A Survey Of New Development In Cyber Security And Networks

Frank Kataka Banaseka
Dept. of Information &Com Tec
Radford University College
Ghana-Accra
frankbanaseka@gmail.com

Patrick Kwaku Kudjo
Dept. of Information Tec
Wisconsin University College
Ghana-Accra
borngreat400@gmail.com

Dickson Keddy Wornyo
Dept. of Information Tec
Datalink Institute
Ghana-Accra
macdicksons@yahoo.com

***Abstract*—The recent developments in wireless communication techniques, mobile cloud computing, and other storage technologies has led to a growing new trends of cyber-attacks on networks and industry. Frequent data breaches in most companies raises questions about the effectiveness of the private sector and governments' information security. There is therefore the need to enhance cyber-security technologies for networks and emerging applications in recent years. This paper is a survey that details new development in cyber security and networks. Our discussions will focus on new developments in Cyber Security for Smart Grid Distribution Networks, analysis of Supervisory Control and Data Acquisition (SCADA) systems, description of Cyber-Physical Systems against Stealthy Deception Attacks, analysis of Gordon-Loeb Model as well as present recent cyber-security breaches and proposed policies for securing Information**

Keywords— Cyber security; Deception attacks; Information security; Smart grid; SCADA.

I. INTRODUCTION

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment[1-4]. Cyber security breaches inflict costs to consumers and businesses. The possibility also exists that a cyber security breach may shut down an entire critical infrastructure industry, putting a nation's whole economy and national defense at risk.[5] Hence, the issue of cyber security investment has risen to the top of the agenda of business and government executives. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation and Confidentiality.[6, 7] It is against this back drop that we deliberate on a survey on New Development in Cyber Security and Networks. The structure of the paper is as follows, Section II discusses new development in Cyber-security for Smart Grid Distribution Networks and Cyber Security of Smart Grid Model. Section III briefly explains Supervisory Control and Data Acquisition (SCADA) systems. Cyber-Physical Systems against Stealthy Deception Attacks is presented in section IV. Section V describes the Cyber security investment using the Gordon-Loeb Model; Section IV gives a highlight of some recent security breaches in the US. Policies for Securing Information are present in section VII. Section VIII concludes the survey

II. CYBER SECURITY FOR SMART GRID DISTRIBUTION NETWORKS

A. *Smart Grid communication system*

New trends in the power industry indicate integration of electrical distribution system with communication networks that form bidirectional power and information flow infrastructure, which is called a smart grid [8-11]. The integration not only moves power automation systems from outdated, proprietary technology to the advanced communication technologies, but also changes the closed power control systems to the public data networks. By adding significant new functionality, distributed intelligence, and state-of-the-art communication capabilities to the power grid, the smart grid infrastructure can be more efficient, more resilient, and more affordable to manage and operate[12]. However, it brings not only great performance benefit to the power industry, but also tremendous risks as well as arduous challenges in protecting the smart grid systems from cyber security threats[9]. Considering the vast scale of a smart grid, it is reasonable to expect that the cumulative vulnerability of the smart grid communication system might also be vast. Virtually all parties agree that the consequences of a smart grid cyber security breach can be enormous.

New functions such as demand response introduce significant new cyber-attack vectors such as a malware that initiates a massive coordinated and instantaneous drop in demand, potentially causing

substantial damage to distribution, transmission, and even generation facilities [13].

A typical smart grid communication system is a horizontal integration of one or more regional control centers, with each center supervising the operation of multiple power plants and substations. A smart grid communication system has a layered structure and performs data collection and control of electricity delivery. A regional control center typically support metering system, operation data management, power market operations, power system operation and data acquisition control. Substations contain Remote Terminal Units (RTUs), circuit breaker. Human Machine Interfaces (HMIs), communication devices (switches, hubs, and routers), log servers, data concentrators, and a protocol gateway. Intelligent Electronic Device (IEDs) are field devices, including an array of instrument transducers, tap changers, circuit re-closers, phase measuring units (PMUs), and protection relays[13].

