Journal of Information Systems and Technology Management – Jistem USP
Vol. 14, No. 3, Sep/Dec., 2017 pp. 385–400
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752017000300006

CYBER SECURITY GOVERNANCE AND MANAGEMENT FOR SMART GRIDS IN BRAZILIAN ENERGY UTILITIES*

Daniel Jardim Pardini https://orcid.org/0000-0003-0422-1639
Astrid Maria Carneiro Heinisch https://orcid.org/0000-0003-1092-9780
Fernando Silva Parreiras https://orcid.org/0000-0002-9832-1501
Universidade Fumec, FACE, Belo Horizonte, MG, Brasil

ABSTRACT

The event of cyber security in critical infrastructures has aroused the interest and the worry of energy utilities, government, regulatory agencies, and consumers as well as of the academic and research institutions. If on one hand it is prominent the vulnerability of the cyberspace, which augments the risk of attacks in the organizational environment, on the other hand, the research leading to alternatives for the governance and management of these critical structures are still too incipient. This study aims at building a theoretical-empirical model of cyber security governance and management and testing it along with academic experts and professionals from the energy sector. By using the Delphi method and statistics techniques for validation, an assessment instrument was developed based on both the constructs: governance and management; and nine dimensions with their respective variables that allowed for an analysis of the situation of the Brazilian energy utilities regarding the protection of their cyberspaces. The contribution of the article reaches two fronts: a conceptual and empirical one as it expands and systematizes the knowledge about aspects of the governance and management of cyberspaces; and a methodological one as it proposes measuring those dimensions in energy utilities.

Key words: Governance, Management, Cyber Security, Operational Risk, Smart Grids.

Manuscript first received: 2016/Dec/17. Manuscript accepted: 2017/Dec/16

Address for correspondence:

Daniel Jardim Pardini, Professor Titular, Programas de Doutorado e Mestrado em Administração e Sistemas de Informação e Gestão do Conhecimento, FACE, FUMEC, MG, Brasil. E-mail: pardini@fumec.br

Astrid Maria Carneiro Heinisch, Pesquisadora e Gerente de Negócios da FITec Inovações Tecnológicas, FACE, FUMEC, MG, Brasil. E-mail: aheinisch@fitec.org.br

Fernando Silva Parreiras, Professor e Coordenador do Programa de Doutorado e Mestrado em Sistemas de Informação e Gestão do Conhecimento da FACE-FUMEC, MG, Brasil. E-mail: fernando.parreiras@fumec.br

*Best Paper Award - Information Management Track in SEMEAD - Management Conferences, 2016, FEA-USP, Brazil

INTRODUCTION

Besides the extensive literature of technical and normative nature that deals with the critical technological structures aimed at the protection of security systems in organizations, the studies on cyber security governance and management are practically unknown, especially concerning the energy sector.

Energy provisioning is considered an essential service, and a key element for the improvement of the quality of life of the population, enhancing social inclusion and sustainable development (Coutinho, 2007). As the demand for energy has been raising at a higher rate compared to its capacity, it is noticeable that over the last 50 years the energy provisioning system worldwide has used technologies developed in the 40s and 50s as fundament; which frequently leads to the saturation of the system (Gellings, 2009).

Many actions have been taken as an attempt to modernize the energy sector and mitigate the risks of power outages. Among them, it is emphasized the implementation of smart grids, object of the present study, aiming at making the electric grids more resilient, safer, more efficient and reliable in the future. The smart grids consist of the increased use of digital information and control technology to improve reliability, security and efficiency to the electric grid (MIT, 2011).

The security of smart grids, also called critical infrastructures, in their physical and operational layers follow the traditional means of protection. However, it is in the cybernetic layer, technological infrastructures for monitoring transmission and distribution of electric grids, that the major concerns for the service providers of the electric sector can be found. This is due to the increasing system vulnerabilities and due to the fact that it is unknown if organization would be prepared to face these threats (Coutinho, 2007).

It is notorious that the absence of a well-defined theoretical basis still prevails, especially for the conceptions of corporate governance and management within the scope of cyber security. The research is evident taking this conceptual gap: What would be the dimensions of corporate governance and management in energy utilities for the cyber security of smart grids? Therefore, the intention is to broaden the knowledge over the management of this new concept of electric energy. This paper targets at identifying, evaluating and describing the dimensions of cyber security governance and management in Brazilian energy utilities regarding the smart grids.

The conceptual framework in the environment of smart grids is handled throughout this article, as well as the conceptions of governance and management in the cyberspace and their dimensions, the theoretical-empirical model and the methodology for research, the validation and application of the model in the scope of Brazilian energy utilities and the conclusion of this study.

THE CONTEXT OF SMART GRIDS: THE CYBERSPACE AND THE THREATS POSED TO ORGANIZATIONAL ENVIRONMENTS

A smart grid is a system for electric grid transmission and distribution using remote sensing, monitoring, bidirectional communication and control systems distributed in the energy provisioning (Newton's Telecom Dictionary, 2009). The control system of electric grid incorporates information and telecommunication technologies intending to monitor the entire energy value chain – generation, transmission, distribution and consumption (MIT, 2011; NIST, 2010; Sorebo & Echols, 2012).

In order to ensure the reliability and operational efficiency of the smart grids, the utilities involved shall perform a dynamic optimization of resources and operations in the network towards cyber security, developing and incorporating real time, automatized and interactive tecnologies; aimed at the demand and generation of energy, using technologies for peak shaving and advanced energy storage, providing relevant information about the measurement of energy consumption and control options for the consumer (MIT, 2011).

