Factors Impacting Attacker Decision-Making in Power Grid Cyber Attacks

Aunshul Rege

Chapter 9

FACTORS IMPACTING ATTACKER DECISION-MAKING IN POWER GRID CYBER ATTACKS

Aunshul Rege

Abstract For several years, security experts and government officials have been warning about a "Cyber Pearl Harbor" – a cyber attack on the nation's power grid. Current cyber security research focuses on the tactical aspects of infrastructure attacks and views attackers as passive agents, downplaying their strategies. The research only minimally incorporates the human element, which limits the understanding of cyber attacks on the critical infrastructure.

This paper explores attacker decision-making with regard to power grid cyber attacks from a criminological perspective. It presents the findings from a survey that explored the technical and non-technical factors influencing attacker decision-making. A total of 330 participants from the ethical hacker community and the power industry were surveyed. Nine factors influencing attacker decision-making emerged and were organized to create the PARE RISKS framework: prevention measures (P); attacks and alliances (A); result (R); ease of access (E); response (R); interconnectedness and interdependencies (I); security testing and audits (S); knowledge and research (K); and system weaknesses (S). This paper makes the case that infrastructure attackers are intelligent, active actors who plan strategic attacks and adapt to their environments. The paper also offers recommendations for cyber security policy, focusing on improved security practices, education programs and mandatory security budgets.

Keywords: Industrial control systems, cyber attacks, attacker decision-making

1. Introduction

The U.S. power grid is a complex networked system that serves more than 300 million people, comprises more than 200,000 miles of transmission lines, and is valued at over $1 trillion [25]. Grid operations are now automated, use

industrial control systems (ICSs) and are connected to the Internet; these have helped improve operations, efficiency and reliability [22, 25]. The increased connectivity, however, has made the grid more vulnerable to (remote) cyber attacks [22, 25]. Former Defense Secretary Panetta warned that cyber attacks on critical infrastructures, such as the power grid, from nation states or extremist groups could be as devastating as the 9/11 terrorist attacks [2, 3, 24]. The grid is considered to be "target number one" for cyber attacks because power disruptions impact other dependent critical infrastructures and have significant economic ramifications, with industry downtime costs exceeding U.S. $6 million per day [1, 21, 25, 30]. Unfortunately, the power sector is not prepared for cyber attacks [27, 29, 30].

In general, research has focused on power grid vulnerabilities and security, attack methods, simulations and analysis [9, 16, 17]. The research is mostly technical in nature and primarily addresses the tactical aspects of cyber attacks on the critical infrastructure. Very little research integrates or even considers the human factors underlying attacks.

Attackers are active agents and they plan and conduct strategic cyber attacks against the critical infrastructure [15, 27]. Understanding how attackers make decisions is important because attack strategies determine the tactics employed in power grid cyber attacks [27].

The criminological discipline provides a framework to investigate the strategic aspect of cyber attacks. One theoretical branch of criminology, the rational choice perspective, views attackers as intelligent individuals who learn from their experiences, adapt to their settings and employ an evolving decision-making process [23, 27]. Using this criminological approach in conjunction with technical research provides a better understanding of how attackers make decisions regarding target selection, exploiting criminal environments, and planning, designing and executing attacks. Such an understanding can help articulate and manage preventative and reactive measures.

This paper explores power grid cyber attacks from a criminological perspective to understand attacker decision-making. It identifies nine factors, technical and non-technical, that impact attacker decision-making. Using the perceptions of power grid representatives and ethical hackers, the paper demonstrates that attackers are indeed active agents who engage in dynamic cyber attacks.

2. Attacker Decision-Making

Four research areas were examined to identify the factors that influence attacker decision-making in power grid cyber attacks. First, the ICS literature was reviewed, which provided information on system components that constitute targets. Second, the literature on ICS vulnerabilities was examined, which offered insight into system design and architectural flaws that are exploited in attacks. Third, the literature on threat agents was reviewed, which identified the assortment of attackers based on type, skill and motivation. Finally, twelve case studies involving malicious acts against the power grid were examined to understand the nature, diversity and intensity of attacker skills

and strategies. The factors that influence attacker decision-making were then extracted and combined to create a PARE RISKS framework: prevention measures (P); attacks and alliances (A); result (R); ease of access (E); response (R); interconnectedness and interdependencies (I); security testing and audits (S); knowledge and research (K); and system weaknesses (S).

