respond to price signals; load-shedding and balancing power capabilities, to flatten the peak demand; incorporating variable power sources, like photovoltaic and wind turbines; or integrating electric vehicles into the power grid [18]. Notwithstanding, by accommodating these innovative energy concepts, the upgrade of the electric power grid rise many security concerns.

3. Cyber Attacks on Electric Power Grids

The development of information and communications technologies have changed the utility landscape dramatically. Today's information society has introduced significant improvements in the network connectivity and diversification of energy sources. Electricity distribution networks rely heavily on a multitude of intelligent systems and devices that communicate among each other in much more advanced ways than in the past [19], [20].

As most power grids are highly interconnected to the Internet nowadays, attackers can easily exploit the network from outside and inside. In Germany, for instance, an European grid operator specializing in renewable energy was the victim of an intense cyber-assault in 2012 that disrupted its Internet

communications for five days [21]. The Wall Street Journal, citing former national security officials, stated that the United States electrical grid have been penetrated by intruders from other countries, who attempted to inject software programs in the system, that would eventually allow remote access for cyber-spies to disrupt or manipulate the electrical systems and its controls [22].

Stuxnet worm [23], is considered one of the most sophisticated cyber-attack registered thus far that was able to affect the industrial control systems globally in 2010 [24]. According to Symantec Enterprise, examples of this attack have been recorded mainly in Iran, Indonesia, India, Azerbaijan, USA, and Pakistan [25].

As a result of electrical failures in 2005 and 2007 in Brazil, the country experienced one of the worst power outage. During these blackouts over 60 million people were affected and more than half of the country was deprived of electricity [26]. Although not confirmed byBrazilian officials, different sources suggest that these major disruptions were caused as a result of cyber-attacks targeting the industrial control systems [17].

Furthermore, researchers have demonstrated a successful worm attack on Smart Grids at the 2009 Black Hat Conference, including remote power on, power off, and usage reporting [15]. It is a clear message that energy infrastructures everywhere are highly vulnerable to cyber-attacks. Consequently, without adequate security procedures in place, these vulnerabilities can easily allow attackers to penetrate the network, gain access to control software, and exploit or potentially sabotage the grid infrastructure in an unpredictable way [16].

4. Cybersecurity Threats to Smart Grids

In the past, when the electric grid was a relatively closed system, and the information flow took place only in one direction, security concerns were related mainly to protecting the physical assets against unauthorized intruders. Today, enhanced two-way capabilities of communication, and the exponential increase in the number of intelligent devices, introduce additional points of access into the power grid network system. From a security perspective, this means that each component in the network can be identified as a potential avenue of attack against the system. With this high level of interconnectivity and information exchange, once a network device have been compromised, the whole network is vulnerable to "contamination" [18].

As the Smart Grid is becoming nowadays a critical component in the electricity delivery system, it is important to make sure the grid is equipped with adequate security mechanisms that are able to guarantee its reliable operation and real-time information exchange within the power infrastructure [20], [27].

Due to its critical nature, the power grid infrastructure is continuously becoming an enticing target for attackers with different capabilities and motivations, which can damage the infrastructure in many ways. Malicious intruders, market competitors, or disgruntled employees can exploit security breaches to cause information leakage, service theft, commit financial fraud, or disrupt power grid operations. Yet, more destructive threats, like massive blackouts, may come from terrorist groups or hostile governments driven by socio-political gain or cyber-warfare motives [23].

The potential threats to the smart grid can be categorized into three different cases in general, including 1) Attempts to take down the grid (i.e., attacks against Availability); 2) Attempts to compromise the electrical service (i.e., attacks against Integrity); and 3) Attempts to compromise data disclosure (i.e., attacks against Confidentiality). Enumerating the whole range of cyber-attacks to the power grid infrastructure is beyond the scope of this research, mainly due to the large-scale of threats and vulnerabilities.