In addition to consumers and energy utilities, the stakeholders in the implementation and application of the smart grids are the regulatory agencies, the service providers, the information technology developers and the researchers and development institutions (R&D) (Momoh, 2012). The identification and mapping of the interactions between the organizations and its stakeholders can be helpful in understanding the roles that the stakeholders and other elements play on the organizational risks.

Hatch & Cunliffe (2013) identify three components to explain the dynamics of interactions between the organization and the environment: the interorganizational network, the general environment and the global international environment. As of the interorganizational network, any organization interacts with other organizations either to hire employees, secure working capital, gain knowledge or to structure, rent or purchase infrastructures and equipment.

Taking into account the general environment, consider those dimensions that directly or indirectly affect organizational activities, as follows: social, cultural, legal, political, economic, technological and physical variables. The global international environment includes the aspects beyond the national constraints of those organized at a global scale. Here we emphasize the institutions that handle common interests and diverse general environments (Hatch & Cunliffe, 2013). If we wanted to define the environmental layers for the cyberspace of smart grids in energy utilities we would have the draft presented in Figure 1 with the respective threats from external environments.

The cyber environment is conceived as as the collection of information and communication technology infrastructures (ICT) of an organization, including the Internet, telecommunication networks, computer systems, personal devices, embedded sensors, processors and controllers (Bodeau et al., 2010).

Provided the context, two big components of the cyber environment can be identified: the communication network which supports the data on the control system and controls the actual physical processes and the internal computer network environment utilized for non-critical operations and administrative tasks (Aitel, 2013). Besides these two infrastructures, it is important to include the operational data referring to critical organization processes. The criticality of the information is also reflected by the criticality of the assets involved in data exchange, also called critical cyber assets. These are the assets contributing to increase the level of automation and system intelligence, although they become more exposed to the actors of this environment (ANSI, 2009; Bodeau et al., 2010; MIT, 2011; NIST, 2010; Sorebo & Echols, 2012).

By integrating their infrastructures to the cyber environment, the organizations create an area of intersection between the organization environment and the cyber environment and then become subjected to external threats. Threats that differ in many perspectives from organizational environment approaches. Table 1 presents a taxonomy of operational risks that might affect the cyberspace.