B. *Cyber Security of Smart Grid Model*

The diagram below shows that smart grids consist of four components: Generation, Transmission, Distribution and Consumption. In the consumption component, customers use electric devices (e.g., smart appliances, electric vehicles), and their usage of electricity will be measured by an enhanced metering device, called a smart meter. The smart meter is one of the core components of the advanced metering infrastructure (AMI) [14]. The meter can be collocated and interact with a gateway of a home-area network (HAN) or a business-area network (BAN).[15] For simple illustration, we denote a smart meter in the figure as a gateway of a HAN. A neighbor-area network (NAN) is formed under one substation, where multiple HANs are hosted. Finally, a utility company may leverage a wide-area network (WAN) to connect distributed NANs.

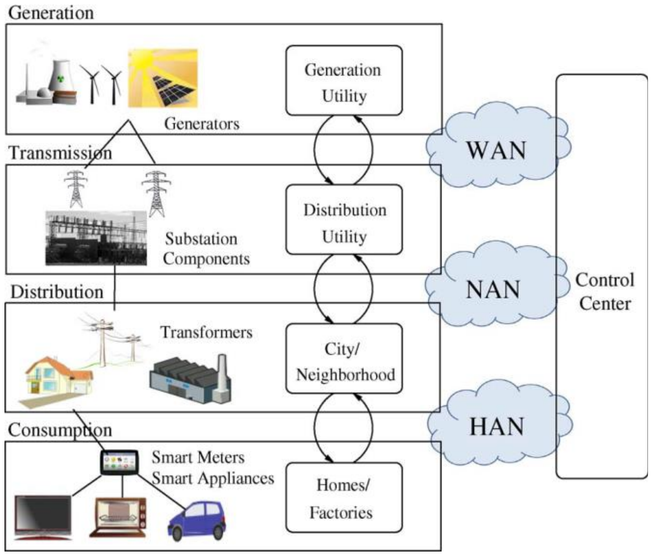

Fig. 1 A cyber security view of smart grid

III. Supervisory Control and Data Acquisition (SCADA) Systems

SCADA systems for power networks are complemented by a set of application specific software, usually called energy management systems (EMS)[16-19] Modern EMS provides information support for a variety of applications related to power network monitoring and control. The power network state estimator (SE) is an on-line application which uses redundant measurements and a network model to provide the EMS with an accurate state estimate at all times. The SE has become an integral tool for EMS, for instance for contingency analysis (CA) which, based on the state estimate, identifies the most severe consequences in case of hypothetical equipment outages[19]. SCADA systems collect measurement data from remote terminal units (RTUs) installed in various substations, and relay aggregated measurements to the central master station located at the control center.

Several cyber-attacks on SCADA systems operating power networks have been reported, and major blackouts, such as the August 2003 Northeast U.S. blackout, are due to the misuse of the SCADA systems. Using intelligent communications, load shedding can be implemented so that peak demand can be flattened, which reduces the need to bring additional (expensive) generation plants online. Using information systems to perform predictive analysis, including when wind and solar resources will produce less power, the utilities can keep power appropriately balanced. As new storage technologies emerge at the utility scale, incorporation of these devices will likewise benefit from intelligent demand prediction. Last, the ability for consumers to receive and respond to price signals will help them manage their energy costs, while helping utilities avoid building additional generation plants[15]. With all these approaches, the smart grid enables a drastic cost reduction for both power generation and consumption. Dynamic pricing and distributed generation with local generators can significantly reduce the electricity bill. Fig. 2(a) shows how to use electricity during off-peak periods when the price is low. Conversely, Fig. 2(b) shows load shedding during peak times and utilization of energy storage to meet customer demand.

