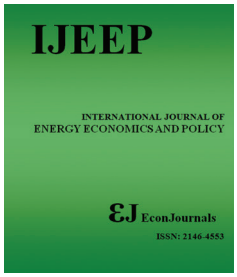


International Journal of Energy Economics and Policy

ISSN: 2146-4553

available at http: www.econjournals.com

International Journal of Energy Economics and Policy, 2017, 7(5), 250-262.

Economic Impacts of Cyber Security in Energy Sector: A Review

Sampath Kumar Venkatachary[1]*, Jagdish Prasad[2], Ravi Samikannu[3]

[1]Amity University, Jaipur, Rajasthan, India, [2]Amity University, Jaipur, Rajasthan, India, [3]Botswana International University of Science and Technology, Palapye, Botswana. *Email: sampathkumaris123@gmail.com

ABSTRACT

The new age "digital age" is bringing rapid change in the form of connections, integration, supply chain management, models and much more. As a result, security is a big business, securing critical data, operations, the customer profile is beyond the four wall of physical security. It is therefore essential to re-look on the definition of security and increase resilience on technology. The electric power system comprises of both IT infrastructures and electrical systems which include cyber systems, people, physical systems, money. Threats can be physical, internal or external threats and cyber threats can emerge from anywhere. Tackling cybercrimes and cyber-attacks on the energy sector poses major challenges on its own. These threats cannot be eliminated but only mitigated. The threat mitigation costs money, efforts, downtime, economic and psychological impacts on the industry that could result in damage to company's performance and the national economies. The paper aims to highlight various security attacks on the energy infrastructure and its economic impacts. While discussing the economics, the paper presents mechanism, and emphasizes the need for global security coordination to mitigate threats.

Keywords: Systemic Cyber Event, Syntactic Attack, Digital Age
JEL Classifications: A19

1. INTRODUCTION

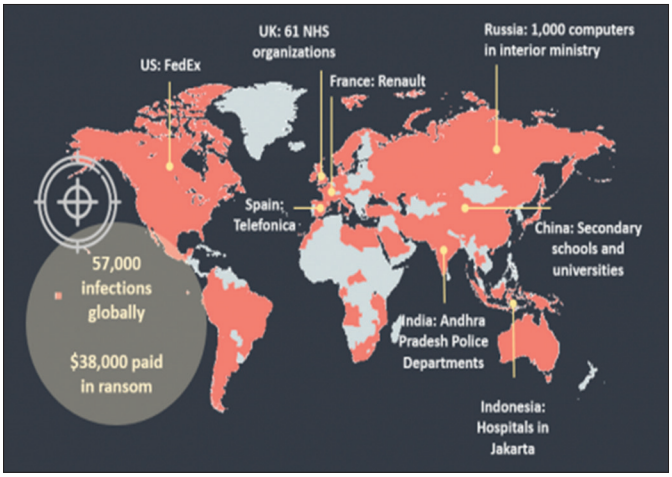
Energy infrastructure (EI) is a part of the critical infrastructure and is arguably one the most important, complex environment as many other sectors depend on it for essential services delivery. It ensures the smooth functioning of modern society and serves as the backbone for economic activities. Therefore, unavailability of this service leads to potential ripple impacts on the economy, civil society risking gross domestic product (GDP), the trade deficit. High-speed internet connectivity has made the world a smaller place. The internet of things has changed the (Vish, 2017) way how the countries have interfaced with each other and revolutionized the business process. Threats are becoming dangerous, more sophisticated, persistent, complex. To understand the dynamics of cyber-attacks fully, it is critical to understand dimensions in cyberspace, which remains confined to its space with no limits on earmarked boundaries or borders. (Marwan, 2017) this hyper connectivity is a powerful tool which is an opportunity for growth in both the public and the private sectors be it Governments or Business, individuals alike.

The motivation of attackers over time has evolved, driven by financial gain. This has resulted in a well-organized crime market for trading in malware and stolen information. This heinous design is intended to create mayhem and cripple the Nations infrastructure facilities (Anand, 2014). Cyber-attacks cause significant loss to intellectual property, business intelligence, economy, can drive up the cost of security, damage reputation of a company and disrupt work flow. Many companies reporting major attacks suffer a 1-5% drop in their stock value (Bryan, 2014). While some companies may overcome these barriers, others may lose everything. Nortel networks, a Canadian based telecom company, filed bankruptcy in 2009 when Chinese hackers infiltrated their network. It took several years for the investigators to discover the extent of damage to critical data (Siobhan, 2012) (Bryan, 2014). The latest energy systems "smart energy systems" deployed across the developed and developing nations, depended on ICT technologies, has led to exponential growth of networked intelligence in the energy sector and the consumer premises. This vast and massively expanding sector have opened up new "attack surface," which forms the backbone of the energy industry. As the energy system is interconnected with every other critical

infrastructure, the cyber security threat is real. (David et al., 2016) James Lewis defines the threat of cyber attacks as "a massive electronic Achilles' heel" (James, 2002). It is a misconception that technologies are immune to any failure, accident, misjudgment or deliberate sabotage. While many small scale cyber security threats are carried out on a daily basis attacks on a larger scale is generally over a period. Technologies like renewable energy system for generating electricity storage has far reaching socio economic benefits. Transformations depend on deployment of virtual power plants, smart grids using smart technology. However, these digitization strategies have both pros and cons. All of these technologies, smart energy system is therefore created through the significantly greater use ICT digitization of power generation and distribution. The increasing decentralization of the energy system which includes a consumer who is also a prosumer across the energy value chain poses a greater threat to the energy sector (David et al., 2016).

The revelations reports on Stuxnet, Duqu, Flame, Shamoon, and Dragonfly portray a glimpse of how cyber attacks is a major battle ground to gather intelligence and launch subversive activities. Most cyber weapons are inexpensive but potent tools that can be used as both offensive and defensive weapons, which can bring down a country's economy or hold it to ransom. The recent well-coordinated attack by Wanna Crypt worm during the month of May 2017 (12th) is a classic example of cyber war. This cryptic attack exposes the vulnerabilities and stark realities of how a worm could cause enormous damage in very little time. Reports indicate that WannaCry caused extensive damage including critical infrastructures like hospitals, railway systems, and telecommunication networks spread across 100 countries globally (Figure 1). Kaspersky reported that Russia was the worst hit with approximately 60% of infected systems and many other nations like Ukraine, Taiwan, India, China, Romania, Spain, Egypt, Brazil, Spain, Italy. Roughly 59000 computers were believed to have been affected at the onset of the worm release in nearly 100 countries, in addition to individuals, the outbreak (Rhidi, n.d.) also affected critical infrastructures in countries including Germany, Russia, and the United Kingdom. In the UK, the NHS had to shut down some of its systems canceling outpatient appointments. The worm released on the internet just made rounds affecting all the computers vulnerable without the user having to click or open a phishing email or document (Rhidi, n.d.) (Alexander, 2017). Though the worm was shut down with little efforts from the security experts, it did draw attention how effective a simple malware could be used to damage systems. With this, it raises the question of states global cyber preparedness towards cyber war. It also brings out that information security industry views cyber-attacks more as a business development than as a tool to pool resources together to eliminate threats. According to Dell's 2015 Annual security report, the cyber-attacks on Industrial Control Systems (ICS), especially against supervisory control and data acquisition (SCADA) systems, doubled in 2014, and there were more than 160,000 incidents (Daniel and Bailey, 2016). This suggests that efforts of information security need to pool together and the community as a whole needs greater active and trustworthy alignment rather than relying on a combination of serendipity and lazy coding to prevent next attack.