3. (Criminological) Theoretical Framework

Routine activity theory (RAT) focuses on the essential elements that constitute a crime. RAT states that three conditions must be met for crime to occur: (i) a likely or capable offender; (ii) a suitable target; and (iii) the absence of a capable guardian [5]. RAT is relevant to this research because it addresses the elements necessary for cyber attacks against the power grid to occur. The potential offenders are cyber attackers who have varying levels of skill and sophistication. Poorly-designed ICSs are suitable targets, and weak real-time intrusion detection systems (IDSs), for instance, represent the absence of capable guardianship. When these three elements coincide in space and time, cyber attacks are more likely to occur. Thus, it is necessary to focus on attack events as well as attacker analyses of the situations, which resonates with the active nature of attackers.

Rational choice perspective (RCP) views criminality as an outcome of the continual interaction between a criminal's desires and preferences, and the opportunities and constraints to commit crime; the attacker is a strategic decision-maker [6]. This theoretical perspective is useful for capturing attacker decisions on tactical measures and assessing whether countermeasures implemented by defenders are strong enough to deter attackers. According to RCP, attackers are rational and intelligent actors who conduct cost-benefit analyses before launching attacks; if the benefits outweigh the costs, an attacker is more likely to target the power grid.

RAT and RCP complement each other because an attacker engages in rational calculations based on the suitability of the target and the absence of capable guardianship. Thus, if a target is suitable (easy to access with exploitable loopholes) and the guardianship is weak or non-existent (poor real-time intrusion detection), then the attacker would perceive the risk to be minimal. The benefits of the attack (service disruption) would outweigh the risk, making the power grid cyber attack more likely to occur.

4. Research Methods

This research used methodological triangulation. Specifically, it used multiple data collection methods (surveys and interviews) to study attacker decision-making regarding cyber attacks on ICSs [8, 14]. Methodological triangulation was used to obtain a more complete, "holistic and contextual portrayal of the unit(s) under study" [13]. The use of different methods uncovered some unique findings that would not have been discovered by a single method [13]. Triangulating surveys and interviews also enabled new concepts to emerge [13]. While

the surveys helped identify factors that influence attacker decision-making, the interviews revealed rich insights into the factors as well as the domain of cyber security.

4.1 Sampling Strategy and Data Collection

While it would have very useful to obtain information from actual attackers, this population was impossible to reach because they belong to an underground culture that is unknown or inaccessible. The vast majority of attacks on the power grid are not publicized. The few cyber attacks that have been publicly disclosed were often through the media, not from official government, security or industry sources; this raised issues of credibility, accuracy and completeness. Moreover, when the sources of attacks were disclosed, they were often foreign-based or nation-sponsored, which prevented jurisdictional access and hindered the identification of the specific source(s) and accountable individual(s).

Survey data for the hacker community was obtained during the 2010 DEF CON Hacker Conference, which had approximately 8,000 attendees with varying levels of knowledge about hacking techniques and attack trends. A total of 202 hacker respondents were sampled. Survey data from the power industry was collected from four sources. The survey was advertised and promoted through the North American Electric Reliability Corporation (NERC), the System Administration, Networking and Security (SANS) Infrastructure Conference, and the EnergySec and SCADASEC mailing lists. A total of 121 industry responses were received.

Some survey participants from the hacker community and from industry identified control system experts, specifically, system penetration testers, who were willing to participate in the interviews. These individuals are known as ethical hackers, who are engaged by the power industry to mimic malicious attackers. They possess the technological savvy to test systems, exploit vulnerabilities and evaluate preventative measures. Moreover, they employ similar decision-making processes as actual attackers when targeting systems.

4.2 Survey and Interview Design

The surveys were administered in paper and online formats. The survey items were categorized to reflect the PARE RISKS framework. A cross-sectional survey was employed to collect hacker and industry perceptions on the factors that influence attacker decision-making. The survey content was based primarily on National Institute of Standards and Technology (NIST) Special Publication 800-82 [26], and included additional items regarding attacker motivations, alliances, research and development, and resources.

