A COMPARATIVE STUDY OF CYBER SECURITY POLICIES

A MASTER'S THESIS

In

The Department Of Information Systems Engineering

Atilim University

By

HAITHEM ABD ESHARF BDERI

JUNE 2017

A COMPARATIVE STUDY OF CYBER SECURITY POLICIES

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OF

ATILIM UNIVERSITY

BY

HAITHEM ABD ESHARF BDERI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER

IN

THE DEPARTMENT OF INFORMATION SYSTEMS ENGIEERING

JUNE 2017

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

_____

(Prof. Dr. Ibrahim Akman)

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

(Assoc. Prof. Dr. Korhan Levent Ertürk)

Head of Department

This is to certify that we have read the thesis "Thesis Name" submitted by "Candidates Name" and that in ouropinion it is fully adequate, in scope and quality, as a thesis forthe degree of Master of Science.

_____

(Prof. Dr. Alok Mishra)

Supervisor

Examining Committee Members

Prof. Dr. Alok Mishra _____

Atilim University-Software Engineering Department

Asst. Prof. Dr. Yavuz İnal _____

Atilim University-Information System Engineering Department

Asst. Prof. Dr. Ahmet Murat özbayoğlu _____

TOBB ETÜ University-Computer Engineering Department

Date (June 2017,29)

ABSTRACT

A COMPARATIVE STUDY OF CYBER SECURITY POLICIES

Bderi,Haithem ABD Esharf

M.S., Information Systems Engineering

Supervisor Prof. Dr. Alok Mishra

June 2017, 109

The cyberspace is expanding faster than ever and with it cyber threats are also increasing making it imperative to have a strong cyber-security policy. Cyber-attacks don't only affect individual users and organization but can also cause national security issues. The different policies of different countries make it possible for hackers and intruders to carry cyber-attack while making it impossible for authorities to trace back offenders. It is important to develop a comprehensive Cyber-security policy to address all kinds of cyber threats so that every offender can be traced back and penalized accordingly. This research work examines and compares different attributes of cyber-security policies of selected countries. This research work identifies some important attributes which can help to develop an all-inclusive cyber-security policy.

Keywords cyber-security , cyber-security , cyber-security policy, cyberspace, comparative study, cyber-security law, network security, cyber threats, cyber-attack,

ÖZ

CYBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRMALI ARAŞTIRMASI

Bderi,Haithem ABD Esharf

Yüksek Lisans,Bilişim Sistemleri Mühendisliği

Tez Yöneticisi Prof, DR Alok Mishra

Haziran,2017, 109 Pages

Siber alan her zamankinden daha hızlı genişliyor ve bununla birlikte siber tehditler artmakta ve güçlü bir siber güvenlik politikası zorunluluğu bulunmaktadır. Siber saldırılar yalnızca bireysel kullanıcıları ve kuruluşları etkilemekle kalmaz, aynı zamanda ulusal güvenlik sorunlarına da neden olabilir. Farklı ülkelerin farklı politikaları, bilgisayar korsanlarının ve davetsiz misafirlerinin, yetkililerin suçluları takip etmesini imkansız hale getirirken siber saldırı düzenlemelerini mümkün kılıyor. Her türlü suçlunun takip edilebileceği ve buna göre cezalandırılabilmesi için her türlü siber tehdide yönelten kapsamlı bir siber güvenlik politikası geliştirmek önemlidir. Bu araştırma çalışması, seçilen ülkelerin siber güvenlik politikalarının farklı niteliklerini inceler ve karşılaştırır. Bu araştırma çalışması, her şey dahil bir siber güvenlik politikası geliştirmeye yardımcı olabilecek bazı önemli nitelikleri tanımlar.

Anahtar kelimeler siber güvenlik, sibergüvenlik, sibergüvenlik politikası, siberalan, karşılaştırmalı incelemesi, sibergüvenlik yasası, ağ güvenliği, siber tehditler, siber saldırı,

To my Parent

ACKNOWLEDGMENTS

I would first like to thank my thesis supervisor Prof. Dr. Alok Mishra of the Software Engineering Department at Atilim University, and I would like to thank the my examining committee members Asst. Prof. Dr. Yavuz İnal of the Atilim University-Information system Engineering Department and Asst. Prof. Dr. Ahmet Murat Özbayoğlu of the TOBB ETÜ University-Computer Engineering Department , for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

APRA	Australian Prudential Regulatory Authority
BIC	Bank Identifier Code
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CASL	Canada's Anti-Spam Legislation
CCA	Controller of Certifying Authorities
CISP	Cyber Information Sharing Partnership
CMA	Communications and Multimedia Act
CNCI	Comprehensive National Cyber-security Initiative
CNII	Critical National Information Infrastructure
CPA	Consumer Protection Act
CRPL	Consumer Rights Protection Law
CSIRT	Computer Security Incident Response Teams
CSIS	Canada's Signals Intelligence Agency
CSI	Container Security Initiative
DAE	Digital Agenda for Europe
DSS	Data Security Standard
EC	European Commission
EC_3	European Cybercrime Centre
EISA	Energy Independence and Security Act
ESIGN	Electronic Signature in Global and National Commerce Act

ETA	Electronic Transactions Act
EU	European Union
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FISS	Fraud Intelligence Sharing System
GDP	Gross Domestic Product
HIPAA	Health Insurance Portability and Accountability Act
IASP	Internet Access Service Provider
ICT	Information and Communication Technology
IEEE	The Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centers
IT	Information Technology
NCIPC	National Critical Information Protection Centre
NCSP	National Cyber-security Policy
NCSS	National Cyber-security Strategy
NIS	Network and Information Security
NITRD	The Networking and Information Technology Research and Development
NSW	New South Wales
NT	Northern Territory
PCI	Payment Card Industry
PDP	Personal Data Protection
PDP	Personal Data Protection

PIPEDA	Personal Information Protection & Electronic Documents Act
PPP	public–private partnership
R&D	Research and Development
SAFE	Security and Freedom through Encryption
SERC	The State Electricity Regulatory Commission
SET	Secure Electronic Transaction
SSL	Secure Sockets Layer
UECA	Uniform Electronic Commerce Act
UETA	Uniform Electronic Transactions Act
UK	United Kingdom
UN	United Nations
USA	United States of America

CHAPTER 1

1. INTRODCTİON

We are living in the era of globalization which is basically the world of computers. The digital sector has become a vital part of almost every society. This virtual world of computers is known as cyberspace. The data floating around the network in computers is known as an object in cyberspace. Cyberspace has become an important part of one's daily life due to the fast commonness of smart devices and internet. From the past two decades, information technology has played a vital role in productivity growth and modern power. Nowadays the productive use of ICT tools and adequate responding to technological trends has been considered as hallmarks of a modern developed society. In few years, utilization of cyberspace will be a critical factor in national competitiveness. The basic consumers or actors of cyberspace are citizens, businesses and government bodies. The digital domain is an important part of almost all spheres of life like for communication, transactions, entertainment, and collaboration. The increasing trend of digitalization is not only important for the comfort and recreational activities but also requisite for economic growth.

The increasing trend of digitalization and excessive reliance on cyberspace by the countries has given ground to cyber threats. Cyber threat refers to actors who exploit cyberspace in order to corrode life, property, operations, information. As the states have

become more dependent on the cyberspace, so it has become a magnetic force to attract all adversary types (Cohen et al., 1999). Reasons of cyber threats cannot be only revolutionary but also gathering intelligence, harm the country's sovereignty, ideological grounds or crime (Anderson, 2012). Sources of cyber threats can be terrorists, thieves, state enemies or organized inside criminals. So cyber threats can be of national and international nature. Regardless the nature of cyber threats, timely and appropriate addressing to the threats is requisite.

The process to secure the information and communications from damage, alteration or use by the unauthorized entity is known as a cyber-security. Cyber-security involves multiple strategies, policies and operations to reduce threats and vulnerability. Electronic assets are the main targets of any cyber threat. Cyber threats affect the ability of the state to achieve its objectives and perform core functions. In this information-driven economic era, security lapse can result in long-term damage to a country's economy and sovereignty as well. Firewalls and anti-virus software are no longer sufficient enough for cyber-security. A broad spectrum approach of cyber-security system across the country, in its network and whole ecosystem is required. Adequate legislature regarding cyber-security and proper implementation of the policy can achieve the broad spectrum approach.

1.1. Need of Cyber-security Policy

As cyber threats are evoking at a fast pace, so digital security is requisite for the proper functioning of any country in the cyberspace. In the era of globalization, ICTs and the internet are requisite to form a solid infrastructure, economic and social developments of a country. For proper functioning all the consumers including government bodies, citizens and business are reliant on digital infrastructure. So a proper and secure digital infrastructure is the need of the hour for every country. When the use of the internet was lesser, the risks and consequences of failures were manageable by few laws at organizational and country level. But due to the critical dependence of the modern economy on the internet, comprehensive approach to cyber-security is vital, which is only possible by proper development and implementation of cyber-security

strategies at national and international level. There is an evolution in government policy making as cyber-security has been prioritized in it.

Almost all the cyber-security policies are the result of rising in information age due to which information technology has gained a central position in all sectors of society, from the life of a citizen to businessman and government. In this era of post-industrial society, information technology has gained the most important, accessible and persuasive position. The whole society is becoming overwhelmingly dependent on the information technology (Petr et al., 2015).

Day by day the potential damage due to cyber-attacks is becoming larger. The greatest cyber threat is the targeting of country's infrastructure assets including telecommunications, defense, power, and transportation. And these cyber-attacks are damaging the economy. The most common and the disruptive cyber-attacks are on critical infrastructures (Geers, 2009). A secure cyberspace is the desire of almost all countries due to the increasing rates of espionage, destruction of critical information and malicious cyber-activity (Bayuk et al., 2012).

Researchers declare that cyber arms race has already begun. Some major powers of the World like the United States and China have prioritized the development of offensive cyber capabilities in their strategic doctrines (Green and Rowe 2015). To protect its military and defense networks, United States has developed its Cyber Command (Glenny, 2011). Generally, cyber threat's seriousness and cyber capabilities development have never been addressed properly at theglobal level.

The main hurdle to developing a global agreement regarding cyber-security is the lack of widely accepted and clear definition of cyber threats. It is still unclear that cyber threats come under Article 51 (Aggression Clause) of UN Charter or under Article 5 (Solidarity Clause) of UN treaty (Zanders, 2009). In the domain of defense, if Cyberspace is at the fifth place after land, sea, air, and space, then it requires physical response just like other kinetic attacks Policymakers, government officials and the professionals are the dominating characters for the development of Cyber-security Policy of the country.

Due to the elevating graph of cyber threats, there is a great chance and in fact in the near future, to have a Universal agreement regarding the need to respond to these cyber threats.

1.2. Analysis of the Countries 'Cyber-security Policy'

It is very time consuming and hectic task to study the cyber-security policy of all countries in the world. To complete the research in time and with available resources seven countries including USA, EU, Canada, Australia, China, India, and Malaysia are selected for the comparative study of their cyber-security policies. The methodology used for the selection of these countries are discussed in chapter four in detail. Fifteen comparators are selected for the comparison. These comparators encompass almost every aspect of cyber-security the methodology for the selection of these comparators are discussed in chapter four in detail.

Comparators	**USA**	**EU**	**Malaysia**	**Australia**	**China**	**Canada**	**India**
Reasons for developing Cyber-security policy	Critical Infrastructure Protection	Cyber Threats	Critical Infrastructure Protection	Development of E-commerce	Critical Infrastructure Protection	Critical Infrastructure Protection	Critical Infrastructure Protection
Actors	Espionage Cybercrime Cyberthreats	Espionage Cybercrime Cyberthreats	Cybercrime	Espionage Cybercrime Cyberthreats	Espionage Cybercrime Cyberthreats	Espionage Cybercrime Cyberthreats	Espionage Cybercrime Cyberthreats
Priority in Government	Included in major infrastructure	In top ten	In top ten	In top ten	Highest Priority	In top seven	In top three
Current Interference Degree	Voluntary self-regulatory	Voluntary self-regulatory	Voluntary self-regulatory	Voluntary self-regulatory	Enforced self-regulatory	Voluntary self-regulatory	Voluntary self-regulatory and strategi

							c
Suggested Interference Degree	Enforced self-regulatory	Enforced self-regulatory	Enforced self-regulatory	Enforced self-regulatory	Enforced self-regulatory	Enforced self-regulatory	Enforced self-regulatory
Implemented in	2008	2013	2006	2009	2016	2011	2013
Cyber Force	Proposed	No	No	No	Yes	No	Proposed
Cyber-security Policy is Fully specified and Implemented	Not yet, few laws are overlapping	Fully specified and implemented	Fully specified and implemented	Fully specified and implemented	Implemented but in the process of major developments	Fully specified and implemented	Fully specified and implemented
Providing Open and Secure Cyberspace	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intelligence Agencies at front end (helping to address Cyber threats)	Yes	Yes	No	Yes	Yes	Yes	Yes

Table 1 Similarities and differences in the cyber-security policies of the comparators are summarized above in tabular form and elaborated as follows

Cyber-security Policy of USA

USA current cyber-security policy is the up-gradation of Comprehensive National Cyber-security Initiative (CNCI) which was implemented in 2008 by President Bush. The current government of Obama prioritized cyber-security policy at the top of government's agenda and implemented Cyberspace Policy Review (CPR) in 2009. There is ten short term and fourteen midterms suggested tasks in CPR. US government had taken 9.11 as momentum and upgraded the cyber threat by including major infrastructure in it and started dealing with it as a national security issue. In February the president signed Critical Infrastructure Cyber-security which focused on the development and implementation of the framework for the reduction of cyber risk and formation of critical cyber-security infrastructure with stakeholders. USA government interference with respect to public-private partnership and cyber-security policy is of voluntary self-regulation degree. Few parts of cyber-security law are overlapped by other laws so it's not yet fully specified. US government is trying to change the degree of intervention from voluntary to enforced Self-regulation (FAS, 2010).

Cyber-security Policy of EU

European Commission (EC) in 2013 presented a cyberspace of open, secure and safe nature. It was based on cyber-security strategy of 2010 (DAE Digital Agenda for Europe). DAE was made up of 101 action plans out of which 13 were related cyber-security. Cyber-security strategy of EU presents 5 basic action plans and stakeholders have to carry out these plans. Network and Information Security (NIS) was suggested to protect information security and for regulation of online stability as per EU's standards. More EU government intervention is suggested as existing voluntary system has not properly responded to the cyber threats. It is expected that EU will change its way from voluntary to enforced Self-regulation (Bendiek, 2012).

Cyber-security Policy of Malaysia

In 1991 Malaysian Prime Minister launched Vision 2020, the main aim of which was to use information technology as a tool for the development of the country. The increasing dependence on digital information has escalated the growth of cyber threats which are endangering the sovereignty of the country. The study to address cyber threats was conducted in 2005 at the national level in collaboration with government officials. The main objectives of the study were an assessment of current cyber risk situations, protection of critical infrastructure and development of an action plan to implement cyber-security strategies. The conclusion of the study was accepted and resulted in the implementation of National Cyber-security Policy (NCSP) on May 31st, 2006. The policy focused on 8 major areas of effective governance, Legislative framework, Cyber-security technology framework, culture Security, R & D towards self-reliance, compliance and enforcement, cyber-security readiness and international cooperation (Hashim, Malaysia's, 2011).

Cyber-security Policy of Australia

Australian government believes that Cyber-security of Australia can be advanced by the national partnership of government, businesses and research communities. Networks of Australia hardly compromise on cyber-attacks that are why open and secure cyberspace is provided by Australia. Australian economy grows through cyber-security innovation. The priority actions of Australian Cyber-security Policy are co-leadership, building strong leadership, detect, deter and respond to cyber threats, to build capacity against malicious cyber activities, to enable cyber-security innovation, research and development. Cyber-security Architecture of the Australian government is made up of special policy adviser on cyber-security, cyber ambassador for international engagement and Australian Cyber-security Center Coordinator for operations (Scully, 2016).

Cyber-security Policy of China

Cyber-security of China is an outcome of several years of study of cyber threats and issues. A new military force was announced and confirmed by Central Military Council of China on January 1st, 2016 the core purpose of which is to handle digital battleground in a technical manner, the name of the new military branch is Strategic Support Force. It has aimed to provide resources to protect China's cyber and space security. There are three drivers in Chinese cyber-security policy Political, Military and Economic. The main objectives of Chinese Cyber policy are To maintain economic growth, to protect the Chinese Communist party's governing power, to ensure military superiority in cyberspace, to advance in alternatives of government handling of cyber-security and to empower China and signal dissatisfaction to developments outside China. Impressive improvements have been made in last two decades in Cyber capabilities of China to strengthen military machine (Ahlgren et al., 2005).

Cyber-security Policy of Canada

The government of Canada has rated cyber-security threats among top seven threats to the country. Terrorists, cybercriminals, and military are characterized as actors in cyber-security by the Canadian government. Cyber-security framework of Canada is similar to Australia, USA, UK and New Zealand with respect to the fact that intelligence agencies are at the front end in the developmental approach. Cyber-security strategy of Canada states that espionage and cybercrime are the utmost priorities in the cyber domain (Freeze, 2012). The cyber-security strategy of Canada is built on three main pillars Government systems security, vital cyber systems security (outside of the federal government) and digital security for Canadians. The responsibility of monitoring and taking action on cybercrime comes in the responsibility of Royal Canadian Mounted Police which works in collaboration with (CSIS) Canada's Signals Intelligence Agency (Black, 2012).

Cyber-security Policy of India

Ministry of Communication and IT of Indian government released the National Security Policy in 2013. The core purpose was to protect the confidential information and sovereignty of the country. The Indian government suggested building National Critical Information Protection Centre (NCIPC) which will act as a control room to eliminate cyber-security threats from nuclear, space and air control. The policy also proposed to have a workforce of 50,000 who will be well trained in cyber-security. The main features of the policy are To build a secure cyberspace, to reduce vulnerabilities to cyber threats, to enhance cooperation among all stakeholders within the country, strategic approach in support to national cyber-security policy, monitor cyber-security compliance and threats at national level and cooperation for cyber-security actions among government and public-private partnerships (Kumar, 2016).