5. Proposed Technical Strategies for Ensuring Cybersecurity in Smart Grids

Cybersecurity for electric power industry is becoming a growing national concern, mainly due to the critical nature of this industry. Therefore, security solutions developed for smart grid networks require more comprehensive security design than for traditional IT networks. While IT networks need to be protected more at the center of the network, where critical data is located, in smart grids, data protection is an imperative at any point in the network [27]. These differences necessitate the need for a particular approach, with proven security techniques and sound policy objectives, specific for the smart grid network. In this section, in addition to the typical cybersecurity mechanisms such as strong authentication, access control, data encryption, firewalls, and intrusion detection, we propose the advanced security strategies to be considered by governments, industry and commercial actors to ensure their cybersecurity for smart grids.

5.1. Make Smart Grids Survivable

As information systems become more complex and their interdependence increases, the availability picture becomes more complicated. Although advanced technologies and system architectures improve the capability of today's systems, we cannot completely avoid threats. This becomes more serious when the systems are integrated with Commercial Off-the-Shelf (COTS) products and services, which often have both known and unknown flaws that may cause unexpected problems and that can be exploited by attackers to disrupt mission-critical services such as smart grids. Organizations, including the DOD (Department of Defense), use COTS systems and services to provide office productivity, Internet services, and database services, and they tailor these systems and services to satisfy their specific requirements. Using COTS systems and services as much as possible is a cost-effective strategy, but such systems — even when tailored to the specific needs of the implementing organization — also inherit flaws and weaknesses from the COTS products and services used.

Traditional approaches for ensuring availability do not meet the challenges of providing assured availability in crowd sourced data resources that must rely on commercial services and products in a distributed computing environment. Therefore, we need an advanced availability approach for mission-critical systems. In order to provide the availability of smart grids, we can apply our previous framework for survivability in mission critical systems [28]-[30]. We defined our definition of survivability, discussed the survivability challenges in component-sharing in a large distributed system, identified the static and dynamic survivability models, and analyzed their trade-offs. Consequently, we proposed novel approaches for component survivability. Finally, we proved the feasibility of our ideas by implementing component recovery against internal failures and malicious codes based on the dynamic model. In this way, we can make the smart grid continue its mission even with cyber-attacks or internal failures.

5.2. Provide More Scalable Security Measures

Current information systems have become more complex and better integrated with other systems. Usually, large distributed systems such as smart grids support many customers and users in various contexts. Nodes may run in heterogeneous environments under different constraints. The complexity of the security aspects in information systems is increasing, which brings a serious scalability problem to security services and management.

The complexity and large scale of control demand an efficient mechanism to deal with which user has what privileges for which contents under what conditions. A conventional identity-based approach may suffice for this purpose if the application is small and involves a limited number of users, and if privilege assignments to users are stable. However, in a large-scale system that supports many users from different organizations requiring different kinds of privileges, the identity-based approach would be severely inefficient and too complicated to manage because the direct mapping between users and privileges is

transitory. Therefore, more scalable security approaches, especially for large systems, are needed for smart grids.

5.3. Embed Security Controls by Design

It is generally acknowledged that security must be engineered into every element of the smart grid system from the earliest stages of the design process. Yet, in many cases, security is the latest concern for equipment manufacturers and is only alerted after the system proves to be vulnerable [3]. Utility suppliers and manufacturers of products of services must be aware of these adverse consequences that may result in huge financial losses for the industry. Accordingly, authentication, authorization, and encryption requirements should be a must for all products and services designed for the electric power industry.

5.4. Employ a Defense-in-Depth Approach

One of the basic security principle for the smart grid is converting "wholesale" attacks, which may put the entire system at risk, into "retail" attacks, which are limited to a very small scope [31] based on the isolation and defense-in-depths approach. The smart grid is a conglomerate of multiple networks with a multitude of communication levels between suppliers, operators, customers, and service providers. Therefore, multiple layers of defense and isolated security domains should be in place to mitigate the wholesale attacks from occurring against the entire system.

5.5. Enhance Traditional Security Measures

Since the reliability and robustness of smart grid services heavily depend on information and communication technologies and their cyber infrastructure, the service providers have been using traditional security measures, such as authentication, access control, authorization, data encryption, public key infrastructure (PKI), firewalls, log analysis, intrusion detection systems, and network security protocols.However, there is a significant gap between their limitations and the new security requirements due to the evolution of technologies and environments. In particular, considering the large scalability and mission-critical availability of smart grids, we should continuously enhance the traditional security measures in order to make them more scalable and robust. For instance, by using the Role-based Access Control (RBAC) mechanisms instead of identity-based access control in a large grid environment, we can provide more scalable access control services [32], [33].