The interviews helped identify additional factors that contribute to the attacker decision-making process. Telephone interviews were used to collect data from penetration testers and industry personnel. The interviews lasted approximately one hour and thirty minutes, and like the surveys, were anonymous and approved by the university's ethics committee.

Table 1. Regrouping of PARE RISKS to SPAARR.

SPAARR	PARE RISKS	Items	Subject to Item Ratio
System	Ease of Access + System Weaknesses	38	11:1
Preventative	Preventative Measures + Security Testing, Assessments and Audits	10	32:1
Attackers	Attacks and Alliances + Knowledge, Skills, Research and Development	23	14:1
Attacks	Attacks and Alliances + Knowledge, Skills, Research and Development	18	18:1
Reactive	Response and Recovery	21	15:1
Result	Results + Interconnectedness and Interdependencies	22	14:1

5. Analysis and Results

Exploratory factor analysis (EFA) was conducted to help determine whether measured variables could be explained by any underlying factors (latent variables) [7, 11]. The literature suggests that, when conducting EFA, there should be approximately ten cases per survey item [7, 10]. Unfortunately, this was not feasible in the research. The survey had 122 items, which would have required a data set of 1,220 cases, but only 322 cases were available. To ensure that the subject to item ratio was at least 10:1, the PARE RISKS factors were logically regrouped into hypothetical categories, SPAARR, which are shown in Table 1.

The principal axis factoring extraction method was used in SPSS. The factors that preceded the last major drop of the scree plot were retained [7, 11]. The direct oblimin method with the default delta (0) value was used, which allowed the factors to correlate [7]. Factor loadings greater than 0.3 were reported; this cutoff is conventionally regarded as a "meaningful loading" [18]. While the retained factors accounted for most of the variance, the remaining factors also accounted for some variance and, as such, a second EFA was conducted that forced all the items to load on the retained factors. Table 2 lists the factors that were retained from the second EFA. A value between 0.7 and 0.8 is an acceptable value for Cronbach's alpha (scale reliability) and was, thus, kept for the EFA [10].

As noted earlier, survey items were predominantly informed by the existing literature, which was technical in nature. Other, non-technical factors were only minimally addressed in the ICS cyber security research. Interviews complemented and supplemented the survey because they had the potential to identify new factors and add more depth to the EFA-retained factors.

The NVivo 9 software was used to code the interview transcripts. NVivo 9 classifies, sorts and arranges information by creating nodes (themes) and subnodes (sub-themes) as they emerge [19, 20]. The transcripts were scanned to

Table 2. Factors retained from exploratory factor analysis.

Grouping	Factors
System	Network security and monitoring; Lack of redundancy; Non-cyber/physical access; Remote access; Authentication
Preventative	Protection updates; Security testing and vulnerability assessment frequency; Ease of bypassing IDSs
Attackers	Commercial; Political; Leisure; Business-financial
Attacks	Information-seeking techniques; Installation techniques; Non-technical techniques; Attack-in-progress techniques
Result	Human health; Information; Environment and health; Order and finance; Plant operations

identify common themes that emerged in the interview transcripts. Three main themes emerged: attacker, target and dynamics.

Table 3. Factors retained from the interview analysis.

Theme	Sub-Theme	Further Sub-Themes
Attacker	Resources	Skills; Money; Time
	Organization	Alliance; Division of Labor
	Attacks	Research; Technique
Target	Accessibility	Electronic; Physical
	Prevention	Existence/Quality; Vendor; Detection
	Weaknesses	COTS; Architecture; Updates/ Testing
Dynamics	Cost-Benefit Analysis	Attack Plan; Decision Trees
	Response	Type: Isolation; Reconnaissance; Feed False Data
		Body: Industry; Public-Private; National; International
	Counter-Response	Alternate Access; Alternate Tactic
	Exit	Delete Evidence; Tracking Complexity

While the interviews yielded rich details on several factors that influence attacker decision-making, all the details cannot be provided here. Table 3 presents a summary of the factors retained from the interview analysis. Only the attacker-related resource factors are discussed here: skills, money and time. These resources are considered to be crucial for the successful planning and execution of cyber attacks on ICSs:

> If anything, some **very very good virus writing**, but more importantly **a very very very deep understanding** of the vulnerabilities

> for that system, how to exploit those vulnerabilities, how to do things with a payload ... *Penetration Tester 2 (Skills)*

> From a monetary investment, ... about **$100,000 for a single zero-day** with an exploit mind you. OK. So they put **4 of them ... Black Market value for a digital cert is b/w a 100K and 200K**... So what does that tell you? It tells you that it was funded. **Quite well-funded** in fact. *Penetration Tester 1 (Money)*

> To me, I would put it at skills, I'd put it at preparation time. I mean, this is **months worth of planning and preparation**, this isn't just a payable coding that's done in a couple of weeks. *Penetration Tester 3 (Time)*

6. Study Limitations

This section discusses the limitations of the study and the revisions made to PARE RISKS.

6.1 Comparing Attack Perceptions and Reality

The study was exploratory in nature and based on hacker and industry perceptions. As such, there was concern if the perceptions reflected reality. Did the PARE RISKS framework, which is based on hacker and industry perceptions, parallel other cyber security studies? Did this framework contribute to industry vulnerability assessments? If so, how?

Two industry assessments served as comparison points. The first report pertained to ICS cyber security assessments conducted by the Idaho National Laboratory (INL) [12], which identified vulnerabilities that could put the critical infrastructure at risk from cyber attacks. The second report was produced by the Control Systems Security Program [28] of the U.S. Department of Homeland Security. This report offers eighteen security assessments of ICS products and installations from 2004 to 2010. Both the reports were based on actual ICS assessments, the former focusing on power grid ICSs and the latter more general ICS vulnerability assessments. The results of the criminological study parallel the two assessment studies very well. Increased access and connectivity, poorly protected networks, weak authentication protocols and infrequent security and patch updates are findings that also emerge from the criminological study.

However, as noted earlier, the INL and DHS assessments were mostly technical in nature. According to RAT, three elements must coincide in space and time for crime to occur: capable offender, suitable target and capable guardian. The INL and DHS assessments focused on the second and third elements of RAT. The criminological study made the case that the first element, the capable offender, should also be considered to obtain a fuller picture of power grid cyber attacks, which require moving beyond the technical knowledge base.

First, power grid cyber attacks involve human (attacker) aspects, such as available resources and research, which can be non-technical. A capable attacker can engage in social engineering tactics that trick power grid employ-

ees into divulging sensitive information. Control system documentation and blueprints are often found online, which attackers can use to extensively study their targets and design system-specific cyber attacks. Also, attackers can physically access corporate networks, bypass firewalls and connect directly to ICSs. These issues, while non-technical, can also contribute to the occurrence of the ICS cyber attacks. Yet, they are not fully addressed in the ICS cyber security assessments.

There are other limitations with this study given the methodology chosen. Selection bias is an unavoidable survey limitation. In this particular context, the hacker and industry respondents may not have had the knowledge necessary to complete the survey. Participants may have been unaware of all the threats and cyber attack scenarios, and may have possessed varying levels of technical expertise. This limitation, however, could not be avoided given the exploratory nature of the research, and that there was no publicly-available list of power grid cyber security experts from which the survey respondents could have been solicited. This shortcoming was managed by comparing the survey responses with the technical vulnerability assessments conducted by INL and DHS, and similar results were found (as discussed above). Selection bias was not an issue for the interviews because participants were experts with more than twenty years of experience in power grid cyber security. As such, they had inside information about prior grid cyber attacks and extensive knowledge about current trends, and the techniques and strategies used by attackers.

6.2 PARE RISKS Revisions

The EFA and interview analysis each yielded several factors that influence attacker decision-making. What did this imply for the original PARE RISKS framework? Was it an adequate framework? Table 4 shows that each of the factors that was retained by the analysis is easily mapped to the nine factors from the original framework.

It is important to note, however, that some of the elements originally included for a few PARE RISKS factors did not emerge in the analysis. EFA sifted through the original PARE RISKS elements and condensed them into a new set of factors. Thus, despite the clean mapping back to the PARE RISKS framework, some of the factors now had fewer items. For instance, the "Response and Recovery" factor was now simply "Response;" the "Recovery" component did not seem to impact the attacker decision-making process. Nor did this component emerge in the interview analysis as a relevant factor that influences how ICS attackers make decisions.