Figure 1: Wanna Crypt worm attack (Rhidi, n.d.)



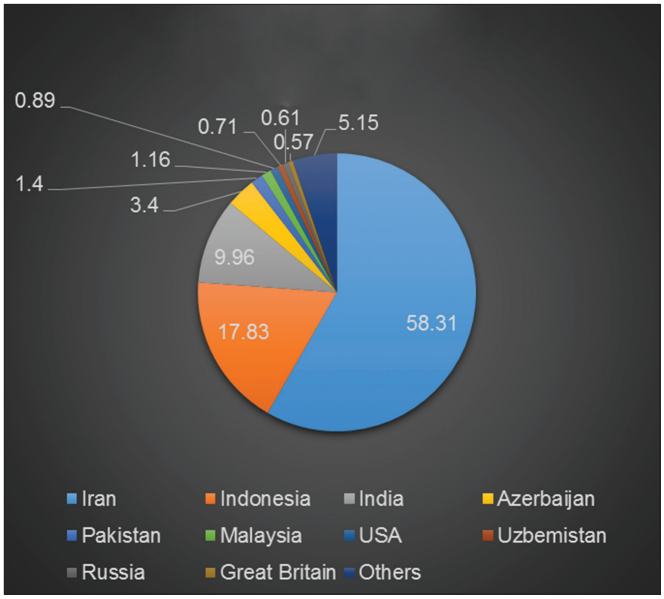
This paper primarily highlights cyber security and importance on well-known emerging concepts, systems and technologies of and how it can contribute to meet the security threats. The paper also highlights different vectors, algorithms used as means for cyber-attack from 2003 on Critical Systems and its impacts. The organization of the paper is as follows: The second section presents cyber security, and related research works in the area, section 3 portrays economics invovled in cyber security, followed by precautions, defense mechanisms and lastly section 4 offers discussion, recommendations and concluding remarks.

2. ANALYSIS OF CYBER SECURITY

Cyber security threat as can be defined as any "possibility of a malicious attempt to damage or disrupt a computer network or system" (Tarja and Martti, 2017). Cyber-attacks on critical infrastructure is lucrative given its importance and impacts on daily operations (Vaidya, 2015). The attacks are carried out by exploiting the vulnerabilities supporting the ICS systems in the CI. There are incidents where personal, financial information, is accessed and hacked almost on a daily basis. Vulnerability to data theft has become one of the major drawbacks of financial and other commercial transactions. The industrial crimes, however, come in a different dimension, where the data is used for espionage or perhaps to bring out an industrial sabotage by breaking into corporate or government network to obtain blue prints or classified information. It is widely possible for an attacker to get inside the network and lurk for months or years scooping information of interest. In many a case, it is an insider threat due to a disgruntled ex-employee. A well-organized crime network targeting this infrastructure sell valuable personal information of compromised accounts for very little money and using the stolen information for any future cyber attacks. Attack strategies provide a more vivid picture to support the argument. ICS forms the core and the backbone of any systems in energy; it is essential to study the vulnerabilities in the system. With more and more information becoming public in ICS, many of the vulnerabilities could lie dormant for years to come before their presence is revealed. Out of the 189 vulnerabilities in ICS components detected, 49% were termed critical, and 42% said to have medium severity (Oxana

et al., 2015). Wide spread attacks on ICS like Stuxnet, slammer or blaster worm (Loney, 2003; Roberts, 2003; David et al., 2003) exploited known vulnerabilities although patches were available for most of them and released in advance. Phishing/spear phishing was the most popularly used mechanism to deploy and deliver malware. DDoS attacks remain popular for disrupting services (Vaidya, 2015). A continued motivated attack on CI can severely and adversely affect the national security and cripple the nation depriving the country of valuable resources. The global data on the cyber security attacks on infrastructure from July 2012 to 2013, on an average, had about 74 targeted attacks per day globally. Of these 8-9 attacks were on energy sector alone accounting for the second most targeted system, accounting for 16.3% (Candid, 2014). According to Symantec, the energy sector was the second most targeted (SenseCy, 2014) sector accounting to 80%. Of this 55 % involved persistent sophisticated attacks by hacktivists, insider threats, and criminals. In the latest report by ICS-CERT (ICS-CERT, 2016) a critical analysis of comparison of data for 2014 and 2015 (ICS-CERT, 2014) (ICS-CERT, 2015) indicates that there has been a substantial drop in the targeted energy sector.

Figure 2: Stuxnet infection (geographic distribution) (Murchu, 2011)



Brazil blackout in March 1999 left nearly 70% in the dark for more than 5 h affecting over 97 Million citizens. In 2003, left parts of US and Canada in chaos, leaving them high and dry without power. In a matter of minutes many places of Pennsylvania, Massachusetts, New York, Connecticut, New Jersey, Ottawa went dark. The darkness caused the public transport system to go out. Many utility corporations were shut due to this power shut down and forced emergency services like hospitals to run on limited power (CIP Center for Infrastructure Protection, 2003). In 2003, slammer worm aka Sapphire disrupted Ohio Nuclear Plant (Kevin, 2003).

Stuxnet attack (Figure 2) on EI in Iran 2010 affected SCADA systems in Bushehr Natanz nuclear power plant. This latter had affected many Windows-based computers in the country. This was designed to spy on the ICS. It was also capable of causing the centrifuges to spin out of control and tear themselves apart. Kaspersky labs first discovered the Stuxnet worm on a request from a Belarusian company on behalf of Iran's nuclear agency. Stuxnet proved how perfect cyber-attack could result in significant physical damage to EI as well as the ensuing consequential/business losses (Charles et al., 2014; David, 2013). In India, it affected close to about 10% of the systems across the country running Siemens SCADA (Murchu, 2011). The target, in this case, was only the Siemens controlled SCADA systems. In this pattern of syntactic attack, the computer infrastructure was damaged, modifying the control logic of the system inducing delay and system being unpredictable and was unique in every attack instance (Amar, 2016). During the same year, 2010, a new Trojan named Night Dragon was injected as SQL injection targeting global oil companies. The attacks had started as late as 2009 to gather information on financial reporting, project details in the industry. The motive was to steal the passwords, dump password hashes, sniff authentication messages and exploit the active directory configuration (Candid, 2014). In 2011, a new malware supposedly thought to be related to Stuxnet was discovered by Kaspersky labs. It was later named as DuQu 2.0 (Anonymus, June 2015). DuQu searches for information and vulnerabilities to attack ICS with a motive to gather information and not destroy in addition to stealing digital certificates. However, use on PC's has been found to delete all information on the system (Anonymus, November 2011). DuQu remains a mystery as its actual and exact method is not entirely known (Anonymus, November 2011). According to McAfee DuQu uses 54 × 54 pixel JPEG file to encrypt dummy files and containers to smuggle data to its command and control center (Anonymus, n.d.; Venere and Szor, 2011; Kim, 2011). On 30th July of 2012, was an unusual Tuesday when more than 600 million people in India, i.e., approximately 10% of the world's population had been left without power for several hours (Benahmed and Smahi, 2016). The cause was not revealed and was simply attributed to grid failure. In yet another attack in the same year (2012), Saudi Aramco was hit by a virus named Shamoom disabling over 30,000 computer work stations which disrupted for months (Candid, 2014; Anonymus, 2012; Leyden, 2012; Perlroth, 2012). Weeks later Qatar reported that one of their gas companies was also affected by the same virus forcing their entire network to be offline for days (KPMG Global Research Institute, 2013). A similar repeated third wave of attacks by Shamoom. W32B (W32.Disttrack.B) was noticed in February 2017 in Saudi Arabia (Anonymus, 2017).