1.3. Research Outline

1.3.1. Research Questions

Comparative analysis of Cyber-security Policies of Malaysia, Australia, USA, China, Canada, India, and EU has been done and other than depicting the common findings of the cyber-security policy of the countries, the research will also address the following questions

What are the basic types of threats within the cyber-security threat scenario for each country?

Like threat actor's typology, motivational capabilities, response to countermeasures, for instance, the way China has framed its Cyber-security policy.

Which organizations have the lead role in the cyber-security policy of each country?

What role is played by the law enforcement organization in the implementation of the cyber-security policy of the mentioned countries?

How is the prioritization of the cyber threats done by each country?

For instance, as per Strategic Defense and Security Review, 2010 of UK, cyber is the highest priority threat.

1.3.2. Research aims and objectives

The aim of the research study is to seek information that how the cyber threats are characterized by the selected states, and how the cyber-security policies of these states address the current cyber threats. Experts suggest publishing strategies and action plans for cyber-security for the development of a cyber-security system of the country (Hamilton and Booz, 2012). A comparison study of cyber-security policies of USA, EU, China, India, Australia, Canada, and Malaysia will be done and common findings in cyber-security policies of the countries will be elaborated.

The objectives of the research study are as follows

- To provide an overview of main cyber threats faced by the countries.
- To provide an overview of the cyber-security capabilities of the countries.
- To compare the common findings in cyber-security policies of the countries.
- To find the level of cooperation among the organizations/ departments in order to address the remaining challenges of the countries.

1.3.3. Research Methods

The methodology is a process to collect data and information. The methodology enables researchers to organize and channelize their efforts to complete research work (Scapens, 2011). The information is gathered through literature study method. It utilizes all available literature such as articles, journals, and documents which have the information related to the above-mentioned research questions. There are three categories of literature study methodology including explanatory, descriptive and exploratory. Exploratory research methodology is used to get the answer of those questions which involve “what” and who. On the other hand, explanatory methodology gives the answer of “how” and “why”. The descriptive methodology uses to analyze and describe a phenomena or sequence of events. The combination of these categories will be used in this research to compare cyber-security policies. There are several benefits of literature study methodology. It helps to collect data and investigate it within the context of research. It also helps to integrate quantitative and qualitative data which are crucial to handle complicated phenomena and perform in-depth research (Zainal, 2007).

The overall research method for gathering research information comprises of two stages First stage includes a search of information through internet academic material and the second stage includes targeted search of websites of government, security departments, and police. Comparative Analysis of academic literature gathered has been done to find the ways in which cyber threats are prioritized by each country's cyber-security policy, roles of government, departments and agencies in each country to address the cyber-security issues. As the research is a rapid comparative analysis so it represents a snapshot of a current era and is based thoroughly on the information provided in open-source documents. All the data and the information are clearly sourced.

1.3.4. The significance of study

The thesis will provide insights on the cyber-security policies of the countries. These insights and comparative analysis of the cyber-security policies will help to provide guidance for the future researchers and policy- makers. These countries were selected as they have multiple commonalities and few differences in their cyber-security policies. This research will also help the new researchers and policy makers of ICT emerging countries to broaden their vision for better cyberspace defense.

The thesis will discuss some unexpected results regarding cyber policies of the developing countries. Like the policy-makers of developing countries are focusing more on security issues and for cyber threats, they have higher risk tolerance than the developed nations. Moreover, the thesis will also highlight the potential ways to reduce the cyber defense cost. The thesis will also focus on universal approach towards cyber issues rather than that of customized approach by each country. The active exploration of the ways to reduce cyber risks by upgrading the cyber-security policies internationally will also be done.

The empirical data set will be built in the thesis to depict the relationships and collaboration among telecommunication, legal, development and private sectors of the mentioned countries for the sole purpose of cyber-security. The thesis will highlight the global efforts and actions regarding cyber-security, cooperation among countries to meet the challenging and dynamic cyber threats. Rather than taking cyber-security as a deployment of the set of security tools, the thesis will deal the cyber-security as a

national and internal mission to accomplish. The thesis will not only identify the basic reasons due to which cyber-security is a threatening challenge for each of the country, but it will also identify the potential ways to address the security challenge.

The structure of research is as follows: Chapter one confers cyber-security threats and policies in Malaysia, Australia, USA, China, Canada, India, and EU. Chapter two discusses cyber-security policy as a motivation to deploy ICT to safeguard potential loss by cyber-attacks in the mentioned countries. The third chapter comprises of multiple studies regarding differences in cyber-security policies of the countries and why cyber threat needs to be treated as a universal challenge? The fourth chapter highlights unaddressed cyber challenges in the countries and cyber-security requirements in the areas.The fifth chapter addresses all open- ended questions regarding cyber-security policies and existing cyber threats in the countries which were not obvious prior to the research. The comparative analysis in the thesis will provide guidance on cyber-security regarding the existing cyber issues.

1.4. Common Attribution Act

Intelligent hackers launch attacks using hidden routes from different countries hence making it trivial to trace down. Tracing the original root cause is necessary to prevent assets for any future misuse. This scenario highlights the importance of having a Global Policy on cyber-attacks. This Global policy also known as a set of Common Attribution Act will make sure that countries share critical information among each other in case of any forensics. An original intruder can only be held responsible for its activities if countries have a common policy and maintain a trust level to ensure that criminal is a criminal no matter where he or she is. One of the major hurdles is foreign policies which are different for each country (Kostadinov, 2013).

Attackers may use naive user's machines to launch a certain attack. All over the world attackers are in search of such easy low hanging fruits. Attackers use them as a shelter so that in the case of any forensic investigation they remain safe from any legal obligations. Therefore it is extremely important to find and sanction the original attacker rather than the innocent individuals (Graham, 2010).

Attributions can be divided into two main categories depending upon the response. Direct attributions are the one in which respective state is responsible for all the acts of an individual that may have led to a certain incident inside and outside the physical boundaries of a country. Indirect attributions are the one in which individual is held responsible and state held no responsibility at all (Mejia et al., 2014).

Different countries over the period of time have formalized Information security policies to investigate and mitigate global cyber threats. The "Global Internet Freedom Act" (S 3093 IS) was proposed in the U.S. Senate on October 10, 2002, to "develop and deploy technologies to defeat Internet jamming and censorship." Their concern is to restrict the information one can access from outside the country. A set has been seen in most of the forensic investigations that attacker develops a launching pad based on the freely accessible information across the geographical borders. Globalization no doubt has provided many advantages to mankind but it is pertinent to mention here that it also gives rises to many security issues as one sitting at one place can gain information of any other country as there are no boundaries in the internet world (David et al., 2003).

CHAPTER 2

2. LITERATURE REVIEW

In this chapter, we will shed light on the increasing trend of the cybercrimes. This required focusing on the importance of training on the means of cyber-security defense. The next point will be the human dimension of cyber-security. Then, the role of the governments in cyber-security and the factors that are responsible for it are mentioned. This is followed by an application that reveals the significance of the cyber-security policies. The chapter will also show the national cyber-security policies in seven different regions: Canada, China, Europe, USA, Malaysia, India, and Australia. These countries were chosen to include a variety of nations in different continents and it is clear that they have different positions in the cyber-security policies and strategies.

2.1. The widespread of the cyber-security crimes

Information Security breaks are increasing with the new tools and techniques. Effective information sharing and coordination during incident resolution are essential for limiting the cyber-attack against organizations and nations. As there were few available means that are insufficient to prevent the cyber-attacks, the Computer Security Incident Response Teams (CSIRT) and Information Sharing and Analysis Centers (ISAC) created new means for developing the incident reporting and coordination. Fire (Firefox for Incident Reporting) is created to provide reporting organization and to share

the incident information in standardizing format with CSIRTs (National and Sectorial) during incident resolution process. The fire also integrated tools to secure communication, sensitive information labeling, real-time interaction with handler & analyst and database of stakeholder point of contacts (Bahuguna and FIRE, 2015). Anwar and Mahmood (2014) discussed some modern cyber-attack related offenses. Smart grid security is important to maintain constant power system operation during the emergency situations. A power failure may occur due to the absence of the suitable security measures and to protect this power system, we must influence on smart grid security problems. In a smart grid environment, electric power infrastructure is well-run by joining the current and future requirements to its consumers. The acceptance of the cyber system has increased the energy efficiency of the grid. It has introduced cyber-attack issues which are important for national infrastructure security and customer pleasure. Due to the cyber-attack, power grid may face operational failures which may damage serious power system components.

Internationally, cybercrime has become a more clear and dangerous risk. When arguing about Cyber Space risks, it is not a problem if mean national infrastructures, private companies, and citizens will be violated, but instead when it happens, when it is recognized that this has taken place, and what is the range of this attack (Leccisotti, et al ., 2013). The high usage of the Internet interconnections is considered the main reason for the increase of the cyber-attack crimes often and Malware is the principal choice to make malicious intents in the cyberspace domain using the present vulnerabilities or by using new technologies techniques. Thus, the improvement of more innovative and effective malware defense mechanisms is considered as an urgent issue to the cyber-security community. New attack methods due to emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure were discussed in (Jang-Jaccard, and Nepal, 2014). Hackers are a risk to the security of an organization's information resources. Johnston, Warkentin, McBride, and Carter (2016) determined the main situational factors that cause information security policy breaches. The results of this model show that dispositional factors act as moderators of the relations between perceptions and intentions to breach information security policy. This

study represented the first information security to identify the presence of these signs and their influence on information security policy violation intentions.

2.2. The importance of raising the awareness and the number of trained professionals in the cyber-security

The Internet is increasing in the daily lives of many persons, organizations, and nations. It has a positive effect on people communication. It has also presented new ways for business and it has offered an opportunity to govern online. Cyberspace offers services and chances. It is followed by many risks that many Internet users don't know. Many countries have developed cyber-security awareness and education processes to decrease the obvious ignorance of the Internet users (Kortjan and Von Solms, 2014). This can be attributed to the fact that the relationship between cyberspace and national security is usually presented as a conclusive and an accepted "truth." Although, there is no natural reason for this link. To be understood, the focus is not only on conversational practices by "visible" elite actors but also on how a range of less visible actors inside and outside of government form a reservoir of acceptable risk representations that affect the daily practices of cyber-security (Cavelty, 2013).

Cyber-attacks caused dangerous risks to government, businesses, and individuals. There is a dangerous shortage of the trained professionals and academic programs to train and produce these professionals. Various countries consider this as a human capital problem such as the US and New Zealand. Fourie, Pang, Kingston, Hettema, Watters, and Sarrafzadeh (2014) discussed the severity and different dimensions of this issue. They presented an analysis of the data from a cyber-security research center collected on cyber-attacks and presented practical solutions and examples from New Zealand. They also drew conclusions built on data that are collected in New Zealand and Japan.

2.3. The human dimension in the cyber-security

The present methods of cyber-security are not working due to a security problem that spreads outside the state. It focuses on the state, the security of the individual citizen and on the security of the whole system. The problem is arising from focusing on information technologies and serious functions of substructures, with little consideration for humans directly. This lack of interest in people makes it easy for state actors to

control the different security needs of human beings in that space. Using cyberspace for national security, both in war fighting and the mass-control has harmful effects on the level of cyber-security internationally. To solve this problem, the cyber-security policy should be anti-weakness and focus on privacy and data protection (Cavelty, 2014). Recognizing human dynamics of cyber-security is important to increase the knowledge of analysts.

Oltramari, Ben-Asher, Cranor, Bauer, and Christin (2014) focused on the requirements for designing a model of cyber-security analyst's decision. On describing the main features of such model, they concentrated on the cognitive aspects and knowledge representation. This by integrating ontological and cognitive architectures in a crossbred-modeling framework, It's possible to characterize and simulate the main structures that direct the decisions of protectors and attackers and mediate interactions among them in the cyberspace. In this regard, "the cyberspace is defined as much by the cognitive realm as by the physical or digital" (Lewis and Timlin, 2011). As a result of this multilayer redness, "cyber-security has become a complicated issue, which requires scientific understanding both in terms of theoretically grounded and empirically validated models (Kott, 2014). Behavior - change interferences are common in areas of human-computer contact, but rare in the field of cyber-security. Coventry et al. (2014) presented methods to work with organizations in order to develop such social interferences. This method uses features of creation together with a set of goals from the behavior change that allows researchers to work together to identify a set of nudges that might promote the best behavioral practice. They described the structured approach utilized effectively in the development of a nudge to relieve insecure behaviors around the choice of wireless networks.

2.4. The role of the governments in improving the cyber-security

The Internet has made the world like a small village by creating new ways of communication. The low connection costs made more people, around the world, to use it. Increasing our dependence on the digital world makes it less safe against the attacks of our digital intimacy. It also affects the digital information of governments who started to use the digital technology in the last years. Hackers tend to attack digital networks,

internet sites, the governmental organization's infrastructures and the individual and the private companies. Governments now try to upgrade plans against these cyber-attacks, including legal measures to protect themselves. Due to speed the nature of the technology, governments need to provide dynamic mechanisms against these attacks (Gurkaynak, et al., 2013). Shackelford and Craig (2014) discussed the suitable role of nation-states in Internet governance and improving global cyber-security. The governments seek to defend their serious infrastructure. This article studied the planned and applied serious infrastructure regulations in China, the European Union, India, the United Kingdom, and the United States. Ultimately, the Article shows that there is a continuum of governmental interests to regulating cyberspace and remarking the importance of finding common ground between stakeholders. Then the global community will be able to achieve agreement on the future of internet governance and support cyber peace. The national cyber-security strategy (NCSS) was published by a group of countries. Although each of these NCSS expects to define the same group of cyber-security dangers, there are large differences among the national focal points and approaches.

It is thought that the use and growth of cyber-space depending on big data, cloud computing and IOT (Internet of Things) will be a key factor which defines national effectiveness. In the intervening time, cyber risk accompanied by the use of cyberspace, risks related to cyberspace, have become enhanced and complicated (Min et al., 2015). This doesn’t mean that the government is only responsible for cyber-security as the public-private partnership is important in making the national cyber-security strategies of the US and the UK because of its negative effect in the case of critical infrastructure protection. Carr (2016) detected a lot of literature on the public-private relationship in facing the challenges in national cyber-security strategies. The research showed a serious difference in the two partners' projections. The private sector is not tending to accept responsibility or liability for national cyber-security. Governments seek to manage national cyber-security raises questions about how states promote their own security in the information age.

2.5. Factors to improve policies of cyber-security

Muhaya (2010) studied the factors that are required for national security policies of different courtiers. These factors were gathered and compared to define the mutual and the rare policy respects among these countries. These countries are USA, Malaysia, Australia, Canada, and China. The study (Muhaya, 2010) can be considered as a leader for the improvement of the current national information security policies in different countries and for the future development of such policies in countries where they do not yet exist. Graves et al., (2016) studied some of the factors that make developing a "science of security" an important research and policy challenge. They focused on how the experimental obstacles of missing data, imprecise data, and invalid inferences can influence and sometimes harm the security decision-making processes of individuals, companies, and politicians. They studied the application of these examples in the setting of country security. Luiijf et al., (2013) investigated and compared 19 NCSS [Australia, Canada, Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, New Zealand, South Africa, Spain, Uganda, the UK (2009 and 2011), and the USA]. This research shed light on the mutual approaches and weaknesses. They presented results and recommendations to help countries in developing their NCSS.

2.6. Application on the significance of cyber-security

The influence of the cyber issues on the safety and flexibility of railway systems has been studied by industry specialists and government agencies. Bloomfield et al. (2016) showed some of the work done by Adelard in this range from an analysis of the vulnerabilities in the ERTMS specifications through the assessment of a high-level cyber-security risk of a national ERTMS implementation and detailed ERTMS systems analysis on behalf of the GB rail industry. This paper focused on the overall methodology for security-informed safety and hazard analysis.

2.7. National Cyber-security Polices in Different Countries

The first country that will be understudy is **Canada**. Bailetti et al. (2013) mentioned that to increase the success and the ability of Canadians, they designed an engine that's formed of five structures an ecosystem, a project community, an outer community, a stage, and an organization. These structures are joined together by the strategic intent, governance, resource flows, and organizational agreements. It's predictable that this engine will increase the number of Canadian companies that spread internationally into products of cyber-security markets, and protect Canada's critical infrastructure which can be considered as a new vision for NCSP (National cyber-security policy) in Canada (Bell, 2006). Now, Canada is considered as one of the most online states all over the whole world and approximately all formal and commercial services are based on the Internet. It can be said that the challenges of the cyber-security are mainly related to the level of the development of the Information and communication technology (ICT) (Lakomy, 2013).

China isn't in the same position as Canada. Although China has made clear progress in its Information and Communication Technologies (ICTs), as a new user of these technologies, it still has a lot of steps away from the developed countries. China is in a weak position of cyber-security policies so in the near future; it will overcome this challenge. This can happen easily in case of increasing interest on the cyber-security policies in China (Subsorn, & Limwiriyakul, 2012). Longdi (2013) mentioned the fact that cyberspace is the 5th domain for human activities after land, sea, air and outer space. Due to the transnational nature of cyberspace, it has become a new border for global governance. Cyber-security has a great association with political, economic and safety interests of countries. China cares about internet development and has made a huge progress. China suffers from cyber-attacks, as it is a late comer in this field. Also, China will seek to a peaceful, safe, open, and supportive cyberspace with the global community. China is linked to cybercrimes of different kinds, ranges, reasons, and goals. Kshetri (2013) developed typology, classification, and characterization of cybercrimes associated with China, which can be helpful in understanding modus operandi, constructions, outlines and personal characteristics of cybercrime organizations and

potential perpetrators. They could make a detailed reference on the main aspects of cybercrimes in China.