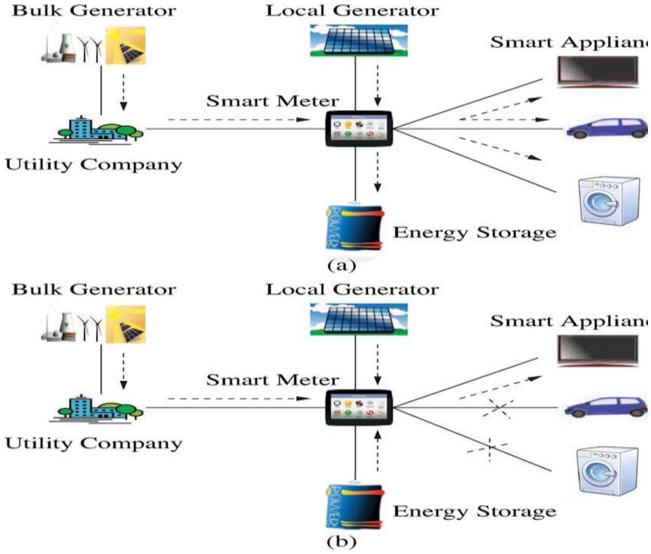

Fig. 2 (a) and Fig2 (b) respectively show the Power usage during off-peak time period. And Power usage during peak time period

IV. Cyber-Physical Systems against Stealthy Deception Attacks

Cyber-Physical Systems (CPS) consists of both logical elements such as embedded computers and physical elements connected by communication channels such as Internet. Cyber-Security is one of the major concerns for many CPSs [9][20, 21]. The methods proposed to solve the cyber security problem for CPSs can be categorized into two classes: information security which is mainly focused on encryption and data security, and secure control theory which studies how cyber-attacks affect the control systems' physical dynamics[22]. The safety tools only using information security are not sufficient for secure control of CPSs because they cannot describe the system's macro-behavior. Therefore, they should be complemented with secure control theory. Secure control theory is based on an attack model, which is a challenging task due to the uncertain and erratic nature of cyber-attacks. Various cyber-attack models for CPSs can be summarized as two kinds:

- The first model, Denial of Service (DOS) attacks refer to obstructing the communication between networked agents. Those attacks can jam the communication channels; attack the routing protocols, etc. As a countermeasure, provides a secure control scheme in the presence of DOS attacks. Another research group applied the game theoretic approach to achieve a robust and resilient control against DOS attacks[22, 23]
- A deception attack which is the second kind of attack model represents the injection of false information from sensors or controllers.

In this attack, the attacker can obtain the secret key or compromise some cyber elements in order to falsify the data [24-26]. This kind of attack has mainly been studied in the electric power distribution application and some other applications can be found in[27]. Some papers also proposed the security indices or vulnerability conditions which allow the attacker to perform an elaborate deception attack[28, 29]

V. Cyber Security Investment using the Gordon-Loeb Model

A. *Economics of Information Security*

With economic activity and national defense heavily and increasingly dependent on networked computer systems, cyber security issues continue to draw increasing attention by the media, as well as by executives at the highest levels of government, industry, and nonprofit organizations. A key reason for this increasing attention on cyber security issues by governments around the world is the eminent threat posed by cyber security breaches to a nation's national defense and the nation's economic strength[5].

Firms in the private sector of many countries own a large share of critical infrastructure assets. Hence, cyber security breaches in private sector firms could cause a major disruption of a critical infrastructure industry (e.g., delivery of electricity), resulting in massive losses throughout the economy, putting the defense of the nation at risk. Moreover, the cyber security activities of a given firm affect not only the probability of that firm suffering a cyber security breach, but also the probability that other firms (and individuals) suffer cyber security breaches. As one example, consider a firm that is not adequately protected against malware that infects the firm's computer system and, although undetected, use that firm's computer as part of a botnet to attack other firms. Since there is no practical way for a firm to be made liable for the entirety of losses from breaches to other firms caused by the vulnerabilities to its own computer systems, complete reliance on market mechanisms to overcome the externalities problem breaks down (i.e., using the terminology of economics, there are market failures). In fact, it is well known that in the absence of government incentives and or regulations (hereafter incentives/regulations) firms will under invest in cyber security activities relative to the quantity that maximizes social welfare. Thus, governments have an interest in providing incentives/regulations to firms to invest in cyber security activities at a level that takes into account not only the private losses incurred by firms from breaches of cyber security, but also the costs of externalities resulting from such beaches.