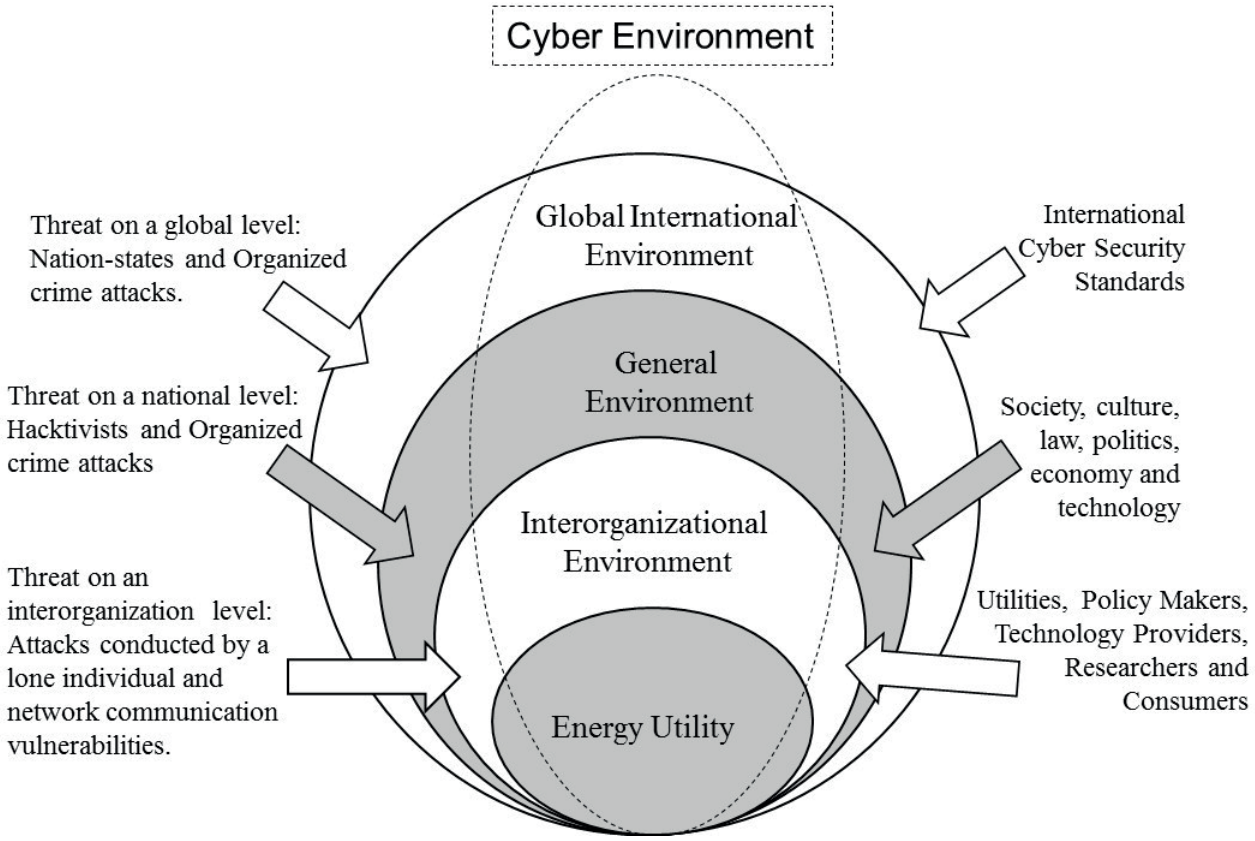

Figure 1. The cyber environment in the organizational context

Table 1. Taxonomy of cyber operational risk

Actions of People	System and Technology failures	Failed Internal Processes	External events
Inadvertent	**HW**	**Process design or execution**	**Disasters**
Errors	Capacity	Process flow	Weather events
Mistakes	Performance	Process documentation	Fire
Omissions	Maintenance	Roles and responsibilities	Flood
	Obsolecence	Notifications and alerts	Earthquake
Deliberated	**SW**	Information flow	Unrest
Fraud	Compatibility	Escalation of issues	Pandemic
Sabotage	Configuration management	Service level agreements	
Theft	Change control	Task hand-off	**Legal issues**
Vandalism	Security Settings		Regulatory compliance
	Coding practices	**Process control**	Legislation
Inaction	Testing	Status monitoring	Litigation
Skills		Metrics	
Knowledge	**Systems**	Periodic review	**Business issues**
Guidance	Design	Process ownership	Supplier failure
Availability	Specifications		Market conditions
	Integration	**Supporting Process**	Economic conditions
	Complexity	Staffing	
		Funding	**Service dependency**
		Training and development	Utilities
		Procurement	Emergency services
			Fuel
			Transportation

Source: Adapted from Cebula & Young (2010, p. 3).

Cyber environment invaders are categorized based on the motivation for the attacks (a hacker or a group). The invader can be a nation, a group of activists, a group of criminals, or an ordinary individual with personal reasons. The objectives also differ, among others: a) to interrupt and destroy technology infrastructures, b) to gather information about operations, projects, business plans and intellectual property or access to a network, c) for financial gain, d) to attract publicity, e) to revenge or simply to prove the ability to hack a particular company. Thus, the means of attacking involve gaining on-site physical access to the control system, violating the operator's internal computer network and mapping the data and connections from the control system aiming at publishing or selling them, enabling others to use it (Aitel, 2013).

GOVERNANCE, MANAGEMENT AND NORMATIVE MODELS OF CYBER SECURITY

Cyber security refers to all the approaches intended to protect data, systems and networks from deliberate and accidental attacks and yet, if required, from the lack of preparation for the recovery of these infrastructures (MIT, 2011). It is a collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that can be used to protect the cyber environment as well as the assets of the users and organizations (ITU-T, 2008). Unlike the conventional models of information security, the objective of cyber security is to reduce the risks concerning the dependency of the cyberspace and the presence of adversarial threats (Bodeau et al., 2010).

Two constructs of cyber security are pivotal to this study: governance and management. The term governance is used to describe a system for controlling or regulating, which includes the process of naming controllers and regulators. Whereas the term Management is adopted to refer to the communication of the responsibilities of controllers and regulators, by using executive actions (Turnbull, 1997). Governance consists of the definition of criteria for decision-making, setting rules, responsibilities, and the boundaries of the autonomy and actions of the involved parties (Roth et al., 2012). The role of governance is not managing, but defining the scope of management.

Considering cyber security, the governance focuses on what the organizations should do differently or adding to what is accepted as good information security governance practices. Using this methodology, the level of readiness of the organization for cyber security is analyzed under the perspective of the following approaches (Bodeau et al., 2010): strategic integration, extending the cyber security strategy beyond the organizational environment, risk mitigation, adaptability and agility in decision making to face cyber-attacks against corporations, senior engagement and commitment from the shareholders and the board of directors and cyber risk analytics.

As of the strategic integration dimension, it is discussed to what extent the cyber security strategy is integrated with other strategies, the mission and risk management of the organization. The perspective of adopting strategies that use resources originating from external environments refers back to the commitment of the company with its partners, suppliers and customers to share knowledge about threats that may affect the organizational activities. In the approach towards mitigating the cybernetic risks, the reference is structuring actions to prevent threats in a normative view of the best practices to avoid unpredicted attacks. Regarding the variable agility in decision making, the conditions provided by the organization to delegate responsibilities in fighting the interests of competitors in violating the cyberspace of the organization are observed. The dimension commitment

of the board of directors indicates the involvement of shareholders, counselors and executives in monitoring the implementation of cyber security actions. Finally, in the analysis of cybernetic risks, it is discussed how the models of threats to the organization environment should be managed and updated (Allen, 2005; Bodeau *et al*., 2010).

In this scenario of cyber security governance, it is still possible to list the recommendations for corporate governance of the OECD - Organization for Economic Cooperation and Development (OCDE, 2004). The document shows the importance of respecting the interests and providing equitable treatment for shareholders; transparency, quality and integrity when releasing information; making use of the responsibilities of the executive board; improving the compliance with legislation; and the effectiveness of regulatory and supervision agencies in monitoring the activities of the sector.