Europe is in an advanced position of the cyber-security development. The European Union's organizational arrangement is a collective actor in a related world trying to establish itself as a strategic actor. However, there are other actors in the world, seeking to change the world concerns to face a number of security-related fears that require advanced and progressive measures to ensure their presence. Cyber-security has become a growing need for increasing the number of attacks on the internet. Today the unfriendly invasion into the cyberspace varies in its nature and frequency. It becomes an urgent to look into the plans or the arrangements that the EU has created to prevent the cyber-attacks (Van et al., 2005). Being aware of the danger of the cyber-crimes, the EU published a Cyber-security Policy and also a proposal for a Network and Information Security Directive (NIS) in 2013. The European Cybercrime Centre (EC_3) aids to defend European people and companies by helping criminal surveys, uplifting the awareness against uprising trends of cyber-attack activities (Sarma, 2016). Information security was presented as an important issue in the regulation in the European Union (EU) to mention the potential risks associated with the widespread use of information technology. Information security can be used to protect and prevent against risks or simplify users in meeting specific requirements with regard to pertinent legislation (Mitrakas, 2006).

India is an example of the country that misses developed strategies in the world of the cyber-security policies. India intends to spend over 5.8 billion to compensate India's weak power sector as a part of its Five-year plan (2012–2017). The federal government focuses on building Information and communication technology (ICT) capability in the state electricity boards. However, there is no power sector specific cyber-security in India. Cyber-attacks cause extensive damage and a risk to National Critical Infrastructure. A lack of security decreases the country's power sector stability. It seeks to build power sector specific cyber-security regulations depending on the knowledge of regulators in other infrastructure sectors (Kumar et al., 2014). The inadequate distribution of simple skills required in a knowledge society is definitely due to the lack of development in the ICT sector which hinders leveraging the yet-untapped

innovation potential of large, young Indian human resources (Bilbao-Osorio et al., 2013). In July 2013, the government of India emerged the National Cyber-security Policy, which proposed 14 goals that included enhancing the protection of critical infrastructure and developing 500,000 skilled cyber-security professionals in 5 years to represent a main component of NCSP in the development of public–private partnership (PPP) efforts to enhance the cyber-security landscape (Kshetri, 2015).

The UK succeeded in bonding their academic foundations with the commercial market in the cyber-security world. Universities and Colleges are using virtual worlds to be like a Second Life to access to the knowledge and the economic development of nations. The ability for using and developing of these virtual worlds is influenced by government policy and investment. Roth (2010) compared the performance, ICT policies and expenditure of the United States (US), the United Kingdom (UK) and Australia since 2006. The US and the UK have utilized virtual world technologies while Australia has ignored the opportunities presented by Virtual Worlds. The United Kingdom recognized the importance of ICTs to support its innovation and competitiveness performance. Thus, it has succeeded to build a well-developed ICT infrastructure due to the successful national cyber-security policy (Bilbao-Osorio et al., 2013). Stoddart (2016) tried to help the UK government in protecting the UK from cyber-attacks on its Critical National Infrastructure by outlining the scope of the problems Britain faces. With a National Cyber-security Centre now being established and an updated National Cyber-security Strategy due in 2016, it is vital for the UK government to take the right approach.

The **Australian** Government considers the cyber-security as an important policy area for two reasons. The first is related to the financial cost and the personal influence that results from the cyber-crimes on businesses and individuals in Australia. The second reason is that the Information and Communications Technology (ICT) is highly affected by the cyber threat depended on the levels of dependence that Australians have, both individually and communally (Brookes, 2015). Borgman et al., (2015) conducted some interviews with members from different government parts, to know whether existing processes are sufficient to achieve the application of ISMS and sorting of data for the relevant SA government bodies. Through these interviews and reviews conducted within

other Australian State, they detected the main areas that the SA Government may need to consider up to June 2017 as a part of the developed roll-out of the other phases of ISMF version three presentations. The Australian government emerged its Cyber-security Strategy in 2009. In addition, a variety of series of laws and rules in identifying, regulating, investigating and prosecuting crimes and criminal behaviors in the cyberspace have been proposed and then put forward by the federal, state and territory governments in Australia. Moreover, Australia's public institutions, governmental and non-governmental organizations have been playing a key role in safeguarding cyber-security while reducing the occurrence of cybercrimes as well (Jiang and Hu, 2013).

Malaysia chose to benefit from the information and communication technology as a mean for its development and this resulted in the growing the use of digital information systems in the industry, in the private and in the public sectors. However, the digital information systems made it under risks, especially to the Critical National Information Infrastructure (CNII) which among others include cybercrimes such as Hacking, Intrusion, Fraud, Harassment, Malicious Code and Denial of Service Attacks so The National Cyber-security Policy (NCSP) is Malaysia's was put in place to ensure the CNII is protected against the faced risks (Hashim, 2011). This research (Mohamed, 2013) debates the role of the government and the organizations in dealing with Cybercrimes, the role of cyber laws, and their work with the traditional law to prevent cybercrimes which are growing in Malaysia. According to this report, what caused a lot of anxiety from the public and the Government is that crimes increased in 2011 compared with 2010. These crimes are causing harm to people, economy and the country. As Malaysia is lacking to the manpower and technology, it's difficult to prevent these crimes. There must be real methods to prevent and detect the cybercrime activities on all networks in order to be able to overcome the attacks such as denial of service attacks (DOS). This is obligatory because the lack of real protection against such crimes can threaten the security of the Malaysia and threaten the development of ICT (Mohamed, 2013).

2.8. Summary

It can be said that the national cyber-security policies and strategies now represent main parts of the national laws and regulations of all countries due to the increase in the number of cybercrimes in all countries and against organizations and individuals. The issue requires cooperation between the public and the private sectors of the society to focus on the war against the cyber terrorism.

CHAPTER 3

3. Cyber-security Policies

3.1. Introduction

The cyberspace is expanding with time due to which stakes for cyber-security are going high due to which it is becoming more crucial to have an all-inclusive policy for the security of cyberspace. Cyber-security is challenging for all countries due to inherited vulnerabilities of the cyberspace and increasing dependency of several systems on cyber technologies. (Amoroso, 2005) It is not only the job of Cyber-security experts to develop effective firewalls and security tools but it is also the job of higher authorities to make special policies to make cyberspace more secure. (Carr and Shepherd, 2010) Most countries make some policies to ensure cyber-security. These policies focus on some traditional attributes and the presence of these features in a policy indicate its comprehensiveness (Bayuk, 2012).

These traditional attributes form the foundation of cyber-security policies but these common traditional attributes are also expanding with the advancing technologies (Ślęzak et al ., 2009). For instance, there was no common policy for cloud computing services a few years ago because this technology was not widely available in most countries but now it has become one of the most demanding technology in the cyberspace. (Tajts, 2012) Similarly, continuous technological advancement is making

cyberspace very sophisticated therefore a well-organized and thoughtful security policy is very crucial (Lehto, 2013).

These common attributes include Consumer Rights, Privacy, Identity Theft, Computer Security, Spam Act, Data security act, Network security laws, Data Security of Cloud Computing, Telecommunication, Smart Grid, National encryption policy, Digital Signature, Cyber protection act, E-banking, and E-commerce. It is important for all service providers in the cyber space to know these common traits especially when they are providing services in multiple countries. Users in any country should also aware of at least those attributes which are directly related to them because every country makes policy not just for service providers but also for users to prevent any kind of undesirable incident in this field (Bayuk et al., 2012). This chapter will present all those attributes and policies related to them. This is will help to take the research work on this topic to next level.

3.2. Common Attributes and Their Importance

These attributes are important for cyber-security policy because these attributes cover most of the cyber-security issues (Chertoff, 2008). It is important to address these issues because every year billions are lost in hi-tech attacks (McKenna, 2005). Privacy and data security are the hottest topics of cyber-security especially in a developed country where awareness and number of multinationals are high (McKim, 2001). Cyber-security regulations have laws for data security, privacy, spamming, telecommunication and network security for more than a decade (Heiman, 2003). Data security, spamming, and privacy attributes are crucial because it increases the confidence of users due to which a number of users increases and with it opportunities for economic activities (Ghosh, 2002). Telecommunication attribute is important to keep the communication services secure (Chen and Gong, 2012). These attributes are still crucial for cyber-security policies but some other advanced attributes like smart grid, cloud computing security and e-commerce has also become a vital part of this policy. The attribute of the smart grid is important to monitor and control power generation, protection, and distribution (NIST, 2010). Cloud computing attribute is crucial for cyber-security policy because it indicates that policy is advanced enough to keep cyberspace secure in the

modern era (Tajts, 2012). Attributes of E-banking, Encryption, and Digital Signature are important for secure transactions. These fifteen attributes are the basic requirement of a comprehensive cyber-security policy in this modern era (Oak Ridge, 2011). Every attribute in the list has its importance to tackle different threats and risks to cyberspace. These attributes also provide direction to improve policy because it is not necessary that a policy work for all stakeholders in all situations (Rosenzweig, 2016). All these attributes can help countries to build a global cyber-security policy which is very crucial to minimize cyber-attacks and create secure global cyberspace (Knapp, 2009). These attributes in a policy do not only make cyberspace more secure but the economy of a country also depends a lot on its cyber-security policy because marketers closely watch different attributes of every country's cyber-security policy (Shields, 2016).

Electronic banking

Basically, all the transactions banking should be secured from incidents, Electronic banking is the present and future of banking. It is important to secure every transaction on any platform (Hawke, 2000; Zhang, 2010). Laws for the Line Encryption compel every bank to use line encryption technique effectively. E-Payment Code forces every bank and financial institute to take appropriate steps to secure transactions on their digital platforms (Weir et al., 2010). These codes and act make it compulsory for every financial institution to use branch connection encryption, digital certificates, and firewalls so that people can enjoy secure digital banking experience (Weir et al., 2009).

E-commerce Law

E-commerce Law is the boost in online shopping has taken E-commerce to the whole new level. Online shopping platforms are providing great service to people but they are also a source to steal users' sensitive information (Zhang, 2010). Every organization with E-commerce facilities must use approved payment method as per local laws (Singleton, 2003). E-Payment code provides directions to E-commerce companies but these codes are not as applicable as they are in the banking sector (Kamath, 2009). However, privacy laws ensure some level of security in this field of cyberspace (Relyea, 2007).

Cyber Protection Act

Cyber Protection Act provides basic security to all users in cyberspace through laws like Electronic Document Act, Privacy Protection Act and Information Technology Acts (Lloyd, 2004; Kamath, 2009). The main purpose of legislation in this field is to ensure that every organization and individual doesn't harm other individuals, organization, state or society in any way (Voeller, 2014). The goal is to develop a secure environment for everyone while keeping the quality of services high (O'Byrne, 2013).

Digital Signature

To secure the data, the existence of digital signature is not enough to protect the digital data. Digital signatures should be sophisticated enough to keep data secure (Hawke, 2000). Electronic Signature Act is used in some countries, which forces every related authority to develop a system of electronic signatures not only to protect data but also to identify people (McCann, 2002; Kamath, 2009). These signatures also keep financial transactions secure. Legislation in this field also includes Digital Signature Act and Information Technology Act (Lloyd, 2004).

Identity Theft

Identity Theft is one of the biggest crimes in cyberspace as it can lead lots of social issues and can also cause national security issues (Kamath, 2009). A lot of legislation work has been done in the field because on social media identity theft is very easy and it is difficult to define identity theft in some cases and it is even more challenging to choose the penalty for seemingly minor cases (Hoffman and McGinley, 2010). Theft and Assumption Deterrence Act prevent people from using the identity of any other person for any reason. Personal Information Protection, Electronic Document Act, and Privacy Act also have laws against identity theft. In some cases of identity theft, Criminal Code can also be applied due to severance of situation (Manz and Best, 2005; Relyea, 2007).

Privacy

Privacy is the right of people in every place including cyberspace and Civil Law Act and Privacy Protection Act are enough to protect the basic privacy of all people (Relyea, 2007). But some technical issues are associated with cyberspace due to which some special legislation is required to define and provide optimum privacy to people (Kamath, 2009). Data Protection Reform is the result of efforts to provide appropriate privacy to all users (O'Byrne, 2013). These reforms also prevent any organization to violate privacy people in the name of security without approval or any strong reason (Yee, 2006).

Computer Security Incidents

The Internet allows computers to connect to remote computers and smart devices but it is also providing a way to hackers to hack computers of other people and sensitive and private data (McCann, 2002; Kamath, 2009). Cyber-security Act prevents any individual and organization to hack computer of any other organization or individual. Before this law, Draft Cyber-security Act was used to keep computers secure (O'Byrne, 2013). Information Technology Act also has clauses to reduce computers security incidents (Lloyd, 2004). Consequently, in this area researchers have reached to keep hackers away from computer users.

Data Security of Cloud Computing

Data Security of Cloud Computing also critical one in order to cloud computing is becoming very popular all over the world and it is considered as the future of IT. There are lots of benefits of this technology but the security of cloud computing is very challenging due to its flexible nature and limited physical structures (Millard, 2014). Digital tools are required to keep cloud computing save and Data Signature Act is used to achieve this goal (Lloyd, 2004). This act forces every service provider to develop a smart system of digital signature to protect data of every user in any cloud. Data Privacy Act also protects the privacy of users of cloud computing services (O'Byrne, 2013; McCann, 2002).

Smart Grids

Smart Grids are one of the applications of computer networks and Smart Grids also come under the cyberspace as they use digital communication process for monitoring and controlling of energy supply (Wang, Liang, Mu, Wang, & Zhang, 2013). The security of these grids is ensured through the Security Acts in the country. Grid Energy Act is also used in several countries to protect grids and people from any harm through these grids (Sorebo and Echols, 2012). Energy Independence Act also people to develop these grids while IEEE Standard Association help keeps the quality and security of smart grids high (IEEE, 2016).

Network Security Laws

Network Security Laws is a compromised network can cause serious threat not only to citizens of a country but also to the state (Saxby, 1995; Kamath, 2009). Every telecom company is required to keep its networks protected from all cyber-attacks including phishing, virus, unauthorized access, Trojan Horses, worms and any other such attack (Wilson, 2014). Even terrorist attacks can be carried out through a conceded network. In countries like USA and Canada acts like Protecting Cyber Networks Act, Cybercrime Act, and National Defense Act are the results of the legislation in the field network (Lloyd, 2004). In this result, networks have been secured from attackers.

Spam Act

Those electronic messages are considered as Spam which contains unsolicited content and sent to a huge number of people. Spamming is mainly used for advertisement of low-quality or illegal products (Dunham, & Bradshaw, 2004). Spam makes the user experience highly undesirable and spreads objectionable messages to people. Moreover, spamming is also used for hacking; ; therefore, special legislation is required to spamming (Voeller, 2014). Spam Act is used to achieve this purpose (Beardwood and Stern, 2014). Information Technology Act also has clauses to control spamming. Directive on Privacy and Electronics Communication is also used in some countries to eradicate spamming activities on cyberspace (Kigerl, 2016).

Telecommunication

Telecommunication is one of the oldest acts in the cyber space and it has gone through several amendments as information technology is advancing and changing telecommunication infrastructure (Crandall, 2006). Legislation in this field includes acts like National Cyber-security Policy and Telecommunication Act (Crandall, 2005). These acts make sure that every service provider takes proper security measures, does not harm state in any way and provide high-quality service to everyone (O'Byrne, 2013; Voeller, 2014).

Consumer Rights Protection Law

Consumer Rights Protection Law is consumer rights change with the evolving technology and changing nature of products and services (Salaün, 1999). Consumers of cyber services have multiple rights. These consumers have the right to privacy and service provider must make appropriate arrangements to protect their customer's privacy (Chin and Yusoff, 2016). Personal data of consumers should not be revealed to any unauthorized entity in any case (Kerber, 2016). It is not only the responsibility of service providers to secure their system but it is also the obligation of government to make proper laws against spamming and take severe action to create a secure cyber environment (McIntosh, 2015).

National Encryption Policy

National Encryption Policy of any country dictates the laws for the protection of virtual data and to secure public and private networks (Meyer, 1996). This policy indicates the intention of a government to protect all communication channels (Wang et al., 2015). Countries develop different regulation for this purpose and some of these regulations and acts include Information Technology Act, Data Protection Regulation, and Secure Public Networks Act (Voeller, 2014). All service providers in the sector telecommunication and cyberspace need to comply with these acts (Matlick, 1998).

Data Security Act

Data Security Act is another influential common attribute in Cyber-security which there are two big categories of data on cyberspace including private data and public data. Public data can be accessed and used by all users but personal data can be accessed only by authorized entities (Hart, 2009). Business organizations may have sensitive data of a large number of people. This data should not be used illegally by any entity (Voeller, 2014). Personal Data Protection Act protects personal data of users in many countries while Data Security and Breach Notification Act is used to prevent any organization or individual to acquire and utilize data of any other individual or organization without proper authorization (O'Byrne, 2013). Data security legislation also includes Data Protection Regulations (McCann, 2002).

3.3. Summary

In conclusion, all these attributes lay the foundation of Cyber-security policies in countries such as Malaysia, Australia, USA, China, Canada, India, and EU where ICT is progressing swiftly and users expect a high level of security. All these laws and traits, mentioned above, cover every vulnerability and security concern of cyberspace. It is important to know that how these traits are important for the security of sophisticated cyberspace in big countries. In the next chapters, the importance of these attributes in Malaysia, Australia, USA, China, Canada, India, and EU will be studied in detail. According to those countries common attributes analysis, the outcomes will become the consequence of comparison common attributes Cyber-security Policies between those countries.

.