Although the original framework was adequate to address attacker decision-making, new elements still need to be incorporated, such as physical access to ICSs. Other new elements included how attackers manage industry responses; for instance, alternate access and techniques could be used to continue the attack. Another addition incorporated the attacker's need for well-designed attack plans, where all possible attack scenarios are mapped out with possible courses of action. Finally, the "Exit Strategy" was also a new addition to the

Table 4. Revised PARE RISKS framework.

Factors	**Items** (New items are italicized)
Preventative Measures	Protection updates Ease of bypassing IDSs Existence/quality Vendor-based Network security and monitoring
Attacks and Alliances	Attacker Type: Commercial; Political; Leisure; Business-financial Organization: Alliances; Division of labor Attack Technique: Information-seeking techniques; Installation techniques; Non-technical techniques; Attack-in-progress techniques Resources: Skills; Money; Time
Results	Data modification; Plant operations
Ease of Access	Electronic/remote; *Physical* Weak authentication
Response	Type of Response: Isolation; Reconnaissance; Feed false data Responding Body: Industry; Public-private; National; International *Counter-Response: Alternate access; Alternate tactic* *Exit Strategy: Delete evidence; Tracking complexity*
Interconnectedness and Interdependencies	Human health; Environment; Civic order; Finance
Security Testing and Audits	Security testing and vulnerability assessment frequency
Knowledge and Research	Research and development *Attack Plan*
System Weaknesses	Commercial-off-the-shelf software Architecture/legacy systems Inadequate redundancy

PARE RISKS framework. Attackers could delete logs or evidence that could be traced back to them, and they could also hop through several transit points in cyber space to mask their digital footprints.

7. Policy Implications

While this study is based on the perceptions of hackers and industry personnel, the policy implications offered here are based on their extensive knowledge base and experience. All the implications cannot be discussed due to space constraints. However, the four most important implications for ICS cyber security policy and practice are presented.

7.1 Better Security Practices

- IDSs may not be the most effective means to detect malicious activity. Human resources for monitoring IDSs and reviewing entry/exit logs are minimal; improving real-time detection mechanisms is a must.

- Poor authentication practices permit malicious entities to easily access ICSs. Better password practices, such as encrypting passwords when they are stored and when they are transferred through internal networks, using complex passwords, frequently changing passwords, and not sharing passwords, can all help minimize unauthorized access to ICSs.

- ICS information can be obtained through various means; malicious entities share this information in online hacking forums and use it to design attacks. While industry cannot control the information released in hacking forums, it can regulate the amount of ICS information (e.g., blueprints, passwords, system versions and vulnerabilities) that is released to unauthorized entities. This would make it harder for malicious entities to study targets and design appropriate attacks, thereby making it more difficult to target ICSs.

- Situational crime prevention focuses on reducing crime opportunities instead of identifying potential attackers based on their characteristics. Situational crime prevention offers 25 crime prevention techniques based on five principal categories of action: (i) increasing the effort required by the attacker to commit the crime by hardening targets; (ii) increasing the risks of detection; (iii) reducing the rewards of critical infrastructure attacks; (iv) removing excuses by educating employees; and (v) reducing provocations by setting formal regulatory policies [4]. Situational crime prevention principles can help design security measures that extend beyond the existing technical solutions.

7.2 Definition (In)Consistency

Hackers and industry personnel feel that there is a lack of consensus regarding how threats, vulnerabilities, risks and consequences are defined. Furthermore, both hackers and industry personnel believe that there is no consensus on these terms within their communities.

> [People] will **confuse threat, vulnerability, and risk and not actually understand what it is** ... but the problem is that the reason we don't understand how to really define risk is because **there is no consensus on how we define threat, vulnerability, and consequence**, which is funny as hell... *Penetration Tester 2*

The different definitions of these terms are problematic because, if there is no clear understanding about the terms and how they are connected, then the identification of security issues and risks are flawed because they are based on different definitions. The (multiple) incorrect views lead to security (and

prevention) measures that are grossly ineffective. One approach for reducing inconsistencies in definitions is to develop a concise set of definitions of threats, vulnerabilities, risks and consequences that are uniformly used and practiced throughout industry. This would minimize confusion about the definitions, allow a common context to compare incidents and help design effective vulnerability assessments, security testing protocols and prevention strategies.