A prelude to developing incentives/regulations that take into consideration the costs of externalities, as well as the private costs, is an understanding of the relationship between the magnitude of externalities and the magnitude of cyber security underinvestment.

B. *The Gordon-Loeb Model*

Gordon-Loeb **(**GL) presents a single period economic model to examine the problem of a risk-neutral firm selecting the optimal level of expenditures on cyber security activities. The GL Model examines how the firm's optimal level of cyber security expenditures, denoted by z^{sc}, varies with two parameters [5, 30-32].The first one denoted by *v* is the probability that a cyber security attack will be successful in the absence of any cyber security expenditures, and the second one denoted by L^p, the expected loss to the firm if the attack is successful. The model is briefly summarized below:

Let $S(z,v)$ denote the firm's security breach function, defined as the probability that an information security breach occurs and where *z* is the firm's monetary investments in cyber security and $v(0 \leq v \leq 1)$ represents the firm's underlying vulnerability to security breaches. GL postulate that the security breach function is twice continuously differentiable and meets the following five regularity conditions:

i. ∀ *z* ≥ 0 , *S* (*z*,0) = 0 ; i.e. if the firm's information is perfectly invulnerable, then it will remain so for all levels of cyber security investments

ii. ∀ *v*∈(0,1) , *S* (0,*v*) = *v* ; i.e. if there is no investment in cyber security, the probability of a successful breach will be the underlying vulnerability

iii. ∀ *v*∈(0,1) and ∀ *z* ≥ 0 and $\frac{\partial S(z,v)}{\partial z} < 0$; i.e. increases in cyber security investment will decrease the probability of a successful breach

iv. ∀*v*∈(0,1) and ∀*z* ≥ 0 , $\frac{\partial^2 S(z,v)}{\partial z^2} > 0$ and; i.e. the security breach function is strictly convex in *z* , *i.e.*, there are diminishing returns to cyber security investment

v. ∀*v*∈(0,1) ,$lim_{z\to\infty} S(z,v) = 0$. i.e. by investing sufficiently in cyber security the probability of a successful breach can be made arbitrarily close to zero.

When making the security investment decision, the firm would choose an investment level z^{SC} so that the total expected net benefits from the investment is maximized:

$$max_z\{v - S(z,v)\}L^p - z \qquad (1)$$

And should satisfy the condition

$$-S_z(z^{sc},v)L^p = 1 \qquad (2)$$

For security breach functions meeting the above five regularity conditions, GL provide some general results concerning the relation between the optimal level of cyber security investment,z^{sc}, and the prior level of vulnerability, *v*. The principal result demonstrated by GL, however, is that for a risk-neutral firm, the optimal investment in information security is generally a small fraction of the expected loss of a breach. Specifically, GL show that for the two broad classes of security breach functions satisfying the regularity conditions given below

$$S_0(z,v) = \frac{v}{(\alpha z+1)^\beta}; where \alpha > 0 \wedge \beta \geq 1 \qquad (3)$$

And

$$S_1(z,v) = v^{\alpha z+1}; where \alpha > 0 \qquad (4)$$

C. Modifying the GL Model to Include Externalities

Let L^E denote the externality costs of an information security breach, defined as the total loss to consumers and other firms, not captured within the private lossL^P , from a breach of information security.