Chapter 4

4. Cyber-security Comparative Scenario

4.1. Introduction and Description

The internet has become a vital part of everyone's life, especially in developed and fast developing countries. More than three billion people in the world who use the internet for personal and professional purpose and their number is continuously increasing. In this scenario, it is very important to ensure the quality and security of cyberspace for all internet users. A well-developed policy is needed for this purpose, which covers all important aspects of cyberspace security (Andreasson, 2012). This chapter will discuss how different attributes in the policy for cyberspace security in different countries have been selected and why these countries are selected. The common attributes of cyber-security in selected countries will be compared to find out how these countries are responding to cyber-security issues in their country. At the end, the result matrix will be presented.

The number of security issues is increasing the number of users and it is not possible to make a list of these issues and make a separate law, act or policy for those issues. Due to this reason, major security issues are categorized in different groups. Countries make policies not for single issues but for each category of issues like spam act, digital signature laws, and cyber protection acts. All these acts and laws in any country demonstrate its cyber-security policy. Due to large number security issues, it is not

possible to have one code of conduct or law to create a secure cyber environment, ; therefore, every country's cyber-security policy contains several attributes (Graham et al., 2011). In this research work, fifteen common attributes are selected for analysis. These common attributes include E-commerce, E-banking, cyber protection act, digital signature, identity theft, privacy issues, computer security incidents, data security, smart grid, network security, spam act, cloud computing, telecommunication, encryption policies and consumers' rights protection. Each attribute encompasses a group of cyber-security issue and different countries respond differently on each attribute. Their response depends on various factors like political dynamics, GDP, cyber-security breach history, and a number of users. These selected common attributes for seven countries are studied to find out how each country is preventing its cyberspace from different issues.

4.2. Selection Methodology

4.2.1. Selection of Attributes

The literature was reviewed for the selection of common attributes of cyber-security policy. It has been observed through the review of literature that some of the biggest issues in the cyberspace are data protection, privacy, and spamming (Stoddart, 2016). Social media is becoming popular but it is also bringing some issues like identity theft which is now become an important part of cyber-security laws. Latest technologies are opening new gates of protection like digital signatures. In future, digital signatures are expected to replace hand signature, ; therefore, digital signature and encryption techniques are needed to be studied (Chatterjee, 2014). Other important internet based facilities are telecommunication and networking. It is important to study how different countries are ensuring the security of these facilities (Au et al., 2014).

E-banking and E-commerce are becoming popular with the increase in online shopping. Every country has a policy for the E-commerce and E-banking. Cloud computing is relatively new technology and developed countries are struggling to develop a comprehensive law to ensure security for cloud-based services. Cloud computing is also growing very rapidly especially in the USA where several companies including Microsoft, Amazon, and Apple are providing cloud-based service to its millions of users.

One of the biggest concern of cloud users is the data security, ; therefore, the attribute of data security in cloud computing is selected for analysis.

4.2.2. Selection of Countries

Seven countries including USA, EU, Australia, Malaysia, China, Canada, and India are selected for this research because all these countries have a large number of internet users. These countries have appropriate laws for cyberspace security due to which their policies can provide a guidance for the development of a comprehensive policy. Moreover, enough amounts of data is available for cyber-security issues and policy in these countries.

- The USA has very high number of Internet users. More than 70% of its population uses the internet and this percentage is continuously increasing. This country's internet industry is a Trillion-dollar industry; ; therefore, it has a very well-developed policy for cyber-security. The USA is also a birthplace of lots of novel Internet services (Kazan, 2016) due to which its policies keep on updating. Due to all these reasons this country is selected for this research.

- The European Union consists of some very rich and developed countries. It has very high literacy rate and almost 80% of its population uses the internet. They use the internet for diverse purposes, ; therefore, they also face security issues of diverse nature. The cyber-security policy for the European Union is also a very comprehensive policy which is also easy to access due to which this country is selected (Štitilis et al., 2016).
- Australia is a developed country with more than 20 million internet users. Australia is hosting a large number of students and it welcomes millions of tourists every year. It means a huge number of people are affected by the cyber-security policies of Australia and this country is also striving to make a flawless policy for all kinds of internet users in this country. (ASSC, 2017)

- Malaysia has one of the fastest growing GDP in Asia. It has very high percentage of internet users as compared to other Asian countries. More than 70% of people in Malaysia use the internet (Cyber-security .my, 2017). Lots of scholars have worked on the cyber-security laws and acts of Malaysia to provide basic information to other scholars; ; therefore, this country is also selected for analysis.
- Canada is another developed country with more than 30 million internet users. 88% of people in this country use internet. This country has faced some serious cyber-attacks; therefore, it is one of the most pro-active countries in terms of cyber-security (Gendron, 2013). This country also has a well-developed policy for cyber-security; therefore, it is also selected.
- China has the maximum number of internet users in the world. World's biggest e-commerce company, Alibaba is operating in this country. This company is offering diverse web-based services in China. It is not possible for such huge number of people to use diverse web-based services without appropriate policy (Miao and Lei, 2016). This research would be incomplete without analyzing policy of this country.
- India is the second biggest country in terms of internet users due to its large number of population. Although the percentage of internet users is relatively very low as compared other countries it has one of the fastest growing IT industry in the world (Samuel, 2017). It also has several laws for different cyber-security issues; ; therefore, it is also selected.

There are some other countries which have a large number of internet users and highly developed infrastructure of the internet but these countries are not selected due to several reasons. One of such country is South Korea. This country has a large number of internet users but most of its official documents for cyber-security are in the Korean language; therefore, these policies are not included in this research. The United Kingdom policies are covered in the policies of EU; therefore, there is no need to mention policies of the UK separately. The inclusion of EU in this research eliminates the need to include EU countries separately; therefore, countries such as Denmark are

not in the list. New Zealand also has well-developed infrastructure but it has very small number of internet users due to its small population. Australia is included in the research to cover the policies of the Australian continent. In Japan publishes official documents are in Japanese languages; therefore, Japan is not part of this study. Singapore has very limited data available on the internet about its cyber-security policies due to which it is also not included in the list.

4.3. Comparison

The cyber-security risk has increased to the higher extent globally that eliminating this risk has become highly difficult. However, the policies developed by the individual countries have controlled this issue to some extent. The e-banking and e-commerce security measures in the U.S are not sufficiently controlled even after the policy development because of the existence of large databases (Kurt, 2015). In comparison, the EU's cyber-security measures with respect to E-banking and E-commerce are effective because they are continuously developing the cyber-security policies on the national level and providing banks with proper infrastructure for sharing information in a private way. At the same time, Scott J. Shackelford 2016 has analyzed that the Canada is facing similar level risk as the United States because it is mostly relying on private self-governed strategies for attributes of network security, data security, e-banking, and e-commerce as compared to applying the approach of top-down direct regulations (Scott J. Shackelford, 2016).

The cyber-security policies with respect to the banking sector and computer security indices of India are not effective because they are only relying on the guidelines with minimum best standards and the large organization has failed to implement these standard set guidelines thereby losing their competence in policy regulations (Shalini, 2015). Moreover, EU is also developing the national strategies related to computer security indices and NIS directives are being put in place for countering this risk. However, the report of Law 360 states that the China is taking effective policy measures for reducing the cyber-security threats to the higher extent.

In 2016, the country has passed a new national security law which covers the information networks, telecommunication, E-banking, cloud computing, e-commerce

under the data localization procedures on the basis of which this data will not be transferred for storage to the international country. In this regard, for the cross-border transfer of data, the organizations would have to pass the data transfer policy from the government officials and approve it before taking further steps. Other attributes such as spam acts, computer indices, and smart grid have not been covered by this policy and a further notice from the government is necessary for covering these areas (Law360, 2016). In addition to this, the research of Jorge Binding and Kai Purnhagen indicates that consumer protection Acts in EU and China are similar to each other because of implementing nationwide strategies (Binding and Purnhagen, 2016).

In Malaysia, the broad ICT infrastructure development has taken place and the government has increased its spending in this regard to secure the e-banking efficiently (Go, 2016). Malaysia is being regarded as the earliest nation in South East Asia for enacting cyber-security policy and it has supported e-commerce, network infrastructure, and cloud computing as the main factor of its policy initiatives. It's cyber-security policies are mostly linked with national defense, public health sector and national image attributes which are out of the scope of this paper and still even after the implementation of these laws, Malaysia is being considered as less competitive with India and Canada to deal with its cyber-security issues (OECD, 2016). Much likely to EU, Australia has implemented a closed engagement between government, businesses, individuals, and the suppliers to protect the e-banking, e-commerce, and cloud computing and consumer protection acts and enforcing the laws that can meet the requirements nationally. In this way, the country is developing national level strategies to reduce its cyber-security threats to the higher extent (Turner, 2015); therefore, under the current studies and evaluations, it can be analyzed that the cyber-security policy implementation in China and EU are highly effective to combat the risks because they cover the large attributes under single policy review supported with a proper infrastructure of implementation. Although, U.S, India, and Australia are becoming strong nations on the map of the world still these countries need to work on effective policy implementation. Further, if policies of countries like Canada and Malaysia are seen individually then they are operating better but on comparison determinants, the countries need to look closer to achieving competitive advantage.

4.4. Result Matrix Table

Table 2 Result Matrix Table

Attributions	USA	EU	Australia	Malaysia	Canada	China	India
E-banking	IT security measures for a business, such as firewalls, updated antivirus protection, 2. Communications safeguarding software.[1]	Use of SWIFT Laws and Safe Harbour Fraud Intelligence Sharing System (FISS)[2]	E-Payments Code[3]	To avoid security breach Security counter measures such as encryption, firewall, SSL and SET[4]	Chip and Pin[5]	Bank Identifier Code (BIC)[6]	line encryption, branch connection, encryption, firewalls, digital certificates[7]
E-Commerce	U.S. Anti-Terrorist Laws & Int'l Business & Trade Creation of CSI ports8	The Electronic Commerce Directive (2000)9	Electronic Transactions Act 1999 (Cth) (ETA)10	The MEPS Secure Electronic Transaction (SET) Payment Gateway for payment mechanism for conducting secure bank/credit card payments over	Secure Sockets Layer (SSL), a protocol for managing the security of message transmission.12	The Chinese E-Commerce Law 13	The Consumer Protection Act, 1986 ("CPA") S.43A of the Indian Technology Act, 2000, ("IT Act") provides for the award of compens

				open networks 11			ation for failure to protect data.14
Cyber Protection Act	USCYBERCOM Comprehensive National Cyber-security Initiative (CNCI) 15	Cyber Information Sharing Partnership (CISP)16	Telecommunication Act 1997, Cybercrime Act 2001, Broadcasting Services Amendment (Online Services) Act 1999 (Cth)17	Electronic Transactions Act 200618	Personal Information Protection and Electronic Documents Act 200019	Cyber Intelligence — "Cyber Soldiers" Hunting for valuable information using viruses, Trojans, hacker software, network obstruction and paralysis. Fusing "swarm" tactics and severe serious viruses to paraly	The Information Technology (Amendment) Act, 200821

						ze the targeted network20	
Digital Signature	Electronic Signature in Global and National Commerce Act (ESIGN), Uniform Electronic Transactions Act (UETA)-adopted by 48 states[22]	EU Directive for Electronic Signatures (1999/93/EC), EU VAT Directive[23]	Capital Territory - Electronic Transactions ACT 2001, New SouthWales (NSW) - Electronic TransactionsACT 2000, Northern Territory (NT) - Electronic TransactionsACT 2000, QLD - Electronic Transactions (Queensland) Act 2001[24]	DIGITAL SIGNATURE ACT 1997[25]	Uniform Electronic Commerce Act (UECA), Personal information protection and electronic document acts 2000, c5[26]	Electronic Signature Law of the People's Republic of China[27]	The information technology Act 2000, Which was further amended in the year 2006 and 2008[28]
Identity Theft	Identity Theft and Assumption Deterrence Act[29]	Criminal Code[30]	The Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 1999, Financial Transaction Reports	Personal Data Protection (PDP) Act 2010 (Act 709)[32]	Personal Information Protection & Electronic Documents Act (PIPEDA) (2005) (S-4), An Act	Criminal Code Network Security Law[34]	Act 2000 (Section 66C - Punishment for identity theft)[35]

			Act 1988[31]		to amend the Criminal Code (identity theft and related misconduct), Electronic Operations Law[33]		
Privacy	Cyber Privacy Fortification Act of 2015[36]	EU's Data Protection Directive[37]	The Privacy Act 1988 (Privacy Act)[38]	Malaysian Personal Data Protection Act 2010[39]	The Privacy ActandPersonal Information Protection and Electronic Documents Act (PIPEDA)[40]	China's Consumer Rights Protection Law ("CRPL")[41]	The Privacy Protection Bill[42]
Computer Security Incidents	Cyber-security Act of 2015 Cyber-security Enhancement Act of 2014 National Cyber-security Protection Act of 2014, Cyber-security Workforce	European Network and Information Security Agency ENISA[44]	Telecommunications (Interception and Access) Act 1979 Privacy Act 1998 (amended 2014)[45]	The National Cyber-security Policy[46]	Personal Information Protection & Electronic Documents Act (PIPEDA) (2005)[47]	Draft Cyber-security Law (July 2015) Antiterrorism Law (effective January 2016) National	Information Technology Act of 2000 (IT Act) Privacy Rules[49]

	Assessment Act[43]					Security Law (July 2015)[48]	
Data security of cloud computing	Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Federal Information Security Management Act of 2002 (FISMA), and Children's Online Privacy Protection Act of 1998[50]	Data Privacy Directive and the future of EU cloud computing[51]	The Australian National Privacy Act of 1988 The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act The Australian Prudential Regulatory Authority (APRA) ---------- May 2015 Cloud Computing in Australia Market Report[52]	Cloud computing in Malaysia's Laws[53]	Personal Information Protection and Electronic Documents Act[54]	China's Cloud Computing Regulations[55]	Controller of Certifying Authorities (CCA)[56]
Smart Grid	The Energy Independence and Security	Directive 2001/77/EC,	The SGA[59]	ASEAN Smart Grid Congress[60]	Green Energy Act[61]	The Amendment of the Rene	IEEE Standards Association

	Act (EISA) of 2007[57]	Directive 2003/54/EC, Green Paper (2005), Directive 2006/32/EC, COM (2007) 723 final. Directive 2009/72/EC, Conclusions of the European Council of February 4, 2011. Commission Recommendation on Preparations for the Roll-out of smart meteri				wable Energy Law (2009). The State Electricity Regulatory Commission (SERC)[62]	(IEEE-SA)[63]

		ng systems (C/2012/1342) --- EC standardization mandate for smart meters (M/441) EC standardization mandate for electric vehicles (M/468) EC standardization mandate for smart grids (M/490)[58]					
Network	ProtectingCyber	The Netw	Cybercrime Act[66]	Communications	National Defense	Network	InformationTechn

Security Laws	Networks Act[64]	ork and Information Security Directive[65]		andMultimedia Act 1998 (‘‘CMA”)[67]	Act[68]	Security Law[69]	ology Act 2000[70]
Spam Act.	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[71]	Directive (**2002/58/EC)**on Privacy and Electronic Communications[72]	Spam Act[73]	Telecommunications Law and the Internet Access Service Provider (IASP)[74]	Canada’s Anti-Spam Legislation 2014 (CASL)[75]	Regulations on Internet email Services[76]	There is no law presently in India
Telecommunication	Telecommunications Act of 1996[77]	Telecommunications Act[78]	Telecommunications (Interception and Access) Act[79]	National Cyber Security Policy (‘‘NCSP”), Telecommunication Act 1950[80]	Telecommunications Act(Canada)[81]	TelecommunicationsRegulationsofthe People's RepublicofChina[82]	Telecom RegulatoryAuthorityIndian Act-1997[83]
Consumer Rights Protection Law	Federal TradeCommission Act, Federal Food, Drug, and Cosmetic Act, Fair Debt	Data Protection Directive, European General Data Protec	Australian Consumer Law[86]	Malaysia's Consumer Protection Act 1999 (CPA)[87]	Consumer Protection Act, 2002, S.O. 2002[88]	[4]China Consumer Protection Law (Amendments 2014)	[5]Consumer Protection Act of 1986 and National Consumer Disputes Redressa

	Collection Practices Act, the Fair Credit Reporting Act, Truth in Lending Act, Fair Credit Billing Act, and the Gramm–Leach–Bliley Act.[84]	tion Regulation 2014[85]				[89]	l Commission[90]
National Encryption Policy	Security and Freedom through Encryption (SAFE) ACT Secure Public Networks Act[91]	EU Data Protection Regulation[92]	Cybercrime Act 2001[93]	NA (Unable to find any specific Policy)	Criminal Code's Lawful Access Powers[94]	State Council Directive No. 273, Regulations on the Administration of Commercial Encryption[95]	Information Technology Act, 2000 National Encryption Policy, 2015[96]
Data Security Act	Data Security and Breach Notification Act of 2015[97]	EU Data Protection Regulation 2018[98]	Privacy and Data Protection Act 2014[99]	Personal Data Protection Act 2010[100]	Canadian Privacy Statutes Personal Information Protection and	No comprehensive, consolidated data protection	The Personal Data Protection Bill[103]

					Electronic Documents Act[101]	law in China [102]	