By means of recommendations and guidelines from the OECD it is possible to elaborate on a set of dimensions from corporate governance applied to cyber security governance for smart grids, as follows:

- The effective legal and regulatory basis in cyber security governance for Smart Grids;
- The relations with stakeholders of Smart Grids in cyber security governance;
- The rising standards of transparency in accordance with corporate governance principles of cyber security management for Smart Grids;
- The equitable treatment of shareholders;
- The responsibilities of the Executive Board in energy utilities regarding cyber security governance for Smart Grids.

In the outline of governance, cyber security management has ANSI/ISA99 (America National Standard Institute) as a normative pillar since it handles security in industrial automation and over the years it has become a key international standard to enable the protection of critical industrial infrastructures. It is a normative management instrument that directly influences the security and health of people and the environment. Probably in the near future, they will reach other areas of application, wider than the ones towards industrial automation.

For operating cyber security management, actions beyond projects are required from the organizations in order to enable the achievement of a higher security level for their processes. The continuous management of security issues is a demand to keep the desired level. Projects are capable of raising the security level however keeping it is improbable using initiatives that are not often aligned with the strategy of the organization. The effective implementation of a cyber security program comprises effective risk management, system development and its maintenance, management information, planning and being able to respond to critical incidents (ANSI, 2009). It is also worth adding the need of preparing and qualifying the human resources involved.

Based on the cyber security governance and management dimensions identified through the models mentioned as theoretical references, a theoretical-methodological model was elaborated to be adopted for the investigative process and field research (Figure 2).

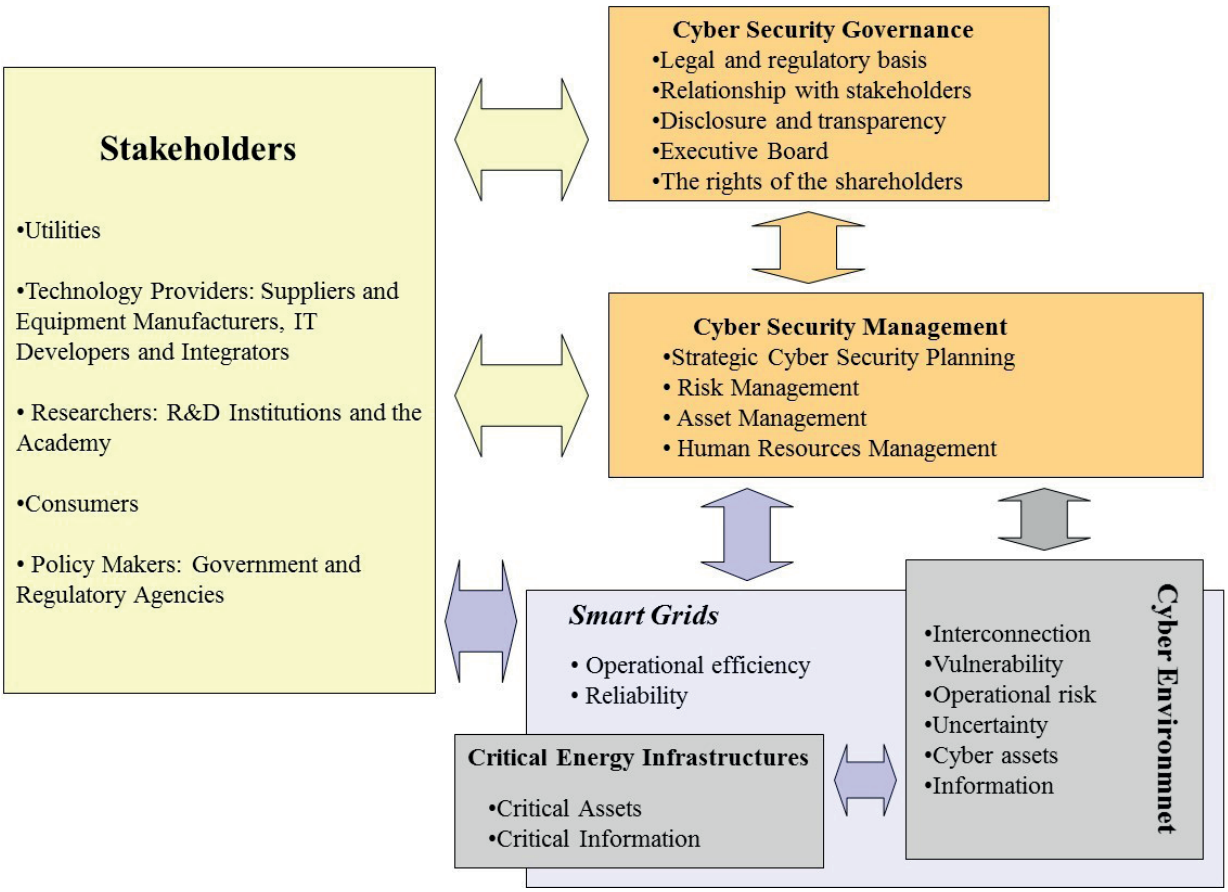

Figure 2. Theoretical-methodological model

METHODOLOGY

This study has an exploratory nature due to the theoretical insipience of the area of investigation and to the need to look into the empirical phenomenon in the sense of constructing and systematizing concepts about the topic (Cooper, Schindler &Sun, 2006). The methodological path was traced in two phases. In the first moment the variables in the researched literature were retrieved composing the dimensions of the theoretical-methodological model proposed to structure the questionnaire. The method adopted was the bibliographical research.