During 2013, North American energy companies were targeted with a simple Trojan known as Dragon fly and in spring 2014 by Havex. The primary technique used in Dragonfly was Remote Access Trojan (RAT), powered by Havex, to provide administrative control over an infected unit. While spear-phishing access, the software, named Havex by the cyber security group F-Secure, was used as watering hole attacks. When a particular unit was compromised, legitimate websites were used for redirection to Dragon fly servers, masking and thus making it difficult for industry experts to suspect the internet site as a source for the Havex. The last phase of the campaign used masquerading techniques by Dragonfly in which legitimate applications of vendor websites were infected by the worm, from which businesses would download the Havex infected software (David, 2014; Anonymus, 7 July 2014).

Often more dangerous and damaging is semantic attacks as it uses the human element by exploiting the confidence of the user in the system (Col, n.d.). In this form of attack, the information keyed in is modified at the whims and fancies of the controller without the knowledge of the user to introduce errors. According to Symantec Research Labs in 2013 parts of Austrian and German power grid collapsed after a control command was accidentally misdirected, by exploiting a human interface (Candid, 2014). The report also suggested that the command packet was broadcast from a German gas company to test their newly installed network branch. This transmitted to Austrian energy power control and monitoring network. It generated huge messages which generated, even more, data packages which in turn flooded the control network which translated as a DDoS attack. As a solution, part of the network had to be isolated and disconnected. It was resolved without any power outages (Candid, 2014). The global concerns about India's network security, however, grew after June 2015 when hackers got into India's National Informatics Centre, thus compromising crucial, sensitive data. The mode of the attack went undetected for months. The Government of India which ran a survey through its nodal agency indicated that over 780 attacks damaged several computers in 88 cities and over 350 hacking attempts on sensitive computer systems (Staff Correspondent, 2014; Amar, 2016). The recent WannaCrypt attack is a systemic (Hanouz, 2016) cyber event in the sense that as an individual component of critical infrastructure system, it caused significant delay, denial of service, breakdown of components, loss, and disruption, that impacted not only originating areas but cascaded into relative geographic regions resulting in adverse effects to both the public, the security companies, economic security and national security. The breach had left many unpleasant and unhappy customers across nations. The details of various facilities attacked, and different algorithms used as means for the attack is shown in Table 1 (Cyber security attacks in various EI facilities).

3. CYBER SECURITY COSTS MILLIONS

In the energy sector, the focus is to ensure reliability and resilience in the event of a cyber-attack. The sector under attack cannot be disconnected from the network it could easily affect the systems resulting in safety issues, blackouts, line faults. Unlike IT cyber security components, which include confidentiality, integrity, and availability, the prerogative in energy sector depends on applications specific to the industry. For example in a generation, transmission and distribution, availability, integrity are the most important components. In a smart grid network like AMI, customer data is most critical. Any form of cyber-attacks or cyber terrorism on the EI will have detrimental effects on the economy. It impacts trade, competitiveness, innovation, economic growth, GDP. It will translate to losses. The losses can be substantial which could result in business disruption, loss of time and money and damage to reputation. On a financial side, the results will be on downtime, productivity loss depending on the attack mode or where the attack is centered, it could be anything ranging from application level vulnerabilities to targeted segment. The economic impact will have many dimensions and aspects with impending effects on society, organization, individual. Many countries spend a major chunk of their budget in fighting with crimes. With the IT infrastructure adding to the list of the Country's Budgets, humongous amount of resources and money need to be invested in cyber security to mitigate risks. The major challenging economic consequences of cyber-attacks are budget constraints and resource limitations" (Lemieux, 2011). Furthermore, the investigation resources like sufficient workforce to be employed in the case of a cyber-attack are always limited. The cost of cyber-attacks will continue to increase as more and more business functions are computerized.

3.1. Measuring Costs in Cyber Attacks

Organizations may have good reasons not to disclose cyber breaches. It is important to note that the mechanism of measuring cyber-attacks depends on accurate cost data assessment. Without standards for measuring costs in cyber-attacks. A cyber-attack involves many associated costs which can neither be quantified or qualified easily. As a result, there exists a gap. This gap on internal data mirrors the absence of public data on cyber-attacks (Brian et al., 2004).

Cyber-attacks are a tax on innovation and slow down the global research and innovation reducing the rate of return to investors and innovator. While Government's across the globe begin systematic efforts to collect and publish data on the cyber-attacks to help countries and companies fine tune their risk and aid in analysis about potential hazards, it has numerous snags and challenges on many fronts. According to many security companies, very few companies are willing to share their attacks patterns on their infrastructure. It simply means that any dollar amount (Costs) for global cyber-attacks is only an estimate based on incomplete or non-reliable data. It is also true that few nations have made reasonable efforts to calculate their losses from the cyber-attacks, most have not. Many developing countries are no exception. The primary reason being "fear of exposure" will lead to company's finances being hit. With companies facing global challenges protecting and enhancing its security on infrastructures due to myths that any exposure could result in larger financial impacts, very few companies come forward to publish their data on potential breach in the security.

According to the latest research report by Ponemon Institute in collaboration with HP on a sample of 237 companies (Ponemon Rept, 2016), it was noted that the cyber-crime had increased when compared to the previous years. EI is still the potential leading sector, next only to financials, regarding the attack. (Ponemon Institute, LLC, April 2011) From the Table 2 and Figure 3, US sample reports the highest total average cost at $15 million followed by Germany, Japan, UK, etc. According to McAfee report 2015 (Carlos et al., November 2015) the losses ranged from $15 billion to $1 Trillion due to various attacks. Computer security consulting firms that compile these figures, often fail to consider the number change that depends on the nature of the attack on the focused firm, it is important to note that the spiraling costs of the cyber security are impacting the economies in many countries.

3.2. Measuring Economics Impacts in Cyber Attacks

Although the impact of cyber-attack has been difficult to measure due to various elements involved in it, from an economic point of

Table 1: Different facilities attacked

Year	Target facility	Country	Agent	Type	Impact	Algorithm	Exploitation vector	References
2003	Banking facility; Ohio nuclear facility	US	Slammer aka Sapphire	Virus	Unknown	PRNG	Multi-vector worm	Martin, (2004) David et al. n.d.; Kevin, 2003
	Railways	US	SoBig	Virus	23,000 miles of one railway line	PRNG	Multi-vector worm	Martin, 2004
2004	National science foundation's Amundsen-Scott South Pole station	Romania	Unknown	Virus	Controlling life support systems of Antarctic research station-cyber terror attack	Unknown	Unknown	Poulsen, 2004
2009	Civil aviation	US	Unknown	Malware	Data compromise; shutdown of systems	Unknown	Unknown	Siobhan, 2009; Elinor, 2009
2009, 2010	Natanz-Iran's nuclear plant (centrifuges)	Iran	StuxNet	Malware	Iran's nuclear centrifuges were replaced at an alarming impact in the range of 1000-2000 nos. The impact of this attack was world wide	MD5, AES	MS10-046 (0-day) MS10-061 (0-day) MS08-067 (patched) 0-day (unpatched); CVE-2010-2568	Nicolas, 2011; Ralph, November 2013; David, 2013; Ellen and Joby, 2012; Naraine, 2010; Sanger, 2012; Thomson, 2013
2011	No specific target; Iran nuclear plants	Iran; no specific target	DuQu	Malware	Targeted;	Camellia, AES, XTEA, RC4, different multibyte XOR-based encryption	CVE-2011-3402	Anonymus, June 2015; Boldizsár et al., 2011; Boldizs'ar et al., 2012; Venere and Szor, 2011; Anonymus, 2011; Iran Admits Nuclear Sites Hit by 'Duqu' Cyber Weapon, 2011
2012, 2015	Saudi Armaco (UAE); RasGas (Qatar)	Saudi Arabia, Qatar	Shamoom (alias) distract	Malware	35,000 Machines; D-Dos attack	MD5, SHA-256		Anonymus, 2017; Leyden, 2012; Anonymus, 2012; Perlroth, 2012
2012, 2015	Iran's nuclear plant, Lebanan, Sriya, Sudan, etc.	Iran, Lebanon, Sriya, Sudan, Egypt	Flame aka Flamer, (Stuxnet. Resource 207)	Trojan	Approx. 1000 Machines	MD5, SHA-256	MS10-061, MS10-046; MS09-025	Boldizsár et al., 2011; Anonymus (sKyWiper Analysis Team), 31 May 2012 (Alexander, 2017; Damien and Christopher, 2012; Ellen et al., 2017; Goodin, 2012