6. Proposed Management Strategies for Ensuring Cybersecurity in Smart Grids

Security mechanisms discussed above are crucial for protecting the smart grid against cyber-attacks, however, the technical solutions only are not enough to build a comprehensive security environment [34]. Consequently, in addition to technology, security encompasses consistent policies, standards, procedures, effective partnerships, and an increased level of cyber awareness among the main stakeholders.

6.1. Establish a Cybersecurity Governance Strategy

A prerequisite for a reliable smart grid infrastructure is the development of a robust enterprise cybersecurity strategy that provides a comprehensive security governance, identifies potential risks to the critical smart grid assets, assigns roles and responsibilities for managing security within the grid, as well as establishes monitoring and evaluation procedures to ensure that all the security standards and guidelines are consistently maintained and followed.

6.2. Develop a Strong Incident Response Plan

Being a strategic target, it is inevitable that at some point the grid will have to face a sophisticated attack to its critical assets. The seriousness of a potential harm is even more critical if it involves an attack aiming

to cause a massive country-wide or regional blackout. An adequate response strategy in place, and the rapidity of response, is of crucial importance in such situations [9], [15]. The plan should identify the critical assets that require immediate attention in case of emergency, and prioritize the event response based on the nature of the attack. Ultimately, the power grid must be able to continue its operations or, at least, recover quickly after a disruption.

6.3. Cultivate a Culture of Security

The human factor represents another opportunity for vulnerability that can become an open door for cyber-attacks. A culture of cyber security among all the stakeholders of electricity power industry will ensure a sustainable electricity delivery system. The smart grid requires "smart" and trained people who can understand the system functionality and are able to adequately implement security policies and apply the existing security standards in the grid's operational settings. Educating customers is also essential to minimize possible security breaches into the system [18]. Governments can encourage a cybersecurity culture by developing ongoing collaboration and trusted relationships with industry.

6.4. Employ a Public-Private Partnership Approach

Generally, critical energy assets and infrastructures are owned and operated by private companies which are accountable to consumers for ensuring the continuity of their electrical power supply. On the other hand, the national security and defense of critical infrastructures from domestic and foreign threats is the core responsibility of the government. Nevertheless, neither the government nor the industry can guarantee the complete security of the entire electric infrastructure. The question is how governments and the industry address this serious and ongoing challenge? A Public-Private Partnership approach might be the answer. According to President Obama's policy on cybersecurity *"the public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure"* [35]. Sustainable collaboration and trusted relationships need to be developed between all the parties involved in the ownership, operation, and regulation of the interdependent electricity infrastructures. Technically, the private owners and operators of the energy assets are in better position to secure their infrastructure. However, the smart grid technology introduces new products and services which are usually deregulated and owned by different entities [6]. We know that energy regulation is a government function, and therefore, the regulatory body of the government is charged with setting security standards and then the private sector is held accountable to meet these specified standards [36]. Moreover, academia, vendors, service providers, manufacturers, standardization organizations, asset operators, and other stakeholders that may provide essential expertise, should work closely together to identify the cyber security vulnerabilities and to mitigate the potential risks. As such, the expertise, information, and cost sharing between the various stakeholders of the energy sector will ensure that the security issues are approached from every angle in a coordinated way and technology resources are maximized to meet the security objectives.

6.5. Comply with Widely Recognized Security Standards

New *standards* and *regulatory* actions have been developed lately aimed at addressing the newly emerged threats of cyber-attacks on critical infrastructure. Therefore, it is extremely important for governments to work consistently with national and international standardization bodies, and industry organizations, as they are able to provide guidance framework and technical solutions on cybersecurity related issues, including for the electric power industry.