The instrument of measurement was validated and tested afterwards along experts from the electric sector having as a reference Brazilian energy utilities. The Delphi method was applied with experts (academic, researchers and professionals) and statistics tests (factor analysis, sphericity, t from Student, Levene, Mann-Whithney and analysis of variance) for the structuring and validation of the questionnaire. The option for the Delphi technique derives from the potential of the instrument in converging to a consensus (or almost) among the experts about the object of this research (Wright & Giovanazzo, 2000)

Data Collection

The identification and description of the dimensions composing cyber security governance and management became evident having a fundament the OECD (2004) orientations concerning

corporate governance, and the researches from international institutions and academics, referring to cyber security management (ANSI, 2009; Bodeau et al., 2010; DOE - US Department of Energy; DHS - US Department of Homeland Security, 2012).

Therefore, 9 dimensions of analysis reflected in 38 variables were identified. Five dimensions of cyber security governance: 1) legal and regulatory basis (normative dimension); 2) interactionist-relational; 3) transparency and inspection; 4) executive board and 5) the rights of the shareholders (OCDE, 2004; OCDE, 2005; Bodeau et al., 2010; DOE - US Department of Energy; DHS - US Department of Homeland Security, 2012. Four dimensions of cyber security management: 1) cyber security strategic planning; 2) risk management; 3) asset management and 4) human resources management (ANSI, 2009; Bodeau et al., 2010; DOE - US Department of Energy; DHS - US Department of Homeland Security, 2012).

A preliminary version of the questionnaire was elaborated and submitted to the analysis of four experts (professionals involved in projects of R&D applied to cyber security for Smart Grids, developed as a partnership working with energy utilities) selected for the sake of convenience for the validation of the dimensions and variables identified. A first version of the questionnaire was finished and structured as an online form in the *Google Docs* website for the first-round answers. At first, 35 experts were contacted and 24 of them willingly joined the research.

The answers obtained in the first round allowed the experts to form a preliminary opinion about the cyber security governance and management practices in energy utilities, although the results produced by the Google Docs tool reflected a significant lack of consensus among the experts in most of the statements. The results from the first round served then as subsidies for elaboration of a new form applied in the second round of the research with the experts who participated in the first round.

Data treatment

The forms filled in by the experts in the second round were stored in a spreadsheet, grouping the answers and comments related to every statement. Through the tool Survey Monkey, the data were statistically worked on, so as to allow an analysis of the consensus relating to each variable.

The analysis of the consensus was carried out from the calculation of the median and the quartiles. The arrival at consensus was measured by the distance between the first and the third quartiles of answers and the value of the median (Wright & Giovanazzo, 2000). In this study, for all the statements presented in the form for the second round of the survey there was an attempt to obtain a distance from the maximum of a unit of the scale between the first quartile and the median and the third quartile and the median.

Afterwards, through confirmatory factor analysis, the suitability of the proposed grouping was verified in various variables in the respective dimensions of cyber security governance and management. However, the KMO (Kaiser-Meyer-Olkin) and Bartlett tests were performed to check the adequateness of the data. In addition to that, the t for Student test was applied to verify the different opinions regarding the governance and management dimensions between the groups of respondents and the Levene test to assess variances obtained. Also, the Mann-Whitney test was used to compare two independent groups as well as the Shapiro-Wilk normality test (Mesquita, 2010).

With the validated evaluation instrument, the analysis of cyber security governance and management in Brazilian energy utilities was described. This analytical diagnostic was carried out by using quality indicators that exemplify the practice, the relevance, the performance and the risk

of every variable composing the dimensions of the constructs governance and management. The following topic deals with the search results.

ANALYSIS OF THE DIMENSIONS OF CYBER SECURITY GOVERNANCE AND MANAGEMENT OF SMART GRIDS FOR BRAZILIAN ENERGY UTILITIES

The results of study are presented in two phases. The first refers to the validation of the theoretical-methodological model and the instrument for measuring the two constructs, cyber security governance and management for smart grids and their respective dimensions and variables. Next, by looking into the opinions of the experts evidenced in the application of the Delphi method, the situation of Brazilian energy utilities concerning the protection of the cyberspace of smart grids is analyzed.

Validation of the evaluation instrument of the dimensions and variables of the theoretical-methodological model

In order to check the adequateness of the grouping of variables in nine dimensions extracted from the management and governance constructs, the confirmatory factor analysis was adopted. For the factor analysis of every dimension, the simple average of four questions referring to every statement in the evaluation instrument was calculated: practice, relevance, performance and decrease of the risk variable for the energy utilities. Proceeded to KMO (Kaiser-Meyer-Olkin) and Bartlett data adequateness tests. Table 2 shows the tests results and the factor analysis for the nine dimensions, indicators that certify the validation of the model.

Table 2. Indicators for the validation of the theoretical-methodological model

Governance and Management Dimensions	KMO	Bartlett	Pvalue	Variance	Variance (%)
1) Legal and regulatory basis (normative dimension)	0,838	44,241	0	3,197	79,92%
2) Interactional dimension	0,683	20,065	0	2,263	75,42%
3) Transparency and inspection (dimension stakeholders)	0,419	23,941	0	2,091	70%
4) Executive Board dimension	0,675	14,287	0,003	2,11	70%
5) The rights of shareholders	0,5	5,19	0,023	1,533	76,67%
6) Cyber security strategic planning	0,666	95,473	0	5,053	63%
7) Risk management	0,801	111,246	0	5,503	68,79%
8) Asset management	0,705	24,029	0	2,373	79,095
9) Human resources management	0,763	44,928	0	3,109	77,73%

Source: Research data

The analysis of the consensus was carried out after two rounds of application of the Delphi technique with the experts. It was possible to identify those variables of the validated dimensions indicating: a) the practice or not of the variable by the utility, b) the importance of the variable for the utility, c) the implications of the variable in the performance and d) the decrease of risk. The quality analysis of the dimensions and their respective variables are handled in the following topic.