(*Contd...*)

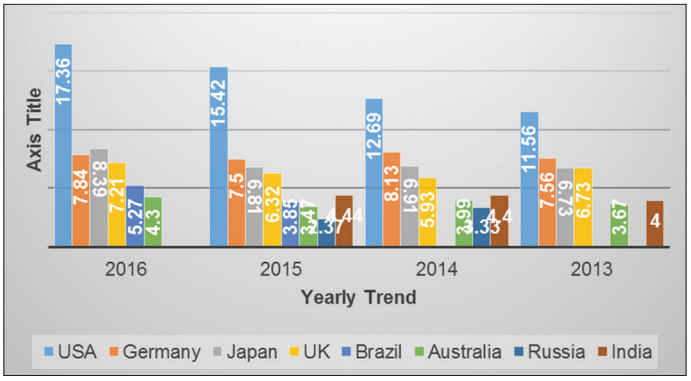
Table 1: (*Continued*)

Year	Target facility	Country	Agent	Type	Impact	Algorithm	Exploitation vector	References
2013	North American energy companies		Dragonfly	Trojan	More than 1000 energy companies in North America and Europe	SHA-1, SHA-256, MD5,	CVE-2011-0611; CVE-2012-1723, CVE-2013-2465; Spear Phishing, Watering hole, Remote Access Tools	Anonymus, 2014; Joel, 2014; Security Response Team, 2014
2014	SCADA/ICS	Europe (France, Germany, Romania, Greece, etc)	Havex	RAT Trojan	Noticed in 146 command and control server	RAT new method	CoInitializeEx, CoCreateInstanceEx; COM	David, 2014; Nell, 2016
2015	Ukrainian Kyivoblenergo	Ukraine	Black energy 3	Trojan	225,000 Customers left without power for 6 h on a cold December	AES	CVE-2014-751; server blocks	Robert et al., 2016
	Polish airlines	Poland	Unknown	Malware	1400 passengers grounded	Unknown	Unknown	Marsh, 2015
2016	Gundremmingen (German nuclear power plant)	Germany	W32.RAMNIT; Conficker	Malware	Isolated Incident on the power plant as the plant was isolated. The previous version of Conficker A, B, C, D, E is reported to have caused damage to 1.7 million people	SHA-1#, RC4, RSA	CVE-2014-4113; TA08-297A (other), CVE-2008-4250 (other), VU827267 (other), Win32/ Conficker.A (CA), Mal/ Conficker-A (Sophos), Trojan.Win32.Agent. bccs (Kaspersky), W32. Downadup.B (Symantec), Confickr (other)	Anonymus, 2011
2017	WannaCry	India, Russia, China, Taiwan, UK-across globe	WannaCry	Malware	World-wide; 200,000 computers including magnetic resonance imaging scanners in NHS, UK. Worst affected countries are Russia, India, Taiwan, Ukraine	RSA, AES	MS17-010 (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, and CVE-2017-0148)	Raj, 2017

Table 2: Total costs of cyber-crimes in seven countries (in Million) (Ponemon Rept, 2016; Ponemon Rept, 2015)

Year	USA	Germany	Japan	UK	Brazil	Australia	Russia	India
2016	17.36	7.84	8.39	7.21	5.27	4.30		
2015	15.42	7.5	6.81	6.32	3.85	3.47	2.37	4.44
2014	12.69	8.13	6.91	5.93		3.99	3.33	4.4
2013	11.56	7.56	6.73	4.72		3.67		4

Figure 3: Cyber-crime trend - costs in million (USD)



view, it is a significant activity. Table 3 portrays a matrix. From the table, it is easy to visualize and summarize different challenges and impacts faced by different agents/adversary. This table is further broken down into various elements in Table 4.

In understanding the elements, different components are impacted at various levels of a security breach. A potential breach in any stage has a profound ripple effect in the other areas as well. For example, a beach in SCADA will potentially affect the monitoring, physical infrastructure, load balancing and other regions.

3.3. Strategic Areas, Precautions, Defense Mechanisms

Considering the impact of the cyber threats, it is essential that proper precautionary measures and defense mechanism be employed in protecting the critical infrastructure of the Nation. Careful strategies are required to mitigate the impacts of threats in the form of cyber-attack. Historical data and well-documented data can be used as metrics to analyze and provide necessary solutions. It is essential that a strong private-public partnership is built to document the disasters since well-documented evidence can be used as metrics for future understanding of cyber-attacks. Cyber security is a complex issue, it is understood only by a small fraction of secluded individuals or cadre, it is essential that participation and training regarding handling need security need to be driven down the chain to the lower level and to apply risk management principles that have worked well. Figure 4, discusses some of the strategic areas. The main partners in the defending cyber security is a proper public-private partnership. This would enhance the various strategies and mechanism to mitigate cyber risks. However, it is essential to understand that some components in designing a security system are unique to each and every user profile, though the common elements will govern the underlying component of the security.

The human element forms the core of cyber-attack and is the weakest link. It is essential that organizations create awareness and enforce strict security policies while educating the simultaneously. The second in line for a cyber-attack is the computers. A compromised computer can be sourced or platform for the attacker's entry into the network of the system to explore deeper. Therefore it is essential and critical to secure and harden the operating system with constant updates and patches. Recurrent awareness training is carried out to help users identify social engineering attacks like BOT's to help them from being a victim. Frequent penetrating testing can be made using sophisticated software's to access vulnerability. This will contribute to access the application against SQL injections and other forms of web attacks. Frequent updates and patches should be made on the software. Latest information on Trojans, viruses, worms should be circulated to create awareness among the employees. Filtering the network traffic with sophisticated firewalls, content filters, intrusion prevention allows the control of data flows. This will also help in monitoring the data both inwards and outwards. This will be a key point in keeping cyber espionage at bay. Endpoint protection can be applied to all IT devices to protect from viruses and worms. ICS; PLC's, SCADA, are non-standard IT systems. These need to be hardened with the increase in security. This can be done through effective policies, constant upgrade of firmware, etc. Hence it is essential that the lockdown tools can be used in protecting critical infrastructure. While in most cases PLC's, SCADA systems are on the isolated network it is essential to ensure that it has redundancy and failover protection. Authentication using hard coded passwords, public key infrastructure's, biometrics should be used in critical areas or key areas. The passwords, access codes should regularly be changed and should adhere to password policy. Strong passwords should be made mandatory. Since most industrial controlled systems have weak authentication, it needs to be substantiated with other security mechanisms where applicable. Although many industries use virtual private network, it is essential that the traffic in them be monitored to prevent any unwanted attack.