[1]http //www.cefims.ac.uk/documents/sample-120.pdf
[2]http //www.cefims.ac.uk/documents/sample-120.pdf
[3]vuir.vu.edu.au/1483/1/White.pdf
[4]http //www.icommercecentral.com/open-access/ebanking-in-malaysia-opportunity-and-challenges.php?aid=38622
[5]http //blg.com/en/News-And-Publications/Publication_4602
[6]https //assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf
[7]http //jsslawcollege.in/wp-content/uploads/2013/05/LAW-RELATING-TO-E-BANKING-IN-INDIA-%E2%80%93-AN-OUTREACH-CHALLENGE.pdf.
[8]http //www.cefims.ac.uk/documents/sample-120.pdf
[9]http //www.cefims.ac.uk/documents/sample-120.pdf
[10]vuir.vu.edu.au/1483/1/White.pdf
[11]http //www.ecommercemilo.com/2014/07/understanding-ecommerce-legislation-malaysia.html
[12]https //www.cgi.com/sites/default/files/white-papers/canada-cybersecurity-legislation-white-paper.pdf.
[13]http //search.proquest.com/openview/3de730959a0587033198b9b1d4bc0615/1?pq-origsite=gscholar&cbl=42517
[14]http //www.usibc.com/sites/default/files/Files/blog/LegalServices_Newsletter.pdf
[15]http //nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf
[16]http //www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf
[17]https //www.sans.org/reading-room/whitepapers/legal/concise-guide-australian-laws-related-privacy-cybersecurity-domains-36072.
[18]https //www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-related-policies-and-laws-malaysia
[19]https //www.cgi.com/sites/default/files/white-papers/canada-cybersecurity-legislation-white-paper.pdf
[20]http //chinascope.org/archives/6385/76
[21]http //www/cyberlawsindia.net/Information-technology-act-2008.html
[22]https //www.docusign.com/learn/esign-act-ueta
[23]https //www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/
[24]http //www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/
[25]http //www.wipo.int/wipolex/en/text.jsp?file_id=228678
[26]http //www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html
[27]http //tradeinservices.mofcom.gov.cn/en/b/2007-11-29/13694.shtml
[28]http //www.dot.gov.in/sites/default/files/itbill2000_0.pdf
[29]https //www.ftc.gov/node/119459
[30]http //www.ejtn.eu/Documents/THEMIS%202016/Semi%20A/Bulgaria_TH_2016_01.pdf
[31]https //ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf
[32]http //agc-blog.agc.gov.my/agc-blog/?p=1298
[33]http //laws-lois.justice.gc.ca/eng/AnnualStatutes/2009_28/FullText.html
[34]https //www.huntonprivacyblog.com/2011/11/08/new-chinese-legislation-includes-provisions-protecting-personal-information/
[35]http //thegiga.in/LinkClick.aspx?fileticket=KX1_Imk_gDs%3D&tabid=589
[36]https //www.law.cornell.edu/uscode/text/42/2000aa

[37]http //ec.europa.eu/justice/data-protection/reform/index_en.htm
[38]https //www.oaic.gov.au/privacy-law/privacy-act/
[39]https //core.ac.uk/download/pdf/41338677.pdf
[40]https //www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/
[41]http //www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf
[42]http //www.outsourcing-law.com/2011/07/2011-indian-privacy-law/
[43]http //www.isaca.org/cyber/pages/cybersecuritylegislation.aspx
[44]http //eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
[45]https //www.sans.org/reading-room/whitepapers/legal/concise-guide-australian-laws-related-privacy-cybersecurity-domains-36072.
[46]http //nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp
[47]https //www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf
[48]http //www.bakermckenzie.com/en/insight/publications/2016/11/final-passage-of-chinas-cybersecurity-law/
[49]http //www.wipo.int/wipolex/en/text.jsp?file_id=185998
[50]http //www.csoonline.com/article/2126072/compliance/compliance-the-security-laws-regulations-and-guidelines-directory.html
[51]http //njb.nl/Uploads/2014/4/Master-thesis-Bart-Schellekens.pdf.
[52]https //www.bluecoat.com/resources/cloud-governance-data-residency-sovereignty/australia-data-privacy-laws
[53]http //cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Malaysia.pdf
[54]http //www.servercloudcanada.com/2015/09/canadian-privacy-laws-canadian-cloud-primer-canadian-businesses/
[55]http //www.china-briefing.com/news/2016/07/12/weathering-chinas-cloud-computing-regulations.html
[56]https //www.dsci.in/sites/default/files/Discussion%20Paper%20on%20Policy%20&%20Legal%20Issues%20in%20Cloud.pdf
[57]http //onlinelibrary.wiley.com.sci-hub.io/doi/10.1002/wene.53/abstract
[58]http //onlinelibrary.wiley.com.sci-hub.io/doi/10.1002/wene.53/abstract
[59]http //www.smartgridaustralia.com.au/
[60]http //www.asean-sgc.com/
[61]https //www.eia.gov/analysis/studies/electricity/pdf/intl_sg.pdf
[62]https //www.eia.gov/analysis/studies/electricity/pdf/intl_sg.pdf
[63]https //www.dsci.in/sites/default/files/Discussion%20Paper%20on%20Policy%20&%20Legal%20Issues%20in%20Cloud.pdf
[64]http //www.isaca.org/cyber/pages/cybersecuritylegislation.aspx
[65]http //www.out-law.com/en/articles/2016/july/eu-network-and-information-security-directive-finalised/
[66]https //blog.appknox.com/glance-australias-cyber-security-laws/
[67]https //teknorus.com/my/cyber-security-law-and-framework-in-malaysia/
[68]https //www.cse-cst.gc.ca/en/inside-interieur/protect-protection
[69]http //www.mondaq.com/china/x/557154/Security/Comments+On+The+Network+Security+Law
[70]http //cyberlawsindia.net/
[71]http //www.pcworld.com/article/114287/article.html
[72]http //eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX 32002L0058
[73]https //blog.appknox.com/glance-australias-cyber-security-laws/
[74]http //www.rajadarrylloh.com/images/pdf/Tel12_Chapter-20_Malaysia.pdf
[75]http //eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX 32002L0058
[76]http //eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX 32002L0058
[77]https //www.fcc.gov/general/telecommunications-act-1996
[78]http //www.en.uke.gov.pl/telecommunications-act-77
[79]https //blog.appknox.com/glance-australias-cyber-security-laws/
[80]https //teknorus.com/my/cyber-security-law-and-framework-in-malaysia/

[81]https //www.fcc.gov/general/telecommunications-act-1996
[82]http //www.china.org.cn/business/laws_regulations/2010-01/20/content_19273945.htm
[83]https //ppp.worldbank.org/public-private-partnership/sector/telecom/laws-regulations
[84]https //www.ftc.gov/enforcement/statutes/federal-trade-commission-act
[85]http //www.hg.org/data-protection.html
[86]https //www.accc.gov.au/consumers/consumer-rights-guarantees
[87]https //www.consumer.org.my/index.php/complaints/rights/254-the-consumer-protection-act
[88]https //www.ontario.ca/laws/statute/02c30
[89]http //www.china-briefing.com/news/2014/04/08/china-introduces-new-consumer-protection-law.html
[90]https //www.ftc.gov/enforcement/statutes/federal-trade-commission-act
[91]https //fas.org/irp/congress/1997_rpt/h105_108p4.htm
[92]https //blogs.sophos.com/2015/01/08/5-things-you-should-know-about-the-eu-data-protection-regulation-even-if-youre-not-from-the-eu/
[93]https //www.ftc.gov/enforcement/statutes/federal-trade-commission-act
[94]http //www.loc.gov/law/help/encrypted-communications/canada.php
[95]https //www.lawfareblog.com/china-encryption-policy-and-international-influence
[96]www.cxotoday.com/story/indias-new-national-encryption-policy-underway/
[97]http //www.isaca.org/cyber/pages/cybersecuritylegislation.aspx
[98]https //heimdalsecurity.com/blog/prepare-for-eu-data-protection-law/
[99]http //www.legislation.vic.gov.au/domino/web_notes/ldms/pubstatbook.nsf/f932b66241ecf1b7ca256e92000e23be/05CC92B3F8CB6A6BCA257D4700209220/$FILE/14-060aa%20authorised.pdf
[100]http //www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf
[101]http //www.edrm.net/resources/data-privacy-protection/data-protection-laws/canada
[102]http //www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/china
[103]http //www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html

4.5. Answers of Research Questions

1- What are the basic types of threats within the cyber-security threat scenario for each country? Like threat actor's typology, motivational capabilities, response to countermeasures, for instance, the way China has framed its Cyber-security policy.

Every country is not facing the same level of different threats. The USA has lots of big corporations with gigantic databases of customers; ; therefore, this country's financial markets are facing the biggest cyber threat of data breach. Smart grid in the USA is also prone to cyber-attacks as they have not updated in last few years. Identity theft and scamming through spam is very common in India, China, and Malaysia, where a large number of people use the internet and most of them, are not aware enough of these threats. The financial situation of people in these countries also encourages them for this kind of illegal activities. Ransomware is one of the most basic threats within the cyber-security threat scenario for Canada, Australia and European countries where GDP is fairly high and lots of multi-national corporation have their databases.

2- Which organizations have the lead role in the cyber-security policy of each country?

The cyberspace in every country is enormous and there are lots of security issues associated with it therefore only a big corporation with huge resources can ensure the security of cyberspace. Moreover, cyber-security also requires the authority to monitor cyber services so that they can investigate any security breach and assess security vulnerability. Due to this reason, cyber service providers and federal government play the most crucial role in the development of policies. Cyber service providers indicate what kind of protection their services require from the law. Every country also develops a special federal department or program which evaluates the current situation and do research on various causes related to cyber-security all around the world to provide recommendations for cyber-security policy. For example, the USA has The Networking and Information Technology Research and Development (NITRD) Program which present the action plan for cyber-security.

3- What role is played by the law enforcement organization in the implementation of the cyber-security policy of the mentioned countries?

Cyber-security is not only about good policy and firewalls but is also about arresting offenders. It is the responsibility of law enforcement agencies to ensure the supremacy of law and implement it on ground level. The nature of cyber threats varies a lot, ; therefore, nature of laws also varies due to one organization can't enforce all laws. Some threats come under the jurisdiction of local government while other come under the jurisdiction of the federal government. In the USA, Federal Bureau of Investigation (FBI) has cyber-security department which investigates cyber-attacks and threats from overseas adversaries. Every state in the USA has its own police department which deals local cases of cyber-attacks. Similarly, in other countries including India, China, Malaysia, Canada, Australia, and European countries police department enforce the law on ground level. These law enforcement organizations arrest culprits after investigation to ensure that people feel safe while using cyber services.

4- How is the prioritization of the cyber threats done by each country? For instance, as per Strategic Defense and Security Review, 2010 of UK, cyber is the highest priority threat.

The threats to every nation differ because of several factors including its foreign policies, geographic realities, and political dynamics. The prioritization of cyber threats is done by analyzing previous cases of cyber-attacks. Recently, USA faced some attacks from Russian and Chinese hackers and authorities in the USA are expecting more attacks in near future; therefore, securing cyberspace from hacking attempts is the first priority in this country. Other countries also prioritize cyber threats according to the frequency of those threats. If a country is facing spamming and privacy violation threats more than other threats then these threats will get priority. The expected financial loss in case of any cyber threat also provides a way to prioritize threats. If a threat can cause extremely high financial loss or social disturbance, then countries focus more on eliminating those cyber threats.

Chapter 5

5. DISCUSSION OF COMMON ATTRIBUTES

E-Banking

The E-banking in the United States, India, and Malaysia are joined by the government policy to use IT security measures through which the organizations will be needed to create firewalls and antivirus to protect data. The policy also influences the companies to build software that can protect data. There is no specific fraud investigation policy in the United States as compared to EU in which Fraud Intelligence Sharing Systems (FISS), Society for Worldwide Interbank Financial Telecommunications (SWIFT) Laws and Safe Harbour are developed that are specifically developed to protect the fraud in the retail banks (Europa.eu, 2017).

Additionally, the results table in chapter four indicates that in Australia, E-payment codes are developed which identifies the ways through which terms and conditions between customers and banks should be set. A similar code related policy is also developed in the China named as Bank Identifier Code (BIC) for sending and receiving money through wire transfers in order to reduce the threat of fake payments between domestic and international countries. Canada does not hold detailed laws for e-banking rather a cryptic chip card named as Chip and Pin policy is used to transfer payments and

digital verifications and any individual not using this mode of the transaction will be considered as involved in fraudulent activities (Table 2 Results Chapter #4.4).

The approach to secure E-banking process depends a lot on the internal dynamics of a country (Malufu, 2013). Therefore related laws are very different in all seven countries. The focus of some countries like India and Malaysia is on encryption whereas the USA also has some tools and software to safeguard communication. The presence of well-establish laws for the security of e-banking indicates that it is a very important attribute of cyberspace security policy. In future, current encryption and software will not be enough to create a secure environment for E-banking because techniques of hacking and intruding are also evolving, ; therefore, it is recommended to keep improving policy according to the developing cyber technologies (Chertoff, 2008).

E-Commerce Law

The Anti-terrorist laws and International Business and Trade Creation of CSI ports have been implemented in the United States to secure the E-commerce related business transactions (Table 2 Results Chapter #4.4). At the Same time, EU, Australia, Canada, China, and India also Supports the E-commerce transaction by implementing laws such as the Electronic Commerce Directive 2000 in EU and the Electronic Transaction Act 1999 in Australia, Secure Sockets Layer (SSL) in Canada and the Chinese E-Commerce Law (Table 2 Results Chapter #4.4). In Malaysia, no Laws exist to support E-Commerce rather a secure electronic gateway is provided to the companies through which they can send and receive free payments through the internet. This network in the Malaysia is a strong and protected mechanism to secure the transactions and reduce the risk of fraud to the higher extent.

The protection under EU Law is stringent because it provides the harmonized rules for the customers and business and develops a secure connection (Europa.eu, 2017). In the same way, U.S also uses the secure connection gateways to reduce the fraud, but it does not provide the linked mechanism as EU. In India, the Consumer Protection Act, 1986 (“CPA”) S.43A of the Indian Technology Act, 2000, provides the organization with compensation when they have failed to protect the data which is a loophole in law because it creates room for fraud (Table 2 Results Chapter #4.4).

In countries like India and China, where a number of internet users are very high, it is crucial to have a policy which attracts investors and businessmen to utilize e-commerce without compromising the security of customers (Oak Ridge, 2011). E-commerce laws in all these countries are somewhat similar as their policies focuses on customer protection. The use of anti-terrorist law for the protection of E-commerce shows the importance of this cyber service. Consumer protection is important for E-commerce laws but it is not the responsibility of service providers only, customers also need to be held liable for irresponsible usage. It is a long shot because consumers can use service as per their own desires but if they held liable then it will become harder for scammers to get success and consumers will also show responsibility while using any E-commerce service (Garfinkel and Spafford, 2011).

Cyber Protection Act

The results table in chapter 4 has indicated that the each listed seven countries support laws for cyber protection which are designed by national authorities (Gustke, 2013). The Chinese protection management and EU's protection management comes at priority list such as creating the software and network paralysis for hackers and Trojan attacks in China and Cyber Information Sharing Partnership (CISP) in EU and Cybercrime Act 2001, in Australia are operating at approximately same mechanism for protecting against cyber-security at national levels (Table 2 Results Chapter #4.4).

The telecommunication act of Australia 1977 restricts the telecommunication transactions under a license and regulates the users to disclose the information on the board so that any hacker can be imprisoned for misconduct. The mechanism of Chinese Acts is very effective because it covers entire ways of data hacking and swam tactics before if anyone considers acting in a fraudulent manner. ; therefore, the policy mechanism under the cyber-security is effective among all countries because every country regulates the telecommunication channels through a regulated infrastructure and reduces the risks and threats associated with data hacks. However, the protection within the Canadian Personal Information Protection and Electronic Documents Act 2000 and Malaysia can be considered as limited as compared to China, EU, US, India, Australia

because Canada and Electronic Transactions Act 2006 of Malaysia do not support the emergency initiatives in the case of any issues in place (Table 2 Results Chapter #4.4).

The dissimilarity in the laws of cyber protection is clearly evident from the policies of all these countries. Australia has not changed its policy from a long time. It is still using broadcasting services and telecommunication acts of the late 1990s. India amended its telecommunication act in 2008 but still, it is not up to date. On the other hand, CISP (Cyber-security Information Sharing Partnership) of the EU is more up to date. This system uses real-time information sharing for the cyber protection. (NSSC, 2016) It is important for other countries to get inspiration from better laws, policies, and systems in order to make their cyberspace more secure. It is recommended to improve the communication between different private industries and government departments to improve the information sharing system. Some laws can help to improve this communication by making it the responsibility of concerned authorities and organizations to sharing that information which can help to improve cyber-security in one way or another (Chertoff, 2008).

Digital Signature

The digital signature policies are initiated for reducing the fraud of faking the identities (Barker, 2006), and each of listed countries supports the digital signature laws to help reduce the risk of frauds. The Australian laws named as Capital Territory - Electronic Transactions ACT 2001, New South Wales (NSW) and Electronic Transactions ACT 2000 for a digital signature is most effective as the country has developed a separate law for each of its territories (Table 2 Results Chapter #4.4).

The Electronic Signature Law of the People's Republic of China provides a private infrastructure between two individuals in contact through which people living far off can confirm the identity of each other and the threat of fraud is reduced (Blythe, 2007). Under EU law of EU Directive for Electronic Signatures (1999/93/EC), the data protection is ensured by providing the certificates to the users and generates E-signatures which first identifies the signatory and then process the transactions. This mechanism is less risky and Indian law named as the Information Technology Act 2000 also promotes

the same kind of mechanism in which person to person communication is ensured thereby develops a protected connection (Table 2 Results Chapter #4.4).

Policies for the digital signature are very similar in all these countries but Malaysia is lagging in this regard as it is still following the digital signature act of 1997. The USA, EU, Australia, Canada, and India have multiple laws to keep the standard of digital signature high enough to protect the digital content. Digital signatures are mostly used by big organizations as there is not any infrastructure and law to allow individual users to have their own digital signature to get the acknowledgment of their digital property and sign contracts more conveniently. The main issue in this regard is that digital signatures can be copied with great precision which makes them vulnerable to security risks. Some new technologies like QR codes and the cryptographic signer are making digital signature more secure and user-friendly (Crypto mathic, 2017). The cyber-security policy of every country should encourage the use of advanced and user-friendly technology to make this cyber service more useful and safer.