Analysis of cyber security governance dimensions in energy utilities

The consensus of the experts about the governance dimensions practiced by Brazilian energy utilities is analyzed next.

Legal and regulatory basis dimension

Two variables of this dimension showed consensus from the experts about the relevance of this normative perspective: the need of energy utilities in complying with cyber security international standards for critical infrastructures in Brazil and the importance of the role the regulator agencies should play for the security of the electric system. It is acknowledged that these two variables reduce the operational risks of the energy utilities in the context of smart grids.

A few comments evidenced the distance that still persists regarding the international standards for the cyber security of critical structures, either for the topic being new, or for the lack of knowledge about it, with focus in operational areas rather than security or the absence of demands from regulatory agencies:

> "*most companies still do not adopt practices in total accordance with the international standards, besides the knowledge about the matter*", depending on whether the "*topic is recent Brazil and the studies in the area are still incipient*"
>
> *"There are infinite security procedures in the company"* however it is not known if "*those that would have been specifically developed for legal, regulatory or contractual compliance regarding critical systems of the operation*."
>
> "*As of the Smart Grid, the energy utilities are mostly worried at first about the technical issues of implementation, application, cost and business impact and not about the issues involving security*."
>
> "[..] *the ANEEL (Brazilian Electricity Regulatory Agency) does not really put into practice a governmental policy that obliges the energy utilities to apply more appropriate methodologies related to the cyber security of its critical areas*."

Interactionist-relational dimension

As far as constant interactions are concerned, the relations of cyber security energy infrastructures between the government and energy utilities should prevail. Although the experts do agree on the relevance of this practice, they converge that these relationships do not prevail in the Brazilian governance system. The respondents also reached a consensus about the relevance of Free communication to be performed about the illegal practices related to cyber security in energy utilities.

The cyber security issue must be extended beyond the concessionaire (Bodeau, et al. 2010). As soon as threats are responded and vulnerabilities are found, the energy utilities should make sure that the relevant data are effectively and appropriately shared so that the stakeholders can also reduce the risk and improve the network resilience and vice-versa. Forums for the sector can make this sharing easier (DOE - US Department of Energy; DHS - US Department of Homeland Security, 2012) which has not been observed by Brazilian energy utilities yet.

Transparency and inspection dimension

The experts agree upon the importance of the access to precise, relevant and opportune information about cyber security, however, they were unanimous about the inaccessibility to precise, relevant and opportune information about cyber security, in the context of shareholders, consumers, directors, auditors, employees and other stakeholders (media, suppliers, creditors and so on) of Brazilian energy utilities. They also refer to the importance of constantly practicing periodic cyber security audit carried out by independent auditors, as a mechanism to enhance the operational performance of energy utilities.

Some opinions from the experts reveal the conditions in which transparency and inspection are observed: "*only when re quired". "The companies still do not know how to deal with the topic from the point of view of their public relations". "It already works corporately but not operationally*."

Executive board dimension

The experts are unanimous and have converging opinions for the relevance of the Executive board being well-informed about the management of operational cybernetic risks. The same consensus is used for the importance of the board defining the investments to be made to protect critical cyber assets. On the other hand, there is also a consensus about the Brazilian governance system which does not maintain a constant interaction in the relations of cyber security of energy infrastructures between government and energy utilities.

The executive board of energy utilities still does not attend the management of operational cyber security, since only the matters of corporate/administrative cyber security are in scope. The justifications are: *"maybe still indirectly, without the formalization of the topic as an indicator (information only by events). "The executive board may not be well-informed since this information flow only happens on demand for there is not a specific communication plan for this purpose"*.

The rights of shareholders dimension

The experts achieved consensus in regard of the rights of the shareholders once the issues related to cyber security are not often approached in general assemblies for shareholders of energy utilities. Curiously and ambiguously, the interviewees converge that cyber security matters when handled in the assemblies can help enhance the operational performance of the companies from the energy sector.

The subsequent analysis refers to the dimension of cyber security management of smart grids in energy companies.

CYBER SECURITY MANAGEMENT IN ENERGY UTILITIES DIMENSION

Strategic planning dimension

If on one hand the experts agree that the energy utilities perform any sort of previous planning for the establishment of actions towards cyber security and the proper monitoring of these actions, on the other hand, in a consensual view they disagree that the shareholders and the board of directors are actively engaged in cyber security decision-making.

By common consent all the experts defined that:

- Previous planning for the establishment of actions towards cyber security and the proper monitoring of these actions must be carried out.
- It is important to consult working partnerships, the suppliers and the consumers of energy utilities for the definition of cyber security strategies.
- It is necessary the integration of cyber security strategies to other strategies of the organization, among them, the Smart Grid one.
- It is necessary to keep the plan for service continuity in case of cyber security incidents.