In-depth defense strategies are needed to provide and exercise proper control on ICS devices especially HMI and devices that control the equipment directly including protection and environmental safety. The following Figure 5 provides layers of steps that are interdependent to be put to use. Each of these elements is inter dependent and essential components as a part of the defense against cyber security attack.

Since defense strategies involve various layers, additional security must be built into the core architecture (Figure 6: Pyramid) as a part of design stage rather than as post design scenario that is after implementation. Different areas that need to be focused and concentrated are physical security which is the first stage and the foremost. This layer is the physical layer where all hardware

Table 3: Economics of cyber threat matrix

Agents/adversary	Threats	Motives	Impacts	Challenges	Economic impacts
State sponsored	Business information Technology transfer New or emerging technologies Trade information; secrets	Political Military advantage Economic disruptions	Advantage Disruption of services, delivery of services, Destruction and disruption of critical infrastructure	Grid stability international links) Noncompliance in the form of considering a cyber attack in the design stage The introduction of DER, addition of new resources and infrastructures Human resources challenge there of due to the weakest link in human capital Emergency response team during cyber attacks	Loss in intellectual capital; business opportunity Regulatory fines Liability to borrowing banks and investors Liability to equipment manufacturers Liability to power producers, generators Impact on stocks and shares Insurance claims
Organized crime	Financial systems Personal information Corporate espionage	Financial gain Collect information for future gains	Costly penalties Consumer problems in the form of law suits Financial losses		
Hacktivists	Corporate secrets Personal information Business information	Political influences Pleasure or personal motive in the form of vengeance Patriotism	Disruption of services, delivery of services Brand and reputation losses; Consumer trust and confidence		
Insiders	Energy market strategies; Business and personal information; Intellectual property	Patriotism Professional revenge Monetary gain	Patent violations; Trade disclosure Brand and reputation National security impact		

DER: Distributed energy resources

Table 4: Various elements and potential financial impact

Cyber security vulnerabilities	Risk categorization	Potential financial impact	Other impacts
Generators			
External monitoring and dispatching	Medium	The cost of replacement of broken equipment	Market disruption; national security; human harm; network effects; safety; physical infrastructure damage
Transmission and distribution-grid control systems			
Digital interfaces	High	Investment loss	Control system breach; impact on network infrastructure
SCADA systems	High	Loss in capital; Liability on equipment; borrowing liability	Equipment damage; centrifuges spinning out of control; compromise in safety
Load balancing and controls (voltage, frequency, monitoring)	High	Loss on revenue due to disruptions; investors interests	Grid stability; service disruption; penalties; law suits
Metering			
Smart meters-connections and interfaces	High	Loss of revenue due to incorrect billing; Insurance claims	Meter tampering; sudden power outages
Billing systems			
Consumer interface	High	Insurance claims on damages	Data privacy loss; consumer protection; consumer trust and confidence; law suits
Consumer privacy	High		
Consumer data	High		

SCADA: Supervisory control and data acquisition

Figure 4 - Cyber security strategic areas

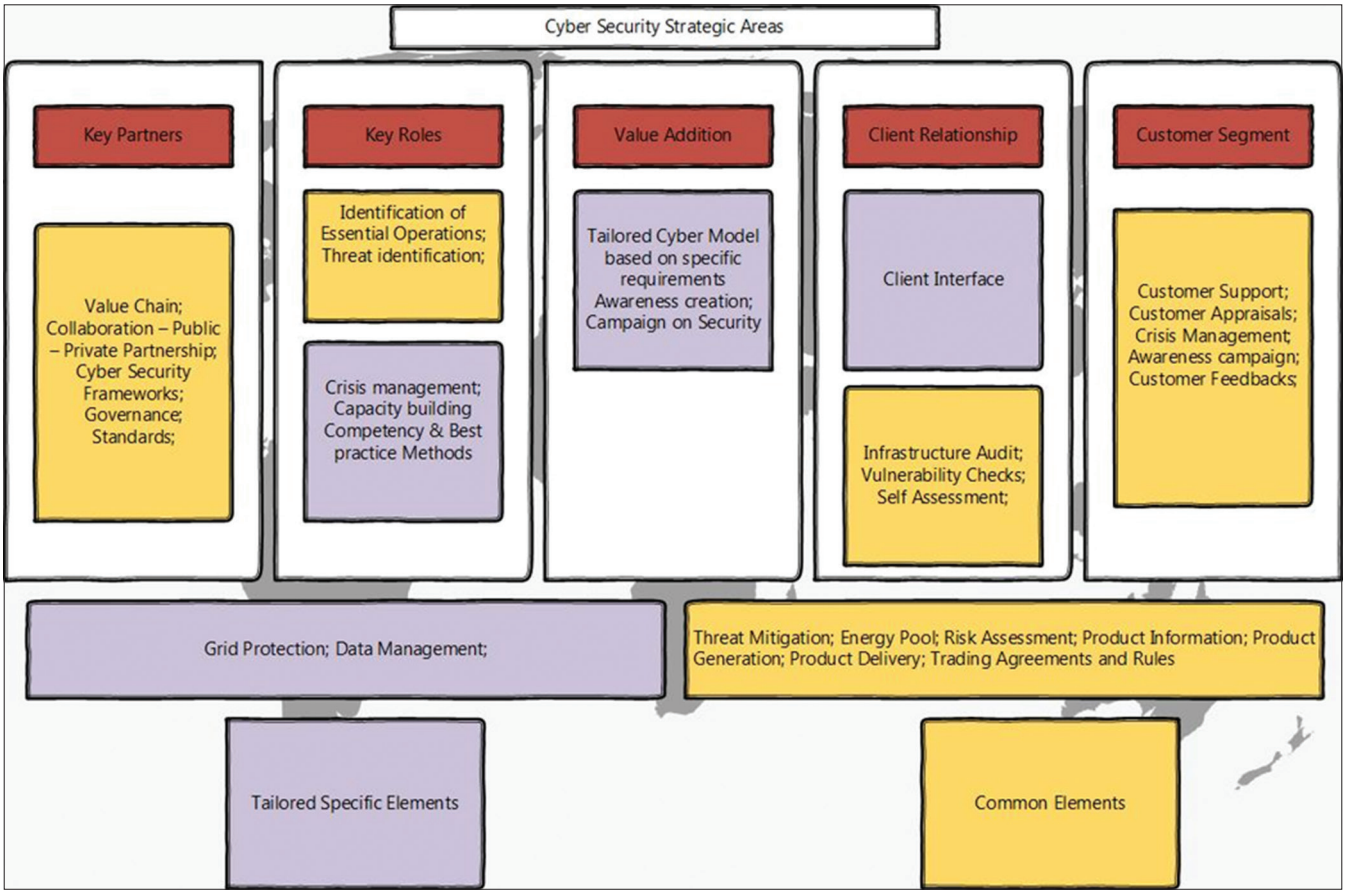
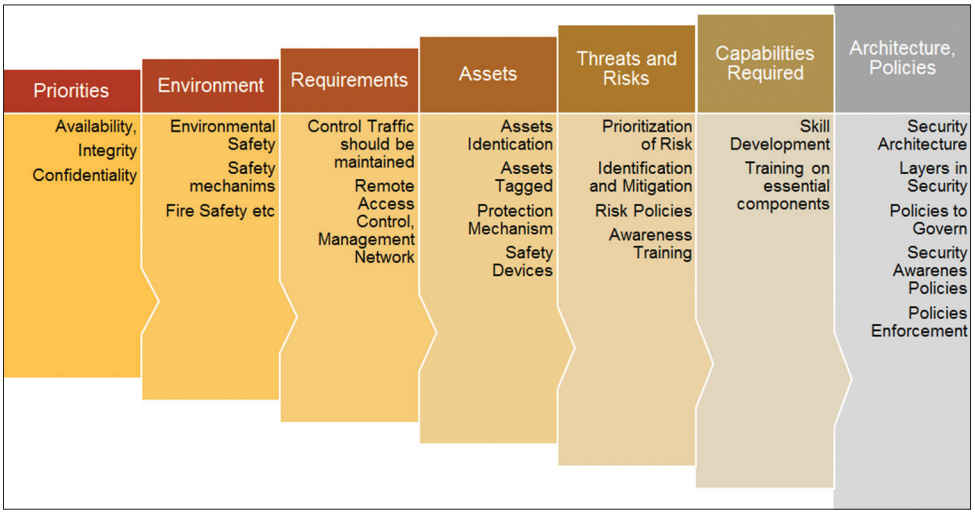
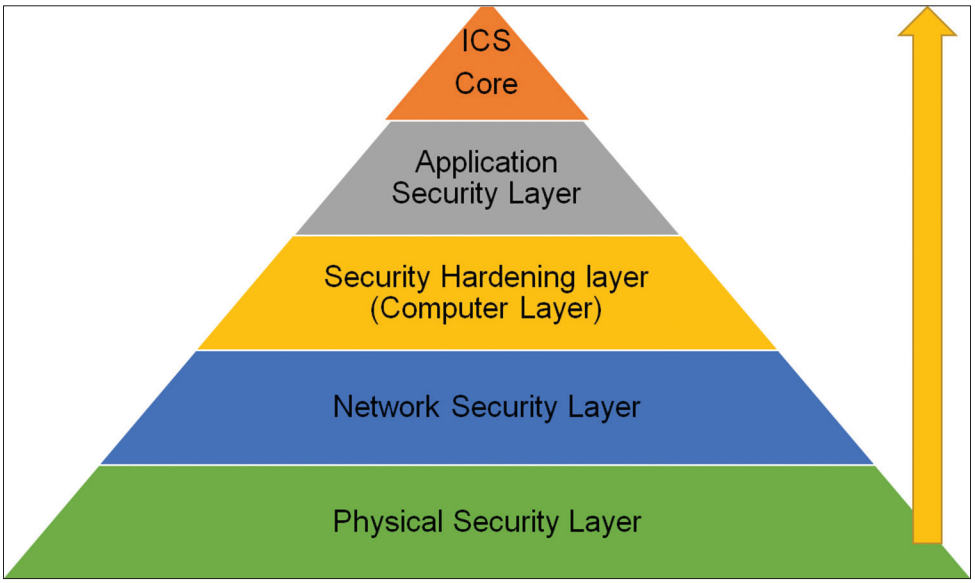