7.3 Education Programs

The hacker and industry groups both believe that stovepiping knowledge impacts the security of ICSs. Industry members who are not involved in security and/or penetration testing activities generally possess limited technical expertise to comprehend the importance of vulnerability assessments and security testing.

> And it **took quite a lot to help educate those guys on what risks are**. I mean, the initial discussion with those guys was "hey – this is regulatory stuff called FERC and NERC, and you know – what do we need to worry about" - I'm like "oh good grief – oh god" – OK people – let's do little bit of education first. *Penenetration Tester 3*

> The SCADA industry professionals have **relatively limited technical expertise at implementing security controls**. Their employers have not put a lot of effort into changing that situation. *Power Grid Representative 4*

Building the knowledge bases of non-technical industry personnel can be done through education programs. These programs should educate company executives and management on the basic ideas of threats, vulnerabilities, risk, and consequences, how they are related, and why they are important.

7.4 Mandatory Security Budgets and Programs

The power sector and the ICS vendor community should have mandatory security budgets. Each power utility should be required to set aside funds dedicated to continuous security monitoring, frequent and rigorous security testing, vulnerability assessments and audits. ICS vendors should be required to follow suit. The interview data revealed that the hacker and industry groups both agree that only a handful of ICS vendors engage in (poorly developed) testing practices, which undermines the effectiveness of their products. Furthermore, vendors need to continue to support their products even after industry updates security measures.

> The problem again is that this goes back to the vendor who says ''well, hey, **we won't support your system unless you were at this version**," and well that version is vulnerable to an attack, so what are we supposed to do? So you have to find **different mitigations or risk, becoming unsupported by the vendor by putting a host of firewalls into your system**. *Penetration Tester 1*

> For most ICSs, **the introduction time frame for a new item of software is umm... the earliest at about three months, typically is six months, twelve months are not unusual**... you don't want the change ... to cause more harm than the change you were trying to defend against. [Updating] is a pretty **slow process**, and only in the rarest case does it happen in less than three months... pressure from some of the larger utilities, **some vendors do testing**. Vendor industry is very **immature ... and their testing is not particularly effective... Some of the vendors don't do any testing at all**. *Penetration Tester 4*

If the vendor software development cycle is indeed a slow process, the power industry should not have to choose between security and support. Instead, security practices and vendor support should be performed synchronously.

8. Conclusions

This study makes the case that power grid cyber attackers are active decision-makers who are influenced by several technical and non-technical factors. Future studies should further explore the complex temporal, interactive and causal relationships underlying attacker decision-making. This study has focused exclusively on the power grid. Future research should test the generalizability of the PARE RISKS framework to other infrastructures, which will help refine the framework and enhance its applicability.

An unexpected, yet important, finding that emerged is that attackers engage adaptive decision-making processes. The participant interviews revealed the temporal and dynamic nature of ICS attacks by focusing on the pre-attack and attack-in-progress periods. The temporal aspect of ICS attacks suggests that ICS attackers engage in extensive research and planning to study the target and its weaknesses before proceeding with an attack. The dynamic property of ICS attacks further supports the notion that attackers are not passive; they learn from their experiences, adjust to their environments and engage a constantly-changing decision-making process. Five distinct stages of the crime script emerge from the interview data: preparation, entry, initiation, attack dynamics and exit. Future research should study these stages, which can help project attacker moves and, in turn, identify the most effective countermeasures.

References

[1] S. Baker, S. Waterman and G. Ivanov, In the Crossfire: Critical Infrastructure in the Age of Cyber War, McAfee, Santa Clara, California, 2009.

[2] A. Beatty, U.S. cybersecurity chief warns of "market" in malware, *Agence France-Presse*, June 17, 2009.

[3] E. Bumiller and T. Shanker, Panetta warns of dire threat of cyberattack on U.S., *New York Times*, October 11, 2010.