The same variables are indicated, as a consensus, as mechanisms to enhance the performance and reduce the operational risks of energy utilities in the context of the smart grids. Some statements reflect the indifference about the practice of strategic planning for cyber security:

> *"The issue of cyber security for operational critical systems is only in the embryonic stage in the concessionaire. The other issues regarding security have always been handled independently."*
>
> *"There are contingency plans being elaborated periodically and also because of the occurrence of important events."*
>
> *"only in a few occasions a strategic operational planning is elaborated, even though, not a long-term planning, except for the administrative issues."*

Risk management dimension

The respondents reached the consensus that in the business risk analysis of the energy utilities the cybernetic operational risks originating from the adoption of information and communication technologies (ICT) in processes of control and automation of the electric system are not yet considered. They also agree that the controls of operational cyber security of the energy utilities are not applied in compatibility with the risks predicted and regularly tested, monitored and revised.

The relevance of some management actions for cybernetic risk have the approval of the experts. According to them these actions enhance the performance and reduce the operational risk of the energy utilities:

- Observe the risks associated to the vulnerabilities, electric system invasions and natural disasters for structuring the energy utilities' processes.
- Monitor the cyber environment considering the risks of the relations between the concessionaire and the involved parties (consumers, suppliers, competitors and so on).
- Observe the operational risks that may end up interrupting or destroying the critical cyber assets, in the establishment of strategies for cyber security risk management.

Some verbal extracts reinforce the characteristics of risk management in energy utilities:

> *"Historically, the specific systems for the operation of the electric system that the Operation Centers use are coordinated, implemented and maintained by engineering areas that should also strongly specialize in cyber security."*.
>
> *"There is no planning for detection, identification, analysis and response to threats and vulnerabilities in cyber security in the energy utilities and they are specifically developed for the critical operation systems of the electric system."*
>
> *"There is a risk management area in the energy utilities, however, actions or guidelines towards critical operation systems observing the operational risks that may end up interrupting or destroying the assets (facilities, services and systems) of the electrical grids, are unknown"*.
>
> [...] *"they only exist for the corporate systems, they are not applied to critical operation systems (supervision and control)"*.

Asset management dimension

The experts consulted agreed by common sense about the importance and positive effects in the performance and reduction of operational risks about the following actions of the asset management dimension:

Monitor the critical cyber assets of the electric system of the energy utilities (including: communication and power system automation assets).

Control the permission and physical and logical access to information technology (IT) and operational technology (OT) assets.

Manage the configuration and changes in the information technology (IT) and operational technology (OT) assets in compatibility with the risk for the critical energy infrastructure.

With regards to cyber security management for smart grids, it is up to the energy utilities to monitor the critical cyber assets of the electric system (including: communication and power system automation assets) and to control the permission and logical and physical access to them; to manage their configuration and changes, in a compatible way with the tolerable risk for critical energy infrastructure. The search results revealed the existence of punctual access controls applied for information technology (IT) and operational technology (OT) systems, which conceptions rely on the fact that they are under the cradle of corporate network, previously protected by general controls. The experts point to the need of specific planning for the control of critical systems, with the definition of new user profiles, access (logical and physical) and domains, as well as the effective management of these controls.

Human resources management dimension

For the experts there is a consensus that the description of roles and positions in energy utilities cyber security operational responsibilities are not clearly attributed. Among the variables of the human resources dimension, only the plans for training and continuous education in operational cyber

security were unanimous among the respondents concerning the positive effects in the operational performance of the energy utilities.

Some other proposals have been identified in the statements: a) implementing practices (plans, procedures, technologies and controls) to create a culture of cyber security and ensure the continuous adequateness and competence of people, compatible with the tolerable risk for the critical infrastructure, b) clear attribution of cyber security responsibilities; c) the use of socialization strategies to raise the awareness of new and old employees and outsourced people about plans, procedures, technologies and controls of operational cyber security and having plans for training and continuous education in operational cyber security for Smart Grids d) considering the records of the employees regarding cases of violation of operational security in the selection and hiring of people, e) the description of roles and positions should be clear about the responsibilities for operational cyber security.

CONCLUSION

Through this study it was possible to structure, validate and evaluate the dimensions of governance and management applied to Brazilian energy utilities in face of the challenges of cyber security presented by the conceptions of smart grids in Brazil.

Although cyber security governance and management is a widely investigated topic in Administration, when it comes to IT security in the scope of the Smart Grids, this approach is still poorly explored. Maybe for the contemporaneity of the theme, the scarcity of research is increased when the focus is limited to cyber security of critical infrastructures that make use of industrial automation and control systems. The characteristics of smart grids, accessible and interoperation systems that handle a great amount of information transiting in complex information and communication technologies making them strategic topics, not only for electric energy service providers but also for the State since the compromise of the electric system affects the society as a whole.

From the literature adopted for the research it was possible to identify the dimensions: normative, interactionist, transparency and inspection, Executive Board and rights of the shareholders for the corporate governance construct; and, strategic planning, risk management, asset management and human resources management for the management constructs. The statistics validation of the model allowed its application in the scope of cyber security of smart grids in energy utilities.

Regarding the normative dimension, in the opinion of the experts, the distance among the energy utilities, government and regulatory agencies was identified, in search of an effective regulatory and legal structure for the cyber security of critical infrastructures in Brazil.

It was also observed that in Brazilian energy utilities the operational cyber security is dealt with in the lowest levels of the organization, based in isolated actions, without strategic long-term planning and focused in processes developed basically by professionals of the area of information and communication technology.