Figure 5 - Defense strategies



devices like panels and areas where CI is put to use. Entry to the facility should be strictly through authentication, and no unauthorized personnel should be allowed. The second layer is the network security layer which involves firewalls, packet tracers, intrusion detection systems, IPS, etc. These equipment should be used in conjunction with proper rugged switches, routers which are used as a part of communication protocol. Frequent analysis should be made on these hardware devices to ensure the functionality and availability of the equipment in case of a cyber-attack. It is also critical to have proper backup and redundant equipment available. The third layer of the security is the hardening layer, which involves, firewall, patch management, virus protection and detection, including administration of the equipment and ensuring that optional components are either switched off or disabling of unused ports, servers, applications controllers. The layer is the application security layer where configuration, management of application access through authentication, authorization, audits, are carried out. Finally, the layer forms the last bit, where the physical ICS reside. The security for this layer involves change control physical and logical access control.

Figure 6 - Defense layers



Human weakness, although varied and different between organizations, run themes across all reported incidents. Many businesses run professional training on best practices for enhancing security, create awareness, provide a safe working environment so that their employee is not the next victim of cyber-attack in the form of social engineering.

4. RESULTS, DISCUSSION, CONCLUSION

Cyber threat, espionage is becoming increasingly common. The threats are real with many actors attempting to gain entry into some of the best practiced and protected systems in the energy sector. Roughly about 4-5 attacks take place on a regular basis in the energy firms with increasingly sophisticated technology with varying degree of threats and tactics. From 2009 to 2017 observations indicate that energy sector has moved up from being low down the top list to become the second most targeted sector. In India, the energy sector is very vulnerable. Most of the energy attacks translate to gathering valuable information rather than being an act of cyber warfare or cyber terrorism. Although the attackers have been focusing on gathering information, with ulterior motives, a day is not far away when these attacks will be to sabotage, leading to huge financial losses crippling the economy or bringing the utility sector to complete standstill. The economic impacts in a small country could translate to many other ripple effects impacting energy firms globally. Energy firms need to be aware of these risks to protect their valuable information as well as their ICS or SCADA networks. The trend of cyber-attacks will get more complicated and will continue increasing as more and more systems get connected on the grid in a distributed model. Protecting these systems from attacks will be key to non-availability, minimize disruptions and losses, minimize downtime, maximize availability and profits while also keeping cyber-attacks at bay. The majority of cyber-attacks can be prevented with constant updates and patches pushed by the vendors, upgrading firmware, etc. The growing inconsistency and lack of specialization have encouraged hackers to exploit the vulnerabilities, and it is noticed that the attacks are not subsiding. This indicates and warrants that valuable lessons be learned from past experiences. It is now time to put a counter offensive in response to a cyber-attack by using and adapting more smart technology devices which must be considered as an integral part of the system rather than an afterthought since the lack of security in smart devices will only worsen the scenario and will have far reaching and damaging effects on the society. In many a case, cyber security is a regulatory compliance issue for many businesses. They need to ensure that they are protected adequately from cyber risks. It is therefore critical for the businesses to know what their obligations, responsibilities are and they need to comply with it. Cyber-attacks and risks should be made a mandate for them to disclose as part of business risks. This may help in assessing how exposed their business is and then what precautionary measures need to be taken to protect their business and their investor's interests.

REFERENCES

Alexander, G. (2017), The Flame: Questions and Answers, Kaspersky Labs, Kaspersky Labs. Available from: https://www.securelist.com/34344/the-flame-questions-and-answers-51. [Last retrieved on 2017 Aug 08].

Alexander, U. (2017), CNN. Available from: http://www.edition.cnn.com/2017/05/14/opinions/wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-urbelis/index.html. [Last retrieved on 2017 Jul 06].

Amar, S. (2016), Spectre of cyberterrorism: A potential threat to India's national security. Indian Journal of Research, 5(3), 1-16.

Anand, K., Krishnan, P., Devendra, K.P. (2014), Facing the reality of cyber threats in the power sector. Energy Policy, 65, 126-133.

Anonymus (sKyWiper Analysis Team). (2012), sKyWIper (a.k.a. Flame a.k.a. Flamer-a complex malware for targeted attacks. Budapest University of Technology and Economics, Department of Telecommunications. Budapest: Laboratory of Cryptography and System Security (CrySyS Lab). Available from: http://www.bme.hu. [Last retrieved on 2017 Nov 06].

Anonymus. (2011), Duqu: Steal Everything, (Kaspersky Labs). Available from: http://www.kaspersky.com/about/press/major_malware_outbreaks/duqu. [Last retrieved on 2017 Sep 05].