Identity Theft

The Identity theft in EU is protected by the criminal code in the EU which is developed by the collaboration between national and territory based authorities, but it still requires the privatization so that identity theft in private and public level can be reduced (Robinson, 2011). The Australian Theft, Fraud, Bribery and Related Offences Act 1999, Chinese Criminal Code Network Security Law, Malaysia's Personal Data Protection (PDP) Act 2010, Canada Personal Information Protection & Electronic Documents Act (PIPEDA) (2005) (S-4), and U.S (Identity Theft and Assumption Deterrence Act) identity theft laws are providing the provisions under which the likelihood of fraud can be reduced to the greater extent as they deal with the mechanism of getting personal information of individuals and provide them security under the policy (Table 2 Results Chapter #4.4). Each country is supporting the laws for protections against identity theft, and U.S and Indian law provisions are seemed to be effective because they are providing policy support through detailed prohibitions and specifying penalties such as 20-25 years of jail (Stroup, 2016).

The EU, Australia, Canada, and China are using criminal code to prevent identity theft. The policies of these countries for identity theft are very similar. India does not have a comprehensive law for this attribute but they have a clause in its IT Act of 2000 which declares any entity a criminal if it imitates any other entity's identity in the cyberspace. Personal data protection laws can also cover this attribute; therefore, Malaysia has only personal data protection act tackle identity theft issues. All countries have a similar law for identity theft but there is still need to develop a comprehensive code because lots of internet users make accounts on different social media websites with the name of different celebrities. Law does not come in action unless someone files a report. Moreover, social media websites also don't go in detail to verify the identity of its users as it can reduce their number of users and also there is no law which compels them to make ensure the verification of all users. Users also hesitate to share their personal details fearing identity theft. There is need to make efforts to solve this dilemma through legislation and advance technology (Hoffman and McGinley, 2010).

Privacy

The privacy protection act is developed by each of the seven countries including U.S, EU, Australia, Malaysia, Canada, China, and India but these laws are intended towards different kinds of privacy protections. For example, results section of Chapter 4 identifies the Cyber Privacy Fortification Act of 2015 U.S and the Indian Privacy Protection Bill provide penalties i.e. imprisonment or fine to the companies that have failed to provide the required level of security to the consumers whereas the China's Consumer Rights Protection Law ("CRPL") provides a loophole for fake product purchase and sells recognition because specifying the professional customers (can buy number of products with reduced cost of goods sold) and normal customers (Wessing, 2016). EU' Data protection directive, Australia's Privacy Act 1988, Malaysia's Personal Data Protection Act 2010, and Canada's privacy protection PIPEDA acts are operating under private and public sector privacy protection laws (Table 2 Results Chapter #4.4). The EU's privacy protection is considered as adequate level personal protection and operates under user as owner mechanism which makes it specifically intended act for the personal data privacy.

Australia is using its old privacy act of 1998. Malaysia is using its personal data protection law for privacy protection too. This same law is also used for identity theft in Malaysia. Similarly, Canada has same law of PIPEDA for identity theft and privacy. Privacy laws in all these countries vary a lot due to the difference of awareness in people. In the USA, EU privacy laws are very strict as compared to Malaysia, China, and India. It is challenging for all countries to protect privacy while giving enough space to law enforcement agencies to access data for the investigation of different cyber-security cases. Latest technologies and cyber services also enable the service provider to access the location of users which makes it more challenging to devise a balanced privacy law (Kulesza, 2013). It is recommended to bring law-enforcement agencies, society leaders, and cyber service providers together to discuss the issue of privacy in order to make a more comprehensive and useful privacy laws (Garfinkel, and Spafford, 2011).

Computer Security Incidents

Cyber-security is incomplete without addressing computer security incidents (Trout, 2007). In the U.S, Australia, Canada, China and India, the laws are operating for protecting the computer security incidents. In the United States, the detailed laws have implemented to reduce the computer security threats such as Cyber-security Act of 2015, Cyber-security Enhancement Act of 2014, National Cyber-security Protection Act of 2014 and Cyber-security Workforce Assessment Act. China is stricter as it has anti-terrorism law for computer security incident. Australia is using old laws, telecommunication act 1079, to prevent computer security incident. Australia has also sung privacy laws for this purpose like Canada (Table 2 Results Chapter # 4.4).

Comparatively, in EU, the European Network and Information Security Agency ENISA is developed which monitors the computer security issues and provides the situation based solutions to resolve the issues. Similar is the case with the National Cyber-security Policy of Malaysia, which involves the resolution of computer security issues with respect to Fraud, Malicious codes, and hacking and denial attacks (Hashim, 2008). In this regard, the fraud investigation is an important factor in entire states, and the policies are produced by specifically targeting the hackers and vulnerabilities are reduced

through using the preemptive tools for national consumer securities. Draft Cyber-security Law (July 2015) and Antiterrorism Law (effective January 2016) of China is under process to develop detailed security policies and to decrease the possibility of cyber-attacks in China. In India, IT laws are used to tackle computer security incidents (Table 2 Results Chapter # 4.4). Computer security incident is one of the most challenging attributes because it encompasses several other attributes like network security, data security, and privacy (Chertoff, 2008).

Data Security of Cloud Computing

Similar to the Computer security incidents, the data security of cloud computing also requires comprehensive and detailed laws for protecting the data of consumers (Tajts, 2012). Cloud computing is secured in the United States by using the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Federal Information Security Management Act of 2002 (FISMA). (Table 2 Results Chapter #4.4). The Chinese Cloud Computing Regulations and EU's Data Privacy Directive, data security cloud computing regulations are associated with global perspectives, and the stringent rules (such as not transferring the personal data of an individual from one country to another with the consent of individual) are imposed (Computerworlduk.com, 2015).

The Australian National Privacy Act of 1988 and Cloud computing laws in Malaysia provides the data security by restricting the companies to not disclose the personal data of individuals under direct marketing. In contrast, the India's Controller of Certifying Authorities (CCA) has provided a specific infrastructure based tool to operate through which DN-specific users name are developed, and data is encrypted under codes (Table 2 Results Chapter #4.4).

These authorities of India are combining the digital signature codes with cloud computing and reducing the risk of frauds. The Personal Information Protection and Electronic Documents Act of Canada provide more authority to the user and help them to monitor their personal cloud data and complain to the regulatory authority in the case of frauds (Table 2 Results Chapter #4.4). Similar to US, Australia, and Malaysia, the companies in Canada need to protect consumer data by taking consent from the

individuals before transferring their data from one platform to another. Security of cloud depends on the whole infrastructure. Any weakness in any part of the infrastructure can make the whole system vulnerable (Yeluri and Castro-Leon, 2014).

Smart Grid

Smart grids allow countries to monitor and control its power generation, distribution, and protection. (NIST, 2010) These grids are becoming popular worldwide. All seven regions except Malaysia in this project has some laws for securing the digital data used in the energy supply network. In the United States, the Energy Independence and Security Act (EISA) of 2007 hold more information about using renewable energy resources rather specifying the digital data protection (Table 2 Results Chapter #4.4). This law has the deficiency in specifying the detailed consumer data protection (Skopik and Smith, 2015). Similar is the issue with Malaysia's ASEAN Smart Grid Congress in which the Congress has provided a detailed security such as technical research and site visits, but it did not provide the details of tool using the digital security under smart grids. On the other hand, EU's Directive 2001/77/EC, Green Paper (2005), Directive 2006/32/EC, COM (2007) 723 final and Directive 2009/72/EC, Australia' SGA Policies, Canada's Green Energy Act, and China's Amendment of the Renewable Energy Law (2009) are providing the detailed mechanism through which policies should be implemented, and the data should be protected in order to reduce the fraud cases (Table 2 Results Chapter #4.4).

These countries are providing the changes in energy supply infrastructure and information technology that will lead to secure the data and provide people a secure connection of using utilities. In addition to this, EC standardization mandate for electric vehicles (M/468) in the EU is much effective to control fraud through the use of electronic vehicles in which consumer data is secured by using encryption techniques (Flick and Morehouse, 2011). India is also using IEEE standards to protect its smart grids (Table 2 Results Chapter #4.4).

Network Security Laws

The security of devices in any network depends on the standard followed by the administrators of networks (Ghosh, 2002). EU holds directives to provide regulation policy guidance for network security, and entire other states are operating with their states associated laws. The Cybercrime Act of Australia detects the frauds by creating the personal information alerts and the credit files checking systems (VEDA, 2016) which are approximately similar to the Communications and Multimedia Act 1998 of Malaysia in which fraud activities are detected by specifying the network identities and informing the regulated authorities with the name of fraudsters (Table 2 Results Chapter #4.4).

The U.S Protecting Cyber Networks Act, India's Information Technology Act 2000, China' Network security laws and Canada's National Defense Laws are operating under the network security protection by listing specific areas of protection such as phishing, Children online privacy, accessing the information and denial attacks, concealing and destroying the information secured on the networks (Table 2 Results Chapter #4.4). The acts of these states provide the data protection networks, but still, most of the countries such as United States, Australia, EU and Canada are lagging in providing IoT security such as to collect the individual data at a secured network place (Talbott, 2016).

Spam Act

The countries such as U.S, EU, China, Canada, Australia, and Malaysia have provided the policy provisions for Spam acts except for India where there is no law developed to reduce the Spam activities. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 of U.S reduces the threat of fraud by restricting the use of deceptive subject lines for marketing the products to the customers (Table 2 Results Chapter #4.4).

Every commercial message is checked against the certain rules and so that the consumer data is not used for ineffective purposes (Westby, 2004).In comparison, the companies in EU are charged with Directive (2002/58/EC) on Privacy and Electronic Communications which is a certain level fee for electronic communication, and the fee form requires the details of the underlying transaction (Europa.eu, 2017). Similarly, the

Anti-Spam legislation of China and Canada's Anti-Spam Legislation 2014 (CASL) is providing the secure marketplace by issuing the detailed notice of regulatory standards and violations to the companies. Australia also has similar spam act for this Cyber-security issue (Table 2 Results Chapter #4.4).

There are several cyber-security issues due to which spamming goes unnoticed. It is also because consumers have accepted spamming as one of the side-effects of using the internet and they do not bother much about it (Trout, 2007). The absence of any well-established law against spamming in the country like India indicates the ignorance of authorities. The increased awareness about spamming and filtering tools has also reduced the impact of spam, but still, this security threat affects thousands of internet users all over the world. It is also challenging to distinguish spamming from mass marketing (Chipman, 2016). The law against mass marketing can trigger a reaction from business organization. It is recommended to develop a standard to define spamming and develop a law which prevents consumers from spam while allowing business organizations to promote their business freely.

Telecommunication

In the United States, the telecommunication law provides the consumer data protection under the programming security and makes the rule for the companies to encounter the data hacking threats in respect of increased competition. National Cyber-security Policy (''NCSP") Telecommunication Act 1950 of Malaysia and EU's Telecommunications Act develops the policy initiatives through infrastructure change and implementing greater national control policies. They have developed an integrated information system approach through which the companies will share the details of the transaction with government oversight bodies, and the regular monitoring will be undertaken (Mosti.gov, 2016).

The Telecommunication Act of China, Australian Telecommunications (Interception and Access) Act, and Indian Telecom Regulatory Authority Indian Act-1997 are operating approximately on the similar mechanism by separating the roles of government and organizations in telecommunication data security (Table 2 Results Chapter #4.4). The Telecommunications Interception and Access Act of Australia restrict the access of

stored communication without authorization. Canada has similar telecommunication act to address related issues.

Since telecommunication is one of the oldest cyber services, ; therefore, its policies are also well-developed and more standardized as compared to policies for other cyber services (Ghosh, 2002). Almost every country has its own telecommunication act which is every similar to each other. The arrival of advanced technologies like 3g and 4g are improving users experience but these technologies are also demanding amendments in the telecommunication acts. The security of telecom service is now more crucial than ever as advanced technologies has also increased the number of users and the sensitivity of their activities has also increased (Chen and Gong, 2012).

Consumer rights protection laws

U.S, EU, China, Canada, Australia, India, and Malaysia are having policies in place for consumer rights protection as laws. EU and China's consumer protection laws are much similar to the privacy laws described above under which the organizations are restricted to misuse the personal data of the consumers and cannot the personal data without the consent of individuals to reduce the likelihood of misconduct and fraud. India's Consumer Protection Act of 1986 and National Consumer Disputes Redressal Commission uses the mechanism of Prima facie to identify and detect fraud and protects the consumer rights through allegations whereas the Malaysia's Consumer Protection Act 1999 (CPA) has implemented a service fee on consumer goods which are aimed at developing technological change for consumer protection in order to reduce the unfair trade of their personal data and the liabilities will be imposed upon the companies using it (Consumer.org.my, 2017). On the other hand, U.S has provided the detailed laws through which it protects the consumer rights such as Federal Trade Commission Act, Federal Food, Drug, and Cosmetic Act, Fair Debt Collection Practices Act, the Fair Credit Reporting Act (Table 2 Results Chapter #4.4), differentiate between each determinant of consumer data threats in order to provide a secure infrastructure. Canada developed consumer protection act is 2002 which is still in use for the protection of consumers' rights.

Consumer rights include privacy protection and data security of consumers, ; therefore, most countries use these two laws for consumer rights (McCann, 2012) but the USA and Australia have more effective policy regarding consumer law. They have a law to protect consumers from any kind of fraudulent activity from any individual or organization which can affect the consumer experience negatively. It encompasses food, drugs, billing, and debts. It is recommended to integrate general consumer rights laws with the laws for the protection of rights of consumers in cyberspace. Sharing and publishing misleading content is also a violation of consumer rights but it is very challenging to implement the law to prevent sharing of content especially in this era of social media. A policy should be developed to protect customers' right without affecting their freedom of expression (Jasper, 2008).

National Encryption Policy

In the United States, the stringent data encryption policies under Security and Freedom through Encryption (SAFE) ACT have been put into place which ascertains that after every fifteen days the government regulatory authority will conduct the review of encryption software and the confidentiality level will be identified (Table 2 Results Chapter #4.4).

In contrast, the Chinese Regulations on the Administration of Commercial Encryption has implemented an industrial based policy on the basis of which an encryption chip will be attached to the mobile phones and the computerized systems through which the risk of fraud will be reduced by encoding the data at the first place where it is generated rather waiting for a fifteen days' time (Segal, 2016). The Information Technology Act, 2000 National Encryption Policy, 2015 of India is considered to be ineffective because it required storing the encrypted data for 90 days which increases the threat of hacks and criminal activities (Shankar, 2015). EU's Data Protection Regulation, Australian Cybercrime Act 2001, Canada's State Council Directive No. 273 has provided a global mechanism for data encryption and authority of amendment rest to the Ministry. However, in Malaysia, there is a need for data encryption policy development as no policies have been developed in the country yet (Table 2 Results Chapter #4.4).

National encryption policies are one of those cyber-security attributes which have been neglected by the majority of countries. Global encryption standard can help to improve the quality of encryption in all countries but it is very difficult as a huge chunk of data has already been encrypted and it becomes very difficult for any organization to change it encryption policy abruptly. The national encryption policy is crucial to access how a country protects its cyberspace. It is recommended to have a policy which allows service providers to encrypt data easily while providing adequate safety to users and identity-based encryption is one way to move forward (Chatterjee, 2014).

Data Security Act

The data security laws are implemented by every country varies with its GDP, population and public awareness (MacKinnon, 2012). The data security act and Breach Notification Act of the United States have provided the suggestions to educate small and large organizations for data security and develop nonbinding best practice tool for online transactions. The frauds, in this case, will be detected by keeping track of the companies' activities and the data usage will interfere in the case of any criminal acts. The Privacy and Data Protection Act 2014 of Australia stipulates the companies to provide consumers with data protection forms and communicate take the consent of consumers for sharing their data otherwise; the companies will be in breach of confidentiality (Business.vic.gov.au, 2016). In Canada's Criminal Code's Lawful Access Powers and India's the Personal Data Protection Bill, similar consent policies have been implemented on the companies with an additional requirement of compliance agreement in Canada and disk imaging in India are implemented (Table 2 Results Chapter #4.4). Even being an advanced country, China does not hold any specific law about data security act. The European Union has well-developed laws in its data protection regulation to tackle data security issues (Table 2 Results Chapter #4.4).

In the case of any data security issue in China, other laws like criminal code can be used to solve the issue but it needs a proper policy to protect data of individuals and organization. Data security is one of those attributes of Cyber-security policy which got serious attention in near past; therefore, all big countries including USA, EU, and Australia have up to date acts and regulation for data security. Data security is also

somewhat related to the privacy therefore in some cases privacy laws can also be implemented to deal with data security cases but all cases of data security can be dealt with privacy laws. This is one reason for China to not have a special law for data security. Authorities may not have realized that data security and privacy are different attributes. There is a need to define and categorize data security and data privacy separately so that special law can be developed to make the digital data more secure (Hijmans, 2014).

5.1. Result Summary Table

Table 3 Result Summary Table

Attributions	USA	EU	Australia	Malaysia	Canada	China	India
E-banking	USA has best policy for e-banking supported by government policies	Only FISS is responsible for E-banking security	Developed e-payment codes	Focus only on encryption	No comprehensive laws	Bank identified codes are used for e-banking security	Focus only on encryption
E-commerce	Anti-terrorist law is used	Electronic Commerce Directive 2000 is used, which is old for recent times.	Old laws like Electronic Transaction Act 1999 are still in policy which may not e enough for modern times	No comprehensive laws	Canada has best policy for E-commerce	China has specific law for E-commerce	India use different laws to protect E-commerce but there are no specific laws
Cyber Protection Act	CNCI is responsible for cyber protection	EU and China has best policy with multiple laws and security measures	Telecommunication law is used for cyber protection	Its policies does not support emergency initiatives	There is no policy to tackle emergency situation	EU and China has best policy with multiple laws and security measures	IT act is used which indicate there is no special law.