The analysis of consensus of the answers extracted with the Delphi technique also allowed to infer that, even the experts still do not have knowledge about the representativeness of the dimensions of governance. The results show a greater knowledge in relevance of operational management of cyber security than for variables with respect to the relevance of the interactions between the board of directors and other institutional organs involved with cyber security.

The research reflects the fact that the board of directors of Brazilian energy utilities is not yet actively engaged in the operational decisions of cyber security. Even if shareholders and executives are interested or start the cyber security process, their previous planning occurs as isolated and operational initiatives and not as part of the process of corporate management and governance. Generally speaking, the conclusion is that all the dimensions described as a result of this study attend Brazilian energy utilities for the governance and management of cyber security for Smart Grids.

The dimension with the best evaluation from the experts, based on the criteria for adoption by Brazilian energy utilities, relevance for the Smart Grid stakeholders, relation with the improved performance and reduction of the operational risk was the management dimension which comprises the management of critical assets, whereas the dimension with the worst evaluation was the dimension of governance that handles the rights of the shareholders.

The present study points to insights for the theorization of this knowledge field rarely approached in literature. The dimensions presented can help in the application and operation of the model of governance and management of cyber security for other sectors. Especially in the scope of critical operation systems of the Brazilian electric system, the results showed that there are no plans for the detection, identification, analysis and response to threats and vulnerabilities in operational cyber security in Brazilian energy utilities.

REFERENCES

Aitel, D. (2013). Cybersecurity essentials for electric operators. *The Electricity Journal*, 26(1), 52-58.

Allen, J. *Governing for Enterprise Security*. Pittsburgh: Carnegie Mellon University, 2005. Available on: <http://www.cert.org/archive/pdf/05tn023.pdf>. Access: April 15, 2012.

ANSI – American National Standards Institute (2009). *ISA – 99.00.02-2009*. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. USA.

Bodeau, D., & Graubart, R. (2010). *Cyber resiliency engineering framework*. MTR110237, MITRE Corporation, September. Available at: <http://www.mitre.org/work/tech_papers/2010/10_3710/10_3710.pdf>. Access in: 15 apr. 2012.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*, Software Engineering Institute. Available at: <http://www.cert.org/archive/pdf/10tn028.pdf>. Access in: 15 may 2012.

Cooper, D. R., Schindler, P. S., & Sun, J. (2006). Business research methods (Vol. 9). New York: McGraw-Hill Irwin.

Coutinho, M. P. (2007) *Detecção de Attacks em infraestruturas críticas de systems elétricos de potência usando técnicas inteligentes.* 260 f. PhD Tesis, Universidade UNIFEI, Itajubá.

DOE - US Department of Energy; DHS - US Department of Homeland Security (2012). *Electricity Subsector – Cybersecurity Capability Maturity Model – ES-C2M2.* Washington: DOE/DHS, 2012. Avaiable on: <http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf>. Acess July 2nd 2012.

Gellings, C. W. (2009). *The smart grid: enabling energy efficiency and demand response.* The Fairmont Press, Inc.

Hatch, M. J., & Cunliffe, A. L. (2013). *Organization theory: modern, symbolic and postmodern perspectives*. Oxford University Press.

ITU-T – International Telecomunication Union (2008). *Recommendation X.1205*: Overview of Cybersecurity. Geneva: ITU-T, 2008.

Mesquita, J. D. (2010). *Estatística multivariada aplicada à administração: guia prático para utilização do SPSS*. Curitiba: CRV.

MIT - Massachusets Institute of Technology (2011). *The Future of the Electric Grid:* An Interdisciplinary MIT Study. Cambridge: MIT.

Momoh, J. (2012). *Smart grid: fundamentals of design and analysis* (Vol. 63). John Wiley & Sons.

Newton's Telecom Dictionary (2009). 25. ed. New York: Flatiron.

NIST – National Institute of Standards Technologies (2010). *NISTIR 7628:* Guidelines for *Smart Grid* Cyber Security National Institute of Standards and Technology Interagency Report 7628. Gaithersburg: Department of Commerce/NIST, 2010. 1 v. 289 p. Avaiable on: <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf>. Access: February 4, 2011.

OCDE (2004). *Os Princípios da OCDE sobre o Governo das Sociedades.* Disponível em: <http://www.oecd.org> .Acesso em: 25 out. 2012.

OCDE (2005). *Diretrizes da OCDE sobre Governança Corporativa para Empresas de Controle Estatal.* Disponível em: <http://www.oecd.org> .Acesso em: 25 out. 2012.

Roth, A. L. *et al*. (2012) Diferenças e inter-relações dos conceitos de governança e gestão de redes horizontais de empresas: contribuições para o campo de estudos. *Revista de Administração da Universidade de São Paulo – RAUSP*, v. 47, n. 1, p. 112-123, jan./fev./mar. 2012.

Sorebo, G., Echols, M. (2012). *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid.* Boca Raton: CRC Press.

Turnbull, S. (1997) Corporate Governance: Its Scope, Concerns and Theories. *Scholarly Research and Theory Papers*, v. 5, n. 4, 180-205.

Wright, J. T. C.; Giovanazzo, R. A. (2000) *Delphi*: uma Ferramenta de Apoio ao Planejamento Prospectivo. *Caderno de Pesquisa em Administração*, São Paulo, FIA/FEA/USP, v. 1, n. 12, p. 54-65.