7. Conclusion

Nowadays traditional power systems are embracing smart grid technologies to enhance energy efficiency, improve system reliability and resilience, and introduce better quality electricity services. However, if notproperly deployed and managed, the benefits resulted from this technological breakthrough might turn into a nightmare for government and industry leaders. We have seen that the power grid in different countries could be extremely vulnerable to cyber-attacks and the effects might be severe. The negative externalities that may result from a successful cyber-attack on the power grid can be devastating and can seriously impact citizens' safety and the national economic security. Therefore, being labeled as a critical infrastructure, smart grid requires a holistic security approach to ensure maximum reliability and availability of electric energy. However, absolute security is not achievable in our real world of permanent technological innovation, and there is not a one-size-fits-all approach to address this complex issue.

Cybersecurity for electric power sector is a critical issue and one of the main challenges facing the energy industry today. To prevent potential threats targeting electrical grid infrastructure, it must be carefully approached as one of the most vital policy and technology topics on governments' agenda. National governments should increase their awareness on risk prevention and response, adopt innovative practices in policy development, and adapt their legislation to pursue those involved in cyber-crimes against their critical infrastructures. Governments should build effective partnerships with infrastructure owners and operators to define a common security vision and establish mutually agreed-upon protective and recovery measures. In addition, security must be part of the design criteria for critical infrastructure development, particularly the electrical grid, in order to prevent any disruptions or restore its functionality under the best possible conditions.

Acknowledgment

Sergiu Conovalu would like to thank Professor Leonard Coburn for his guidance and advice provided during hisclass on Global Energy Policy, as well as Professor Joon S. Park for his valuable insights and shared knowledge on information security matters.

References

[1] EC. (2013, July). European Commission: Critical Infrastructure. Retrieved July 13, 2013, from http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

[2] OECD. (2008). OECD recommendation of the council on the protection of critical information infrastructures, OECD Ministerial Meeting on the Future of the Internet Economy, Seoul.

[3] IBM. (2012). *Best Practices for Cybersecurity in the Electric Power Sector*, IBM Corporation, Somers, NY.

[4] GAO. (2004). *Critical Infrastructure Protection. Challenges and Efforts to Secure Control Systems,* United States General Accounting Office, Washington.

[5] Baker, S., Filipiak, N., & Timplin, K. (2011). *In the Dark. Crucial Industries Control Cyberattacks,* McAfee & Center for Strategic and International Studies, Santa Clara, CA.

[6] Mo, Y., Kim, H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE.*

[7] Spoonamore, S., & Krutz, R. (2009). *National Security Risks and Concerns of Smart Grid*.

[8] OE. (2013, June). Office of Electricity Delivery & Energy Reliability, Retrieved June 5, 2013, from http://energy.gov/oe/technology-development/smart-grid

[9] NIST. (2010). *Guidelines for Smart Grid Cyber Security, 3*, National Institute of Standards and Technology., U.S. Department of Commerce.

[10] EC. (2011). *Smart Grids: From Innovation to Deployment,* European Comission, Brussels.

[11] Lu, X., Lu, W., C. Wang, *et al.* (2010). Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid. *Proceedings of the 2010 Military Communications Conference*.

[12] Ponemon Institute. (2011). *State of IT Security*, Study of Utilities & Energy Companies, Ponemon Institute LLC.

[13] Rogers, W. (2011, April). How to be smart about our energy and cyber security goals. Retrieved June 10, 2013, from http://www.cnas.org/blogs/naturalsecurity/2011/04/how-be-smart-about-our-energy-and-cyber-security-goals.html

[14] McAfee & CSIS. (2010), In the Crossfire: Critical infrastructure in the age of cyber war. Retrieved July14, 2013, from http://resources.mcafee.com/content/NACIPReport

[15] Metke, A. R., & Ekl, R. L. (2010). *Smart Grid Security Technology,* Motorola, Inc., Schaumaburg, IL.

[16] EPRI. (2009). *Report to NIST on the Smart Grid Interoperability Standards Roadmap,* Electric Power Research Institute.

[17] CBS. (2010, June). *CBS News Cyber War: Sabotaging the System,* retrieved June 18, 2013, from http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[18] Hayden, E. (2010). *There is NO SMART in Smart Grid without Secure and Reliable Communications, Verizon Business Energy and Utility Solutions.*

[19] Pearson, I. L. (2011). Smart grid cyber security for Europe, *Energy Policy,* 5211-5218.