Anonymus. (2011), Security Response-W32, Ramnit Analysis, Symantec, Symantec Labs, Symantec. Available from: https://www.symantec.com/security_response. [Last retrieved on 2017 Nov 06].

Anonymus. (2011), W32.DuQu-The Precursor to the Next StuxNet, Symantec Response, Symantec Labs. Available from: https://www.symantec.com/security_response. [Last retrieved on 2017 Jun 09].

Anonymus. (2012), Aramco Says Cyberattack Was Aimed at Production, (The New York Times). Available from: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html. [Last retrieved on 2017 Dec 06].

Anonymus. (2014), Energy Firms Hacked by Cyber-Espionage Group Dragonfly, BBC News, BBC. Available from: http://www.bbc.com/news/technology-28106478. [Last retrieved on 2017 Sep 06].

Anonymus. (2014), Security Response-Dragonfly: Cyberespionage Attacks Against Energy Suppliers, Symantec Labs, Symantec Labs. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf. [Last retrieved on 2017 Nov 06].

Anonymus. (2015), The DuQu 2.0 Technical Details-The Mystry of DuQu 2.0-Sophisticated Cyber Espionage Actor, Kaspersky Labs, Reserach Labs, Kaspersky Labs.

Anonymus. (2017), Shamoon: Multi-Staged Destructive Attacks Limited to Specific Targets, (Symantec Labs). Available from: https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets. [Last retrieved on 2017 Aug 06].

Anonymus. (n.d.), Available from: https://www.en.wikipedia.org/wiki/Duqu. [Last retrieved on 2017 Jun 08].

Benahmed, K., Smahi, A. (2016), Security concerns in smart grids: Threats vulnerabilities and countermeasures. In: Renewable and Sustainable Energy Conference (IRSEC), 2015 3rd International. Marrakech, Morocco: IEEE. p1-6.

Boldizsár, B., Gábor, P., Levente, B., Márk, F. (2011), Duqu: A Stuxnet-Like Malware Found in the Wild, Budapest University of Technology and Economics, Department of Telecommunications. Budapest, Hunguary: Laboratory of Cryptography and System Security (CrySyS). Available from: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. [Last retrieved on 2017 Nov 06].

Boldizśar, B., Ǵabor, P., Levente, B., Ḿark, F. (2012). The cousins of stuxnet: Duqu, flame, and gauss. Future Internet, MDPI, 4(4), 971-1003.

Brian, C., William, D.J., Mark, J., Baird, W. (2004), The Economic Impact of Cyber-Attacks, CRS: Congressional Research Service, Government and Finance Division, CRS Report for Congress: The Library of Congress. Available from: https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf. [Last retrieved on 2017 Dec 08].

Bryan, W. (2014), Impact of Cyber Attacks on the Private Sector. MidPoint Group.

Candid, W. (2014), Targeted Attacks Against the Energy Sector, Security Response. Mountain View, CA: Symantec Labs.

Carlos, C., Diwakar, D., Paula, G., Suriya, N., François, P., Eric P, Arun P, Avelino R, Craig S, Rakesh S, Rick S, Dan S, Bing S, Chong X. (2015), McAfee Annual Lab Reports. McAfee Labs, McAfee.

Charles, B., Justin, B., Chris, B. (2014), Market Review 2014: Cyber-Attacks Can the Market Respond, Willis. Available from: http://www.docplayer.net/785007-Energy-market-review-2014-cyber-attacks.html. [Last retrieved on 2017 Jun 08].

CIP Center for Infrastructure Protection. (2003), Blackout: A Case of Study of the 2003 North American Blackout with Exercice. Available from: http://www.cip.gmu.edu/wpcontent/uploads/2013/10/blackout-learner-version.pdf.

Col, S.S.R. (n.d.), Cyber Secuiry in India's Counter Terrorism Strategy. Available from: http://www.ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf. [Last retrieved on 2017 Jun 08].

Damien, M., Christopher, W. (2012), Flame: World's Most Complex Computer Virus Exposed, (The Telegraph). Available from: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html. [Last retrieved on 2017 Dec 06].

Daniel, W., Bailey, S. (2016), The Growing Threat of Cyber-Attacks on Critical Infrastructure, (Huffington Post). Available from: http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html. [Last retrieved on 2017 Jun 15].

David, H., Sacha, M., Usen, A., Edward, C. (2016), Cyber Security Strategy for the Energy Sector. Industry Research and Energy, Policy Department, Directorate General of Internal Policies. Brussels: Eurpoean Union. Available from: http://www.europarl.europa.eu/studies.

David, K. (2013), The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program, (I. Specturm, Producer). Available from: http://www.spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. [Last retrieved on 2017 Jun 08].

David, M., Vern, P., Stefan, S., Colleen, S., Stuart, S., Nicholas, W. (n.d.), The Spread of the Sapphire/Slammer Worm. Available from: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html#2. [Last retrieved on 2017 Dec 06].

David, M., Vern, P., Stefan, S., Colleen, S., Stuart, S., Nicholas, W. (2003), Inside the slammer worm. In: IEEE Computer and Security, 1540-7993, 1-7. Available from: http://www.cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf. [Last retrieved on 2017 Jun 15].

David. (2014), Havex Hunts For ICS/SCADA Systems, (F-Secure Labs). Available from: https://www.f-secure.com/weblog/archives/00002718.html. [Last retrieved on 2017 Jul 15].

Elinor, M. (2009), Report: Hackers Have Broken Into the Air Traffic Control Mission-Support Systems of the U.S. Federal Aviation Administration Several Times in Recent Years, (ZDNet). Available from: http://www.zdnet.com/news/report-us-airtraffic-control-systems-hacked/300164. [Last retrieved on 2017 Dec 06].

Ellen, N., Greg, M., Julie, T. (2017), U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say, (Washington Post). Available from: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. [Last retrieved on 2017 Dec 06].

Ellen, N., Joby, W. (2012), Stuxnet was Work of U.S. and Israeli Experts, Officials Say, (Washington Post). Available from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. [Last retrieved on 2017 Dec 06].

Goodin, D. (2012), Discovery of New "Zero-Day" Exploit Links Developers of Stuxnet, Flame, (Arstechnica). Available from: https://www.arstechnica.com/security/2012/06/zero-day-exploit-links-stuxnet-flame. [Last retrieved on 2017 Dec 06].

Hanouz, M.D. (2016), Understanding Systemic Cyber Risk-Global Agenda Council on Risk and Resilience, World Economic Forum. Available from: https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk. [Last retrieved on 2017 Sep 06].