Digital Signature	Multiple laws are there for digital signature	It has directives for electronic signature but they need upgrading	Australia has best policy and laws	Its lagging with old laws of 1997	It has multiple laws but there is no special law.	China has private infrastructure	Same IT Act of 2000 is also used for this attribute
Identity Theft	USA and India has best policy in this regard	Only criminal code is used, there is no special law.	Personal protection laws are used, there is no special law.	Personal data protection is protecting identity theft.	Only criminal code is used, there is no special law.	Only criminal code is used, there is no special law.	USA and India has best policy in this regard
Privacy	USA give punishment for inadequate security but policy need improvement	EU has best policy for privacy protection	Privacy act of 1988 is still in use which is not good enough for modern times	Personal data protection is also used for privacy protection	Canada policy is similar to the policy of Malaysia	China consumer protection law has loopholes	India gives punishments but policy is not very effective
Computer Security Incidents	USA has most comprehensive laws and best policy for this attribute	EU also has well-developed system with ENISA	Australia is using old laws	Its policy varies with the nature of incident	Canada is using PIPEDA for this attribute too.	China is using anti-terrorism law for this attribute	India has no better answer then IT law for this attribute.

Data Security of Cloud Computing	USA has several laws to protect its cloud computing infrastructure	EU has under-developed policy	Australia has several laws and it has best policy as compared to other countries	Malaysia has special laws for this one.	Canada is using personal protection policies for this attribute too.	China policy has global perspective	India is providing infrastructure through CCA
Smart Grid	No special laws for smart grids but other laws EISA provide some guidance	EU has more specific and best policy for smart grid.	Australia also don't have any special law,	ASEAN is used to get directions	No special law, green energy act is used for this attribute	Renewable energy laws are used, no special law present	Like EU, India also follow some IEEE standards
Network Security Laws	USA has special laws for this one	EU has special directives but its policy is still lagging	cyber-crime laws are used to handle any security issue of this category.	Using old acts of 1998	National defense act is used, it means there is no special law	China has special law and has best policy in this regard	IT act is used for this attribute too
Spam Act	USA has several laws to protect users from spam.	EU also has well-developed infrastructure to control spam	It has special spam act	No special laws. Telecommunication act is used for this attribute.	Canada has best legislation in this regard.	China is using old regulations which was used for email protection	No special law in India

Telecommunication	There are special laws but they require modification.	Old telecommunication act is in practice	Australia has best policy with interception and access laws	Using old laws	Canada also has special act	China also has special laws for this one	Old laws are still in practice
Consumer Rights Protection Law	USA has best policy to protect the rights of consumers	EU developed law recently in 2014	General consumer law is in practice	Old law of1999 is in practice	Canada has special law but it requires amendment	China amended its laws in 2014 to improve them	Using old laws
National Encryption Policy	USA has best policy in this regard with SAFE	Data protection act is used for encryption	No special laws	Basic criminal codes are used	Canada has global mechanism in its policy	China has industrial based policy	India has special laws but they are considered ineffective
Data Security Act	USA has a modern policy which is very effective.	EU has most advanced and best policy for this attribute	Privacy laws are used	Personal information policies are also used for this attribute	Malaysia, Canada are also using personal information protection policy to secure data	No special laws as criminal code is used	Personal data protection is used which required modification

5.2. Summary

There are several attributes of cyber-security which plays a critical role in protecting the cyberspace. The most significant attributes among them are selected to compare the policies of different countries. Some countries are handling some attributes better than others. It indicates that policy of one country cannot be termed as best but it can be said that a certain country has the best policy for the given attribute. For example, the USA has the best policy for electronic banking which is supported by the government but Canada has best policy for E-commerce and Spam Act. China and EU have several laws and security measures for cyber protection act; therefore, these countries' policies can be followed for cyber protection act. The European Union also has the best policy for privacy, data security and smart grid. The USA is providing the best approach to develop the best policies for consumer rights, national encryption and identity theft. India also has a well-developed policy for identity theft. The policy of Australia can be followed by the digital signature, telecommunication and data security of cloud computing. It indicates every country has its own strengths and weaknesses when it comes to cyber-security.

5.3. Recommendations

The cyber-security policy should be flexible to allow the state to improve it with time as the technology advances. Every country focuses on protecting its own cyber space which allows hackers and intruders to violate cyber space of any country while sitting in any other country. The policy of a country should also prevent any person to violate the cyber-security of any other country while sitting in it or using its cyberspace. In this way, hackers will find difficult to hack or intrude.

It is recommended to all countries that they should study the policies of other countries and get inspiration and include issues related with their context. There is nothing wrong in it and this approach can help to develop a comprehensive and effective policy.

One of the attribute; E-banking has to developed cyber technology by improving the policy to reduce the threat of any hackers; therefore, the development of E-commerce laws is significant for consumer protection, and the responsibility of protections is not only for the service provider. In cyber protection act, the evolving information sharing

system should improve the communication among all private and governments departments. Regarding the digital signature, each country must be supported this technology to keep the digital content safe. For the identity theft, there is a requirement to improve technology and legislation that encourage users for sharing their identity, increased meeting between decision makers and service providers; society leaders lead to more global for applicable privacy laws. The development of data security in cloud computing infrastructure eliminates weaknesses in information security system. It is recommended to improve standards network security law in some countries such as USA and EU, Canada's Internet Of Things security policies have deficiency to gather the personal data in safe place.

Nowadays, variance in telecommunication infrastructure between states that make the security of telecom service is a critical issue especially when increased users and activities. ; therefore, other countries should support in increasing the efficacy of their communication infrastructure to find the solution. The publishing data privacy of consumer rights is a huge issue particularly in the social media area, for this reasons It is recommended to find a new approach that protects privacy consumer.

The growth of international laws in data protection area, it is recommended to include a policy which permits service providers easily encrypt data and enough security to usage, and identity-based encryption is one of them. One of the sensitive issues is data security act in cyberspace; the security classified data and privacy security separately. Consequently, the developing special law makes digital data much secure.

All the recommendations mentioned above obtained after studying and comparing many of the results through papers published in this regard indicate the need to consider seriously the development of unified legislation that contributes to raising and developing the use of cyberspace and this contributes to reducing the disparity between countries in the infrastructure.

CHAPTER 6

6. CONCLUSION

Cyber-security is one of the significant factors in any country's development. Responsible countries develop special policies to make cyberspace safe and secure for all users in their country. Cyber-security is important because every private and public organization use cyberspace at some level and compromise on cyber-security can cause serious loss of revenue and stress in society. Cybercrimes can even compromise the national security, ; therefore, it is important to deal with such crimes vigilantly. There should be well-established laws to tackle cyber-crimes but it is important to identify major cyber-security issues so that a comprehensive policy can be developed (Bayuk, 2012).

Stakeholders of cyberspace include users, service providers, business organizations (including all those small, medium and multinational organizations which use the internet for any business operation), state and government of the country. All stakeholders play their role in developing a policy for cyberspace security but government plays the central role in developing and modifying the policy. A comprehensive policy addresses all issues related to the cyber-security. Some most common attributes of cyber-security policy include E-commerce. E-banking, Cyber Protection Act, Digital Signature, Identity Theft, Computer Security Incident, Privacy,

Data Security in Cloud Computing, Smart Grid, Spam Act, Telecommunication, Consumer Rights Protection Law, National Encryption Policy, Data Security Act and Network Security Act. Every country should address these attributes while developing their Cyber-security policy.

Seven regions Australia, USA, EU, Canada, China, India, and Malaysia are selected for the examination of these common attributes. These countries are selected because they have a large number of internet users, well-developed IT infrastructure and a comprehensive cyber-security policy for most of these common attributes. These countries have enough resources available on the internet about its policies, ; therefore, these countries were suitable for this research study. These countries policies showed serious similarities in some of its policies. The policy to tackle security telecommunication issues was very similar. Some policies are very different. The policies for cloud computing data security are different. The USA, EU and Australia have an relatively better policy for data security in cloud computing as compared to policies of Malaysia, China, and India. In India, Enterprises such as Ashok Leyland, Tata Elxi, Bharti, Infosys, Asian Paints, and Maruti are utilizing cloud computing. Approximately,1,500 Enterprises in India have been used (voice-chat-data) cloud-based on communication services by sellers such as Cisco WebEx and Microsoft, and US government extends that in the vicinity of 2010 and 2015, its spending on distributed computing will be at roughly a 40-percent yearly development rate (CAGR) and will pass $7 billion by 2015 (Lori M. Kaufman, IEEE Security & Privacy, 2009). Consequently, developed countries are embracing new technologies faster than developing countries.

Some attributes are linked with each other such as Data Security and Privacy are related to each. These attributes can be addressed through one single policy or law. Some countries use one policy to address multiple threats. For instance, Canada has criminal code to deal with identity theft and this code is also part of national encryption policy. Since some countries have multiple laws and acts for single attributes. For example, Digital Signature Law in Australia has used many laws which are Electronic Transactions ACT 2001, New South Wales (NSW) and Electronic Transactions ACT 2000 (Chapter # 4.4 Results).It shows their concern toward that specific attribute. For

instance, in EU there are several directives for smart grid which indicate that the technology of smart grid is thriving in this region and stakeholders are taking interest in it.

It has been observed that every country has its own way to secure its cyberspace. Their priorities differ with the political situation, economic condition, and awareness of users. In developed countries like USA, Australia, and EU, privacy and data security are taken very seriously and they have a very strict policy for these attributes. In light of customer feedback and various claims asserting serious security violations, the act incorporated an arrangement gone for ensuring consumer protection (McKim, 2001). Some laws protect people from cyber-attacks but these laws can also prevent law enforcement agencies to investigate different crimes more freely. The law enforcement agencies require special access to some data for investigation but they cannot be allowed to access any individual's or organization's data without any serious reason. Every country is addressing these issues in its own way. The pressure from the general public and business organizations play an important role in this regard. It indicates that it is not easy to develop a policy which addresses all issues associated with it. Countries should also get assistance from the policies of other countries.

The policy of a country for cyber-security also affects its economy. Investigations concerning the stock value effect of digital assaults demonstrate that recognized target firms endure losses of 1%-5% in the days after an assault and for the medium New York Stock Exchange company, value drops of these sizes convert into shareholder losses of between $50 million and $200 million (Cashell et al.,2004). Business organizations can work freely in a country which provides adequate security and freedom to all users. It can increase the imports of a country through increased investment in the various business markets through different cyber services. Governments also take assistance from the private sector to build a more user-friendly and powerful policy so that it can attract a maximum number of people to use their cyberspace for business (Gallaher et al., 2008).

It is also a fact that it is not enough to develop a policy only. The government should have strong law enforcement agencies to implement its policies otherwise good policies

are not going to provide all its benefits. The policy should develop after reviewing the opinion of all major stakeholders including law enforcement agencies. It can help the government to implement its policies relatively easily (Bayuk, 2012).

The development of a comprehensive cyber-security policy is the first step to creating a secure cyberspace. These policies are providing the base for all efforts of a country to eliminate all cyber-security risks; therefore, all countries should have a department to develop and access its policies. For instance, in the USA according to FBI official website (https //www.fbi.gov/investigate/cyber) the developing association with other federal agencies offices, including the Department of Defense, the Department of Homeland Security, and others—which share comparative concerns and resolve in battling cybercrime. All these common attributes are very important for the cyber-security. Cyberspace in any country cannot be secured without the development of a wide-ranging policy for all these attributes. If all countries agree on these attributes and develop a global policy for the cyber-security, then the cyberspace can become more secure.

6.1. Limitations

This study uses literature review to find out most common attributes for the cyber-security policy. Several research papers and cyber-crime cases were reviewed to develop a comprehensive list of common attributes. One limitation of this research is that no questionnaire was used and no interview was conducted to get the opinion of professionals in different countries. The comprehensive interviews with some professionals in selected countries could help to make a better list of common attributes. The time constraints and limited budget prevented to conduct interviews or use a questionnaire. The inclusion of more common attributes could make the research work more comprehensive and time-consuming.

Only public documents of selected countries were used to get the information about different policies of selected countries. The latest documents of some countries were not available on the official websites of those countries. For instance, there was no document available for the spam act law in India. Similarly, national encryption policy of Malaysia was not available on any official website of the country. On the ground level, there can be some laws and policies to protect cyberspace.

The cyber-security policies of only seven regions (USA, EU, Australia, Malaysia, Canada, China, and India) are examined. There are lots of other countries with a large number of internet users and well-established IT infrastructure. There were different issues to avoid those countries. For example, Japan and South Korea have more than 115 million inter users. More than 90% of this country's residents use the internet. Public documents of this country and policy statements were available in the Japanese and South Korea languages; ; therefore, it was not possible to examine cyber-security policy of Japan and South Korea without the assistance of expert translator which could cause time and budget problems. It is a limitation of this research that only policies of a selected number of countries are examined. Moreover, the discussion and conclusion of this research are qualitative in nature. This type of research is subjected to biases which are another limitation of this research.

6.2. Future Research Direction

This research work examines common attributes of Cyber-security policies based on the policies of seven regions countries. A country can develop a fitting cyber-security policy with the help of this research but this research can be extended in several directions to gain additional benefits. Here are some future works that can be conducted in this field.

There is a need to examine the cyber-security policies of other countries which have a large number of IT users and well-developed IT sector. This kind of study will explore other important attributes of cyber-security policies which can help countries to improve their policy. The study of policies of other countries will also reveal more techniques and methods of Cybercrimes which can help law enforcement agencies to tackle similar cybercrimes in their countries. Since the analysis of policies of a large number of countries will require a large amount of time and resources therefore proper sponsor will be required for such research in order to obtain useful results. This research work on fifteen common attributes can contribute a lot to such comprehensive future research works.

Since the cyberspace is expanding continuously and technologies associated with it are also improving, ; therefore, challenges for cyber-security is also increasing. Simple policies can help to tackle Cybercrimes and Cyber-security issues of present time but these policies may not be effective in future. There is a need to develop a more dynamic policy which can work for a long time and allow authorities to make quick adjustments. Advanced level research can be conducted to find a way to develop a dynamic policy (Howard and Prince, 2011). One example such policy is the telecommunication act of the USA. It was developed in 1996 and it is still effective with all modern technologies, devices, and system in the telecommunication industry.

The difference in the policies of different countries also leads to some Cybercrimes. For instance, a hacker can try to intrude in a network or hack a system of a country while sitting in a country with lenient or no policy against intrusion and hacking (Janczewski and Colarik, 2008). A global policy for cyber-security can improve the user-experience of all internet users in the world. A comprehensive research work is required to find out

how a global policy can be developed. It is possible for a country to develop a policy which not only protects cyberspace within the country but also prevent people in its boundaries from harming cyberspace of other countries in any way. It can even improve the relationship between different nations (Andreasson, 2012). This research work can provide a base to develop such policy or conduct advanced level research for this cause.

REFERENCES

Amoroso, E. (2005). *Cyber-security* (1st ed.). Norwood Mass. Books24xs7.com.

Anderson, R. (2012). *Measuring the cost of cybercrime*. Retrieved 10 November 2016, from http //weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Andreasson, K. (2012). *Cyber-security Public Sector Threats and Responses* (1st ed.). Boca Raton, Fla. CRC Press.

Ahlgren , Magnus Breidne & AndersHektor (2005), IT Security in the USA, Japan and China https/www.tillvaxtanalys.se/download/18.6a3ab2f1525cf0f4f9a7059/1454413210502/IT+security+in+the+USA,+Japan+and+China-05.pdf

Andreasson, K. (2012). *Cyber-security Public Sector Threats and Responses* (1st ed.). Boca Raton, Fla. CRC Press.

Annegret Bendiek (2012). European Cyber-security Policy. https //www.swp berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf

Anwar, A., & Mahmood, A. N. (2014). Cyber-security of smart grid infrastructure. *arXiv preprint arXiv* 1401. 3936.

ASSC. (2017). *Australian Cyber-security Centre (ACSC). Acsc.gov.au.* Retrieved 5 May 2017, from https //www.acsc.gov.au/

Au, M., Carminati, B., & Kuo, C. (2014). *Network and System Security* (1st ed.). Cham Springer International Publishing.

Hashim B, M. S.Malaysia's National Cyber-security Policy The Country's Cyber Defense Initiatives, 2011. IEEE Xplore Digital Library.

Bahuguna, A.FIRe. Firefox for Computer Security Incident Reporting and Coordination. *IITM Journal of Management and IT*, 2015.**6**(1) p 3-11.

Bailetti, T., Craigen, D., Hudson, D., Levesque, R., McKeen, S., & Walsh, D. A. Developing an Innovation Engine to Make Canada a Global Leader in Cyber-security. *Technology Innovation Management Review*, 2013. **3**(8) p 5-14.

Barker, E. (2006). *Recommendation for obtaining assurances for digital signature applications* (1st ed.). [Gaithersburg, MD] National Institute of Standards and Technology, Technology Administration.

Bayuk, J. (2012). *Cyber-security policy guidebook* (1st ed.). Hoboken, N.J. Wiley.

Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., & Weiss, J. (2012). *Cyber-security Policy Guidebook* (1st ed.). Somerset Wiley.

Beardwood, J., & Stern, G. (2014). Entry into Force of Canada's Anti-Spam Law. *Computer Law Review International*, 15(2). http //dx.doi.org/10.9785/cri-2014-0204

Bell, C. Surveillance strategies and populations at risk Biopolitical governance in Canada's national security policy. *Security Dialogue*, 2006. 37(2) p 147-165.

Bilbao-Osorio, B., Dutta, S., & Lanvin, B. The global information technology report 2013. *In World Economic Forum* p 1-383.

Binding, J., & Purnhagen, K. (2016). Regulations on E-Commerce Consumer Protection Rules in China and Europe. *Policy Review*, 65.

Binti Mohamed, D. Combating the threats of cybercrimes in Malaysia The efforts, the cyber laws and the traditional laws. Computer Law & Security Review, 2013.**29**(1) p 66-76.