[4] R. Clarke, Situational crime prevention, in *Environmental Criminology and Crime Analysis*, R. Wortley and L. Mazerolle (Eds.), Willan Publishing, Portland, Oregon, pp. 178–194, 2008.

[5] L. Cohen and M. Felson, Social change and crime rate trends: A routine activity approach, *American Sociological Review*, vol. 44(4), pp. 588–609, 1979.

[6] D. Cornish and R. Clarke (Eds.), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, New York, 1986.

[7] A. Costello and J. Osborne, Best practices in exploratory factory analysis: Four recommendations for getting the most from your analysis, *Practical Assessment, Research and Evaluation*, vol. 10(7), pp. 173–178, 2005.

[8] N. Denzin (Ed.), *Sociological Methods: A Sourcebook*, McGraw-Hill, New York, 1978.

[9] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Symantec, Mountain View, California, 2011.

[10] A. Field, *Discovering Statistics Using SPSS*, Sage Publications, London, United Kingdom, 2013.

[11] N. Grant and L. Fabrigar, Exploratory factor analysis, in *Encyclopedia of Measurement and Statistics*, N. Salkind (Ed.), Sage Publications, Thousand Oaks, California, pp. 332–335, 2007.

[12] Idaho National Laboratory, NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, INL/EXT-10-18381, Idaho Falls, Idaho, 2010.

[13] T. Jick, Mixing qualitative and quantitative methods: Triangulation in action, *Administrative Science Quarterly*, vol. 24(4), pp. 602–611, 1979.

[14] N. King and C. Horrocks, *Interviews in Qualitative Research*, Sage Publications, Thousand Oaks, California, 2010.

[15] McAfee, Advanced Persistent Threat, Santa Clara, California (`blogs.mcafee.com/tag/advanced-persistent-threat`).

[16] National Security Telecommunications Advisory Committee, Electric Power Risk Assessment, Washington, DC (`www.solarstorms.org/ElectricAssessment.html`), 2000.

[17] P. Oman, E. Schweitzer and J. Robert, Safeguarding IEDS, substations and SCADA systems against electronic intrusions, *Proceedings of the Western Power Delivery Automation Conference*, 2001.

[18] E. Pedhazur and L. Schmelkin, *Measurement, Design and Analysis: An Integrated Approach*, Taylor and Francis, New York, 1991.

[19] QSR International, NVivo 9 Features and Benefits, Melbourne, Australia (`www.qsrinternational.com/products_nvivo_features-and-benefits.aspx`).

[20] QSR International, What is Qualitative Research? Melbourne, Australia (`www.qsrinternational.com/what-is-qualitative-research.aspx`.

[21] R. Rantala, Cybercrimes Against Businesses, 2005, Special Report NCJ 221943, Bureau of Justice Statistics, U.S. Department of Justice, Washington, DC, 2008.

[22] A. Rege, Cybercrimes against critical infrastructures: A study of online criminal organizations and techniques, *Criminal Justice Studies*, vol. 22(3), pp. 261–271, 2009.

[23] A. Rege, Offender decision-making in industrial control systems cybercrime, presented at the *Cyber Infrastructure Protection Conference*, 2012.

[24] S. Sloane, The U.S. needs a cybersecurity czar now, *Bloomberg Businessweek*, August 13, 2009.

[25] Staff of Congressmen Edward J. Markey (D-MA) and Henry A. Waxman (D-CA), Electric Grid Vulnerability: Industry Responses Reveal Security Gaps, U.S. House of Representatives, Washington, DC, 2013.

[26] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2012.

[27] L. Tinnel, O. Saydjari and D. Farrell, Cyberwar strategy and tactics: An analysis of cyber goals, strategies, tactics and techniques, *Proceedings of the IEEE SMC Workshop on Information Assurance*, pp. 228–234, 2002.

[28] U.S. Department of Homeland Security, Common Cybersecurity Vulnerabilities in Industrial Control Systems, Washington, DC, 2011.

[29] U.S. Government Accountability Office, Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities and Remaining Challenges, Report No. GAO-05-327, Washington, DC, 2005.

[30] B. Wingfield, Power-grid cyber attack seen leaving millions in dark for months, *Bloomberg*, January 31, 2012.