ICS-CERT. (2014), Year in Review, NCCIC, NCCIC. US: Homeland Security. Available from: https://ics-cert.us-cert.gov/sites/default/files/.../Year_in_Review_FY2014_Final.pdf. [Last retrieved on

2017 Aug 08].
ICS-CERT. (2015), Year in Review, NCCIC, NCCIC. US: Homeland Security. Available from: https://ics-cert.us-cert.gov/sites/default/files/.../Year_in_Review_FY2015_Final.pdf. [Last retrieved on 2017 Aug 08].
ICS-CERT. (2016), Year in Review, NCCIC, NCCIC. USA: Homeland Security. Available from: https://www.ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf. [Last retrieved on 2017 Aug 08].
Iran Admits Nuclear Sites Hit by 'Duqu' Cyber Weapon. (2011), (FoxNews). Available from: http://www.foxnews.com/tech/2011/11/14/iran-admits-nuclear-sites-hit-by-duqu-cyberweapon.html. [Last retrieved on 2017 Dec 06].
James, L. (2002), Assessing the Risks of Cybertwrrorism, Cyber War, and Other Cyber Threats. Washington DC: Center for Strategic and International Studies.
Joel, T.L. (2014), Defending Against the Dragonfly Cyber Security Attacks, BELDEN. Available from: http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf. [Last retrieved on 2017 Sep 06].
Kevin, P. (2003), Slammer Worm Crashed Ohio Nuke Plant Network, (Security Focus). Available from: http://www.securityfocus.com/news/6767. [Last retrieved on 2017 Dec 06].
Kim, Z. (2011), Son of Stuxnet Found in the Wild on Systems in Europe. Available from: https://www.wired.com/2011/10/son-of-stuxnet-in-the-wild. [Last retrieved on 2017 Sep 06].
KPMG Global Research Institute. (2013), Energy at Risk, KPMG. Available from: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/energy-at-risk.pdf.
Lemieux, F. (2011), Investigating Cyber Security Threats, Exploring National Security and Law Enforcement Perspectives, Cyber Security Policy and Research Institute, George Washington University.
Leyden, J. (2012), Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits-First Hacktivist-Style Assault to Use Malware? (The Register). Available from: http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis. [Last retrieved on 2017 Dec 06].
Loney, M. (2003), SQL Slammer Worm Wreaks Havoc on Internet, (ZDnet). Available from: http://www.zdnet.com/article/sql-slammer-worm-wreaks-havoc-on-internet. [Last retrieved on 2017 Jun 06].
Marsh, R. (2015), Hackers Successfully Ground 1,400 Passengers, (CNN). Available from: http://www.edition.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/index.html. [Last retrieved on 2017 Dec 06].
Martin, G.M. (2004), Prioritizing cyber vulnerabilities. Homeland Secuirty, National Infrastructure Advisory Council. US: Homeland Security. Available from: https://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf. [Last retrieved on 2017 Aug 08].
Marwan, A. (2017), Cyber attacks and terrorism: A twenty-first century conundrum. (Springer, Edition) Science and Engineering Ethics, 1, 1-14.
Murchu, L.O. (2011), Stux Net Modus Operandi, Symantec, Symantec Security Response, Symantec. Available from: https://www.sans.org/summit-archives/file/summit_archive_1493844778.pdf. [Last retrieved on 2017 Nov 06].
Naraine, R. (2010), Stuxnet Attackers used 4 Windows Zero-Day Exploits, (ZDNet). Available from: http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347. [Last retrieved on 2017 Dec 06].
Nell, N. (2016), The Impact of Dragonfly Malware on Industrial Control Systems, SANS Institute, SANS Institute InfoSec Reading Room, SANS. Available from: https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672. [Last retrieved on 2017 Jun 06].
Nicolas, F.L.O. (2011), Symantic Response-W32, Stuxnet Dossier, Symantec Labs, Symantec. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
Oxana, A., Sergey, G., Gleb, G., Olga, K., Evgeniya, P., Sergey, I.S., Alexander, A.T. (2015), Industrial Control Systems Vulnerabilities Statistics, Kaspersky, Kaspersky Labs, Kaspersky.
Perlroth, N. (2012), Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, (The New York Times). Available from: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html. [Last retrieved on 2017 Dec 06].
Ponemon Institute, LLC. (2011), State of IT Security: Study of Utilities and Energy Companies, Ponemon Institute, LLC. Available from: http://www.ponemon.org/local/upload/file/Q1_Labs%20_WP_FINAL_3.pdf.
Ponemon Rept. (2015), Cost of Cyber Crime Study, Ponemon Institute LLC, Ponemon Institute Research Report. USA: Ponemon Institute in Collaboration with HP.
Ponemon Rept. (2016), Ponemon Institute Research Report: 2016 Cost of Cyber Crime Study and Risk of Business Innovation, Ponemon Institute LLC, Ponemon Institute LLC in Colloboration with HP. USA: Ponemon Institute LLC. Available from: https://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation. [Last retrieved on 2017 Aug 08].
Poulsen, K. (2004), South Pole 'Cyberterrorist' Hack wasn't the Firstm, (The Register). Available from: http://www.theregister.co.uk/2004/08/19/south_pole_hack. [Last retrieved on 2017 Dec 06].
Raj, S.C.W. (2017), Is Wanna Cry Really Ransomware? Available from: https://www.securingtomorrow.mcafee.com/executive-perspectives/wannacry-really-ransomware/?ito=446. [Last retrieved on 2017 Aug 06].
Ralph, L. (2013), To Kill a Centrifuge-Technical Analysis of What Stuxnet's Creators Tried to Achieve. Munich: The Langer Group. Available from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf. [Last retrieved on 2017 Nov 06].
Rhidi, K. (n.d.), Fronteranews. Available from: https://www.fronteranews.com/news/global-macro/1-the-10-countries-most-affected-by-the-wannacry-malware-attack. [Last retrieved on 2017 Jul 06].
Robert, M.L., Michael, J.A., Tim, C. (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case. Washington, DC: SANS. Available from: https://www.ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. [Last retrieved on 2017 Aug 05].
Roberts, P. (2003), Blaster Worm Spreading; Experts Warn of Attack, (Computer World). Available from: http://www.computerworld.com/article/2571072/malware-vulnerabilities/blaster-worm-spreading--experts-warn-of-attack.html. [Last retrieved on 2017 Jun 15].
Sanger, D.E. (2012), Obama Order Sped Up Wave of Cyberattacks Against Iran. (The Newyork Times). Available from: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. [Last retrieved on 2017 Dec 06].
Security Response Team. (2014), Security Response-Dragonfly: Cyberespionage Attacks Against Energy Suppliers, Symantec Labs, Symantec Labs. Available from: ???. [Last retrieved on 2017 Nov 06].
SenseCy. (2014), Tag: Energy Sector: Cyber Threats to Oil and Gas Industry. Available from: https://www.blog.sensecy.com/tag/energy-sector. [Last retrieved on 2017 Aug 08].
Siobhan, G. (2009), FAA's air-traffic networks breached by hackers. The Wall Street Journal. Available from: http://www.online.wsj.com/articles/SB124165272826193727. [Last retrieved on 2017 Dec 06].

Siobhan, G. (2012), China Hackers Suspected in Long-Term Nortel Breach, Wall Street. Available from: https://www.wsj.com/articles/SB10001424052970203363504577187502201577054. [Last retrieved on 2017 Mar 03].

Staff Correspondent. (2014), Centre to Shield India from Cyber Attacks Proposed. New Delhi: The Hindustan Times.

Tarja, R., Martti, L. (2017), Cyber Threats Mega Trends in Cyber Space, International Conference on Cyber Warfare and Security. p323.

Thomson, L. (2013), Snowden: US and Israel Did Create Stuxnet Attack Code, (The Register). Available from: http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet. [Last retrieved on 2017 Dec 06].

Vaidya, T. (2015), 2001-2013: Survey and Analysis of Major Cyberattacks, Cornell University Library, Computers and Society (Computers and Society (cs.CY); Cryptography and Security (cs.CR), Cornell University. Available from: https://www.security.cs.georgetown.edu/~tavish/cyberattacks_report.pdf.

Venere, G., Szor, P. (2011), The Day of the Golden Jackal-The Next Tale in the Stuxnet Files: Duqu, McAfee. Available from: https://securingtomorrow.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files/. [Last retrieved on 2017 Sep 06].

Vish, N. (2017), Available from: http://www.vishnandlall.org. [Last retrieved on 2017 Jun 08].