Let L^{SC} represent the total social costs of an information security breach defined as the sum of the firm's private loss plus the externality costs

i.e., $L^{SC} = L^P + L^E$ (5)

The GL Model can then be easily extended to incorporate the externalities. The social optimal level of investment for the firm, denoted z^{SC} , is the level that maximizes expected benefits net of both the private loss and externality costs:

$$max_z\{v - S(z,v)\}L^{SC} - z \qquad (6)$$

And Z^{SC}should satisfy the condition

$$-S_z(z^{SC},v)L^{SC} = 1 \qquad (7)$$

By comparing (6) and (2), and assuming $L^E > 0$ and that increasing information security investment decreases the probability of an information security breach, but at a decreasing rate *i.e.*, regularity assumptions 3 and 4), one can see that$z^{SC} > z^{SC}$. That is, the socially optimal amount for the firm to invest in information security is greater than the firm's optimal amount. This is merely a formal demonstration that firms, without additional incentives, will under invest in information security. In order to examine the possible magnitude of a firm's under investment in information security relative to the amount that maximizes social welfare, the security breach function of the class I type specified is first examined. Then, the firm's optimal investment in information security is given by:

$$z^{SC}(v) = \frac{[(v\alpha\beta L^P)^{1/\beta+1} - 1]}{\alpha} \qquad (8)$$

VI. SOME RECENT CYBER SECURITY BREACHES IN THE US

Alexis Kleinman in 2014 reported that about five (5) million Gmail usernames and passwords were compromised. About 100,000 were released on a Russian forum site. Apple iCloud technology reported that Hackers used passwords, hacked with brute-force tactics and third-party applications to access Apple user's online data storage, leading to the subsequent posting of celebrities' private photos online[33]. It is uncertain whether users or Apple were at fault for the attack.

The U.S. Transportation Command contractors, according to a Senate report revealed that networks of the U.S. Transportation Command's contractors were successfully breached 50 times between June 2012 and May 2013[34-36]. At least 20 of the breaches were attributed to attacks originating from China.

VII. POLICIES FOR SECURING INFORMATION

As cyber-attacks on retail, technology, and industrial companies increase so does the importance of cyber security. From brute-force attacks on networks to malware compromising credit card information to disgruntled employees sabotaging their companies' networks from the inside, companies and their customers need to secure their data. To improve the private sector's ability to defend itself, the following policies should put in place[37]:

A. Create A Safe Legal Environment For Sharing Information

As the world experiences technological growth, private companies are in most ways at the forefront of cyber security. Much like government agencies, companies must share information that concerns cyber threats and attack among themselves and with appropriate private-public organizations. It is important to create a safe environment in which companies can voluntarily share information without fear of legal or regulatory backlash [19].

B. Work With International Partners

In relation to the Back-off malware attacks, they can affect hundreds if not thousands of individual networks. These infected networks can then infect companies outside a country and foreign companies, there is therefore the need for governments and other international organizations to work together to increase overall cyber security and to enable initiate actions against individual cyber criminals and known state-sponsored cyber aggressors[38].

C. Encourage Cyber Insurance

Successful cyber-attacks are inevitable because no security is perfect. With the number of breaches growing daily, a cyber security insurance market is developing to mitigate the cost of breaches. Private-public organizations should encourage the proper allocation of liability and the establishment of a cyber insurance system to mitigate faulty cyber practices and human error.

VIII. CONCLUSION

The recent increases in the rate and the severity of cyber-attacks on companies all over the world indicate a clear threat to businesses and customers. As businesses come to terms with the increasing threat of hackers, instituting the right policies is critical to harnessing the power of the private sector. In a cyber environment with ever-changing risks and threats, the government needs to do more to support the private sector in establishing sound cybersecurity while not creating regulations that hinder businesses more than help them. Extending and applying the GL Model for deriving the optimal level of investment in cyber security activities is critical. This extension focuses on examining the impact of considering the costs associated with the externalities of cyber security breaches in addition to private costs. As a critical infrastructure, smart grid requires comprehensive solutions for cyber security. Comprehensive communication architecture with an inbuilt security is needed from the very beginning to ensure a secured information system. A smart grid communication security solution requires a holistic approach including traditional schemes such, trusted computing elements,

authentication mechanisms based on industry standards. Clearly, securing the smart grid communication infrastructure will require the use of standards-based state-of-the-art security protocols.

REFERENCES

[1]R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security,* vol. 38, pp. 97-102, 2013.