[20] Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 1344-1371.

[21] Euractiv. (2012, December). European renewable power grid rocked by cyber-attack. Retrieved July 15, 2013, from http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541

[22] Gorman, S. (2009, April). *Electricity Grid in U.S. Penetrated by Spies.* Retrieved July 18, 2013, from http://online.wsj.com/article/SB123914805204099085.html

[23] Knapp, E. D. (2011). *Securing Industrial Network Security: Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems,* Waltham: Elseiver.

[24] BIPR. (2012). *Cybersecurity Issues and Policy Options for the U.S. Energy Industry,* Institute for Public Policy of Rice University.

[25] Symantec. (2010, July). *W32. Stuxnet.* Retrieved July 2, 2013, from http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

[26] Mylrea, M. (2009, November). *Brazil's Next Battlefield: Cyberspace*. Retrieved June 24, 2013, from http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/

[27] Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy*.

[28] Park, J. S., Chandramohan, P., Suresh, A. T., Giordano, J., & Kwiat, K. (2013). Component survivability for mission-critical distributed systems. Special issue on cloud and pervasive computing. *Journal of Supercomputing*, *66(3),* 1390-1417.

[29] Park, J. S., & Chandramohan, P. (2004). Static vs. dynamic recovery models for survivable distributed systems. *Proceedings of the 37th Hawaii International Conference on Systems Sciences (HICSS-37)* (pp. 1–9). Big Island, Hawaii. IEEE Computer Society.

[30] Park, J. S., Jayaprakash, G., & Giordano, J. (2006). Component integrity check and recovery against malicious codes. *Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications (AINA)* (pp. 466–470). Vienna, Austria, April 18-20. IEEE Computer Society.

[31] SSN. (2012). *Smart Grid Security Myths vs. Reality,* Silver Spring Networks, Redwwod City.

[32] Park, J. S., An, G., & Liu, I. (2011). Active access control with fine-granularity and scalability. *Security and Communication Networks*, *4(10),* 1114-1129.
[33] Park, J. S., Sandhu, R., & Ahn, G. J. (2001). Role-based access control on the Web. *ACM Transactions on Information and System Security (TISSEC)*, *4(1),* 37–71.
[34] DOE, & DHS. (2012). *Electricity Subsector: Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0,* Department of Energy; Department of Homeland Security.
[35] White House. (2009). *Cyberspace Policy Review*. Retrieved June 25, 2013, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.p
[36] Tagert, A. C. (2010). *Cybersecurity Challenges in Developing Nations,* Carnegie Mellon University, Pittsburg, PA.

Sergiu Conovalu was born in Mindic, Republic of Moldova, in 1984. He received the B.E. degree in electronic engineering from the Military Technical Academy, Bucharest, Romania, in 2007, and the executive master's degree in public administration from the Maxwell School of Citizenship and Public Affairs, Syracuse University, New York, US, in 2013. He also holds a certificate of advanced studies (CAS) in e-government management and leadership from the School of Information Studies and CAS in security studies from the Institute for National Security and Counterterrorism, both pertaining to Syracuse University. In 2007, he started his military career as an engineer within the National Army of the Republic of Moldova at the Information and Communication Center of the Main Staff of the National Army. In 2010, he transferred to the Ministry of Defense, serving as a policy analysis specialist, where he was still employed when submitting this paper at ICINS 2015.

In December 2014, Mr. Conovalu participated at the 14th Young Faces Conference: Cyber Security Winter School, co-organized by DCAF and DiploFoundation in Petnica, Serbia, where his research paper was published under the name: Public Policy Tools to Promote Cybersecurity for Critical Infrastructure Protection.

Joon S. Park is a professor at the School of Information Studies, Syracuse University. Over the past decades he has been involved with theoretical/practical research and education in Cyber Security. He is a Syracuse University's point of Contact (POC) at the Center of Academic Excellence (CAE) in Information Assurance/Cyber Defense (IA/CD) and CAE-R (Research), which are designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS). He served as the founding director of the Certificate of Advanced Study (CAS) in Information Security Management (ISM) program from 2003 to 2013.