[2]W. Stallings and L. Brown, "Computer security," *Principles and Practice,* 2008.

[3]D. Korff, "CYBER SECURITY DEFINITIONS–a selection," ed: Oxford.

[4]N. Kshetri, "Cybersecurity and Development," *Markets, Globalization & Development Review,* vol. 1, 2016.

[5]L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model," *Journal of Information Security,* vol. 6, p. 24, 2014.

[6]J. B. Joshi, W. G. Aref, A. Ghafoor, and E. H. Spafford, "Security models for web-based applications," *Communications of the ACM,* vol. 44, pp. 38-44, 2001.

[7]D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576,* 2009.

[8]H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine,* vol. 8, 2010.

[9]H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy,* vol. 8, 2010.

[10]J. Cuellar, *Smart Grid Security*: Springer, 2013.

[11]P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy,* vol. 7, 2009.

[12]Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys and tutorials,* vol. 14, pp. 998-1010, 2012.

[13]S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, pp. 1-5.

[14]A. Faruqui, R. Hledik, S. Newell, and H. Pfeifenberger, "The power of 5 percent," *The Electricity Journal,* vol. 20, pp. 68-77, 2007.

[15]Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig*, et al.*, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE,* vol. 100, pp. 195-209, 2012.

[16]C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems,* vol. 23, pp. 1836-1846, 2008.

[17]S. A. Boyer, *SCADA: supervisory control and data acquisition*: International Society of Automation, 2009.

[18]R. L. Krutz, *Securing SCADA systems*: John Wiley & Sons, 2005.

[19]A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC Proceedings Volumes,* vol. 44, pp. 11271-11277, 2011.

[20]L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Machine Learning in Cyber Trust*, ed: Springer, 2009, pp. 3-13.

[21]R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology,* vol. 12, pp. 161-166, 2011.

[22]C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *American Control Conference (ACC), 2013*, 2013, pp. 3344-3349.

[23]W. Liu, C. Kwon, I. Aljanabi, and I. Hwang, "Cyber security analysis for state estimators in air traffic control systems," in *AIAA Guidance, Navigation, and Control Conference*, 2012, p. 4929.

[24]A. A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," in *HotSec*, 2008.

[25]C. Yang, H. Zhang, F. Qu, and Z. Shi, "Performance of target tracking in radar network system under deception attack," in *International Conference on Wireless Algorithms, Systems, and Applications*, 2015, pp. 664-673.

[26]S. Bodmer, M. Kilger, G. Carpenter, and J. Jones, *Reverse deception: organized cyber threat counter-exploitation*: McGraw Hill Professional, 2012.

[27]Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, 2011, pp. 4066-4071.

[28]H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*, 2010.

[29]O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 220-225.

[30]J. Willemson, "Extending the Gordon and Loeb model for information security investment," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, 2010, pp. 258-261.

[31]R. Böhme, "Security metrics and security investment models," in *International Workshop on Security*, 2010, pp. 10-24.

[32]S. Farrow and J. Szanton, "Cybersecurity Investment Guidance: A Note on Extensions of the Gordon and Leob model."

[33]S. Kovach, "We Still Don't Have Assurance from Apple That iCloud Is Safe," *Business Insider,* pp. 14-9, 2014.

[34]L. Jensen, "Challenges in Maritime Cyber-Resilience," *Technology Innovation Management Review,* vol. 5, p. 35, 2015.

[35]S. Jasper, "Deterring Malicious Behavior in Cyberspace," DTIC Document2015.

[36]S. Amoaning-Yankson, "A resiliency framework for planning in state transportation agencies," Georgia Institute of Technology, 2013.

[37]R. Walters, "Cyber attacks on US companies in 2014," *Heritage Foundation Issue Brief,* vol. 4289, 2014.

[38]S. P. Bucci, P. Rosenzweig, and D. Inserra, "A congressional guide: Seven steps to US Security, Prosperity, and Freedom in Cyberspace," *Backgrounder,* 2013.