Black, D. (2012). *Royal Canadian Mounted Police (2011); The RCMP's perspective on a Canadian cybercrime strategy*. Retrieved 10 November 2016, from

http //www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Report s-Presentations/Octopus2011/WS3_David_Black_CCFC.pdf

Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., & Tonks, S. The risk assessment of ERTMS-based railway systems from a cyber-security perspective Methodology and

lessons learned. *In International Conference on Reliability, Safety and Security of Railway Systems*, 2016.p 3-19.

Blythe, S. E. (2007). China's New Electronic Signature Law and Certification Authority Regulations. *Journal of Intellectual Property*, 1-32.

Borgman, B., Mubarak, S., & Choo, K. Cyber-security readiness in the South Australian Government. *Computer Standards & Interfaces*, 2015.**37** p 1-8.

Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel (2004). *The Economic Impact of Cyber-Attacks*.
.http//www.au.af.mil/au/awc/awcgate/crs/rl32331.pdf

Brookes, C. (2015). Cyber-security Time for an integrated whole-of-nation approach in Australia. *Indo-Pacific Strategic Papers.*

Business.vic.gov.au. (2016). Privacy and Data protection Act 2014. Department of Economic Development, Jobs, *Transport and Resources*, 2-20.

Carr, J., & Shepherd, L. (2010). *Inside cyber warfare* (1st ed.). Sebastopol, Calif. O'Reilly Media, Inc.

Carr, M. Public–private partnerships in national cyber-security strategies. *International Affairs*, 2016.**92**(1) p 43-62.

Cavelty, M. D. Breaking the cyber-security dilemma Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, 2014.**20**(3) p 701-715.

Chatterjee, S. (2014). *Identity-based encryption* (1st ed.),US Springer.

Chen, L., & Gong, G. (2012). *Communication system security* (1st ed.). Boca Raton, FL CRC Press.

Chertoff, M. (2008).The cyber-security challenge. *Regulation & Governance,* 2(4), 480-484. http //dx.doi.org/10.1111/j.1748-5991.2008.00051.x

Chin, O. & Yusoff A., S. (2016). Remedy as of Right for Consumer Protection. *Mediterranean Journal Of Social Sciences*.

http //dx.doi.org/10.5901/mjss.2016.v7n2p142

Chipman, S. (2016).Spam or not-spam. *Psyccritiques*, 61(2).

http //dx.doi.org/10.1037/a0040047

Cohen, E., Khalilzad, Z., & White, J. (1999). Strategic Appraisal The Changing Role of Information in Warfare. Foreign Affairs, 78(5), 168.http //dx.doi.org/10.2307/20049472

Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber-security Strategy (April 2016).

Computerworlduk.com. (2015). 10 things you need to know about the new EU data protection regulation. *computerworlduk.com*, 1-10.

Consumer.org.my. (2017). *The Consumer Protection Act.* Retrieved 5 19, 2017, from consumer.org.my https //www.consumer.org.my/index.php/complaints/rights/254-the-consumer-protection-act

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. Scene A structured means for creating and evaluating behavioral nudges in a cyber-security environment. *In International Conference of Design, User Experience, and Usability*, 2014.p 229-239.

Crandall, R. (2005). *Competition and chaos* (1st ed.). Washington, D.C. Brookings Institution Press.

Crandall, R. (2006). Competition and chaos U.S. telecommunications since the 1996 Telecom Act. *Choice Reviews Online*, 43(05), 43-2895-43-2895.

http //dx.doi.org/10.5860/choice.43-2895

Cryptomathic. (2017). *Product Sheet Signer Freedom to digitally sign documents remotely, Fully IDAS compliant. Cryptomathic.com.* Retrieved 21 May 2017, from

https//www.cryptomathic.com/hubfs/docs/cryptomathic_signer product_sheet.pdf?t=1495211003090

Cyber-security .my. (2017). *Cyber-security Malaysia | An Agency Under MOSTI. Cyber-security .my.* Retrieved 5 May 2017, from http //cyber-security .my/en/about_us/contact/main/detail/732/index.html

David A. Wheeler Gregory N. Larsen (2003), Techniques for cyber-attack Attribution References for cyber-security Policy each country

Donthula Ravi Kumar (2016), Cyber-security Policy and Implementation

https //www.ijarcsse.com/docs/papers/Volume_6/7_July2016/V6I7-0149.pdf

Dunham, M., & Bradshaw, A. (2004).*The Spam Act* (1st ed.). [Adelaide] Law Society of South Australia.

Dunn Cavelty, M. From Cyber-Bombs to Political Fallout Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 2013.**15**(1) p 105-122.

Economides, G., Philippopoulos, A., & Vassilatos, V. (2014).Public, or private, providers of public goods?A dynamic general equilibrium study. European Journal Of Political Economy, 36, 303-327. http //dx.doi.org/10.1016/j.ejpoleco.2014.09.00

Mejia Eric F., Colonel, USAF (2014), Act and Actor Attribution in Cyberspace

http //www.au.af.mil/au/ssq/digital/pdf/spring_2014/Mejia.pdf

Europa.eu. (2017). *E-Commerce Directive.* Retrieved 5 19, 2017, from europa.eu

http //ec.europa.eu/internal_market/e-commerce/directive/index_en.htm

Europa.eu. (2017).*Summary of Legislation.* Retrieved 5 19, 2017, from europa.eu

http //eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX 32002L0058

FAS (2010) The Comprehensive National Cyber-security Initiative, *Federation of American Scientists, White House release.* Available at https //fas.org/irp/eprint/

Flick, T., & Morehouse, J. (2011). *Securing the smart grid* (1st ed.). Rockland, Mass. Syngress.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). *The global cyber-security workforce an ongoing human capital crisis.*

Freeze, C. (2012) Canada needs to take threat of Chinese cyber espionage more seriously

Gallaher, M., Link, A., & Rowe, B. (2008). *Cyber-security* (1st ed.). Cheltenham, UK Edward Elgar.

Garfinkel, S., & Spafford, G. (2011).*Web Security, Privacy & Commerce* (1st ed.). Sebastopol O'Reilly Media, Inc.

Gendron, A. (2013). Cyber threats and multiplier effects Canada at risk. Canadian Foreign Policy Journal, 19(2), 178-198.
http //dx.doi.org/10.1080/11926422.2013.808578

Ghosh, S. (2002). P*rinciples of Secure Network Systems Design* (1st ed.). New York, NY Springer New York.

Green and Rowe **(**2015**).** Attribution of Cyber Warfare *Cyber Warfare: A Multidisciplinary Analysis* on (ch3).

http://faculty.nps.edu/ncrowe/3%20-%20Rowe%20chapter%20070214.htm

Go, C. L. (2016). E-Banking in Malaysia Opportunity and Challenges. *Journal of Internet Banking and Commerce,* 1-10.

Graham, D. (2010). *Cyber threats and the law of war.* Journal of National Security Law and Policy, 4, 87-104.

Graham, J., Howard, R., & Olson, R. (2011).*Cyber-security essentials* (1st ed.). Boca Raton, FL Auerbach Publications.

Graves, J. T., Acquisti, A., & Christin, N. Big data and bad data on the sensitivity of security policy to imperfect information. *The University of Chicago Law Review,* 2016.p 117-137.

Gurkaynak, G., Yilmaz, I., & Taskiran, N. P. Governmental Efforts and Strategies to Reinforce Security in Cyberspace. *International Law Research,* 2013.**2**(1), 185.

Gustke, C. (2013). The EU has strong standards and enforcement. And the rest of the world is playing catch up. *BBC*, 1-10.

Glenny (2011). The Cyber Arms Race Has Begun. *Governments are ramping up investment in cyber weaponry as well as cyber-security, opening a dark new frontier*. https://www.thenation.com/article/cyber-arms-race-has-begun/

Ghosh (2002). Telephone penetrations and economic growth: evidence from India. https://link.springer.com/article/10.1007/s11066-012-9067-z

Hart, J. (2009). Remote working managing the balancing act between network access and data security. *Computer Fraud & Security*, 2009(11), 14-17.

http //dx.doi.org/10.1016/s1361-3723(09)70141-1

Hashim, M. S. (2008). Malaysia's National Cyber-security Policy The country's cyber defense initiatives. *IEE Explore*, 1-29.

Hawke, J. (2000). *Bank regulators' evaluation of electronic signature systems* (1st ed.). Washington, DC U.S. General Accounting Office.

Heiman, B. J. (2003) *Cyber-security Regulation is Coming Here!*, Presentation delivered to the 12th Annual RSA Security Conference.

Hijmans, H. (2014). Lee A. Bygrave, Data Privacy Law, an International Perspective, Oxford University Press, Oxford, 2014, 272 pages, 234 x 156 mm, 75, ISBN 978-0-19-967555-5. *International Data Privacy Law*, 5(1), 88-90.

http //dx.doi.org/10.1093/idpl/ipu031

Hoffman, S., & McGinley, T. (2010). *Identity theft* (1st ed.). Santa Barbara, Calif. ABC-CLIO.

Howard, D., & Prince, K. (2011).*Security 2020* (1st ed.). Indianapolis, Ind. Wiley Pub.

IEEE.,(2016). IEEE Transactions on Smart Grid publication information. *IEEE Transactions On Smart Grid*, 7(4), C2-C2. http //dx.doi.org/10.1109/tsg.2016.2580009

Hamilton, Booz .A, (2012). Preserving the safety of your world. https://www.boozallen.com/expertise/cyber.html

Janczewski, L., & Colarik, A. (2008).*Cyber warfare and cyber terrorism* (1st ed.). Hershey Information Science Reference.

Jang-Jaccard, J., & Nepal, S. A survey of emerging threats in cyber-security. *Journal of Computer and System Sciences,* 2014.80 (5) p 973-993.

Jasper, M. (2008). *Consumer rights law* (1st ed.). New York Oceana.

Jiang, L., & Hu, Z. Australia's Policies and Practices in Combating Cybercrime. Australian Studies in China. 2013.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. Dispositional and situational factors influences on information security policy violations. *European Journal of Information Systems,* 2016.**25**(3) p 231-251.

Kenneth Geers (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. http://www.tandfonline.com/doi/pdf/10.1080/19393550802676097

Kamath, N. (2009). *Law relating to computers, internet & e-commerce* (1st ed.). Delhi Universal Law Pub. Co.

Kazan, H. (2016). Contemporary Issues in Cyber-security. *Journal Of Cyber-security Research (JCR),* 1(1), 1. http //dx.doi.org/10.19030/jcr.v1i1.9745

Kerber, W. (2016). Digital Markets, Data, and Privacy Competition Law, Consumer Law, and Data Protection. *SSRN Electronic Journal*.

http //dx.doi.org/10.2139/ssrn.2770479

Kigerl, A. (2016). *Email spam origins does the CAN SPAM act shift spam beyond United States jurisdiction?.* Trends In Organized Crime.

http //dx.doi.org/10.1007/s12117-016-9289-9

Knapp, K. J. (2009) *Cyber-security and Global Information Assurance Threat Analysis and Response Solutions Threat Analysis and Response Solution*. IGI Global,

Kortjan, N., & Von Solms, R. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal,* 2014.**52**(1) p 29-41.

Kott, A., (2014). Towards fundamental science of cyber-security. *In Network Science and Cyber-security,* p 1-13. Springer New York.

Kshetri, N., (2013). Cybercrime and cyber-security issues associated with China some economic and institutional considerations. *Electronic Commerce Research.,* 13(1) p 41-69.

Kshetri, N (2015). India's Cyber-security Landscape The Roles of the Private Sector and Public-Private Partnership. *IEEE Security & Privacy.*, 13(3) p 16-23.

Kulesza, J. (2013). International law challenges to location privacy protection. *International Data Privacy Law,* 3(3), 158-169. http //dx.doi.org/10.1093/idpl/ipt015

Kumar, V. Ananda, Pandey, K. and Punia, D., (2014). Cyber-security threats in the power sector Need for a domain specific regulatory framework in India. *Energy Policy,* 2014.**65** p 126-133.

Kurt, A. (2015). Effectiveness of Cyber-security Regulations in the US Financial Sector *Information Security Policy and Management,* 1-75.

Lakomy, M., (2013). The Significance of Cyberspace in Canadian Security Policy. Central European *Journal of International & Security Studies,* 2013.**7**(2) p 62-79.

Law360. (2016). 3 Ways Cyber-security Law In China Is About To Change. *Cov.com,* 1-98.

Leccisotti, F. Z., Chiesa, R., & De Nicolo, D., (2013) Analysis of possible future global scenarios in the field of cyber warfare National cyber defense and cyber-attack capabilities. *In Handbook of research on civil society and national security in the era of cyber warfare,* 2013.p 181-204. IGI Global.

Lehto, M. (2013).The Cyberspace Threats and Cyber-security Objectives in the Cyber-security Strategies. *International Journal Of Cyber Warfare And Terrorism,* 3(3), 1-18. http //dx.doi.org/10.4018/ijcwt.2013070101

Lewis, J. A., & Timlin, K. Cyber-security and cyber warfare. *Center for strategic and international studies*. 2011.

Lloyd, I. (2004). *Information technology law* (1st ed.). Oxford University Press.

Longdi, X. China's Internet Development and Cyber-security and policies and practices. Conference "China's Cyber-security and Cyber defense policies and strategies" - Paris, 1 July 2013.

Lori M. Kaufman (2009). *Data Security in the World of Cloud Computing* .IEEE Security & Privacy . http //ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5189563

Luiijf, E., Besseling, K., & De Graaf, P. Nineteen national cyber-security strategies. *International Journal of Critical Infrastructures* 6, 2013.**9**(1-2) p 3-31.

Luiijf, E., Besseling, K., & Graaf, P. (2013).Nineteen national cyber-security strategies. International Journal Of Critical Infrastructures, 9(1/2), 3.

http //dx.doi.org/10.1504/ijcis.2013.051608

MacKinnon, L. (2012). *Data Security and Security Data* (1st ed.). Berlin, Heidelberg Springer Berlin Heidelberg.

Malufu, K. (2013). *E-Banking Security* (1st ed .). Saarbrücken LAP LAMBERT Academic Publishing.

Manz, W., & Best, R. (2005).*Federal identity theft law* (1st ed.). Buffalo, N.Y. Hein.

Matlick, J. (1998). *U.S. encryption policy* (1st ed.). San Francisco, CA Pacific Research Institute for Public Policy.

McCann, A. (2012). *Know Your Rights* (1st ed.). Dublin Orpen Press.

McCann, T. (2002). *Information security* (1st ed.). Morristown, NJ FEI Research Foundation.

McIntosh, C. (2015). Cyber-security who will provide protection?.*Computer Fraud & Security,* 2015(12), 19-20. http //dx.doi.org/10.1016/s1361-3723(15)30113-5

McKenna, B. (2005). 2.4 billion lost to hi-tech crime. *Computer Fraud & Security,* 2005(4), 2. http //dx.doi.org/10.1016/s1361-3723(05)70191-3

McKim, R. (2001). Privacy notices What they mean and how marketers can prepare for them. *Journal Of Database Marketing & Customer Strategy Management*, 9(1), 79-84. http //dx.doi.org/10.1057/palgrave.jdm.3240061

Meyer, H. (1996). The new US encryption policy. *Computers & Security,* 15(7), 585. http //dx.doi.org/10.1016/s0167-4048(97)88115-1

Miao, W., & Lei, W. (2016). Policy review The Cyberspace Administration of China. *Global Media And Communication*, 12(3), 337-340.

http //dx.doi.org/10.1177/1742766516680879

Millard, C. (2014). *Cloud computing law* (1st ed.). Oxford University Press.

Min, K. S., Chai, S. W., & Han, M. An International Comparative Study on Cyber-security Strategy. *International Journal of Security and Its Applications,* 2015.**9**(2) p 13-20.

Ministry of Science, Technology and Innovation, Malaysia, "National Cyber-security Policy The Way Forward," Federal Government Administrative Centre. July 2006

Mitrakas, A. Information security and law in Europe Risks checked? *Information & Communications Technology Law*, 2006. 15(01) p 33-53.

Mohamed, D. Combating the threats of cybercrimes in Malaysia The efforts, the cyber laws and the traditional laws. Computer Law & Security Review, 2013.**29**(1)p 66-76.

Mohd Shamir b Hashim (2011), Malaysia's National Cyber-security Policy

http //ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5978782

Mosti.gov. (2016).National Cyber-security. Ministry of Science, *Technology And Innovation*.

Muhaya, F. Dominant factors in national information security policies. *Journal of Computer Science,* 2010.**6**(7) p 808.

NIST. (2010). *Guidelines for smart grid cyber-security* (1st ed.). Gaithersburg, MD U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

NSCS (2016). *Cyber-security Information Sharing Partnership (CiSP) - NCSC Site. Ncsc.gov.uk*. Retrieved 21 May 2017. from https //www.ncsc.gov.uk/cisp

Oak Ridge. (2011). *Validating Cyber-security Requirements* (1st ed.). Oak Ridge, Tenn. Oak Ridge National Laboratory.

O'Byrne, S. (2013). *Data security, data mining, and data management* (1st ed.). New York Nova Science.

OECD (2016). *Digital Economy Policy Legal Instruments.* OECD.

Oltramari, A., Ben-Asher, N., Cranor, L., Bauer, L., & Christin, N. General requirements of a hybrid-modeling framework for cyber-security. *In Military Communications Conference (MILCOM),* 2014 IEEE p 129-135.

Petr D., Chroust Gerhard & Oškrdal Václav (2015). Information Technology and Society Interaction and Interdependence. *Interdisciplinary Information Management Talks, 23nd on* (pp. 91). https://www.zsi.at/object/publication/3889/attach/IDIMT_proceedings_2015.pdf

Public Safety Canada, Government of Canada (2010) Canada cyber-security strategy.

Relyea, H. (2007). *Privacy protection* (1st ed.). [Washington, D.C.] Congressional Information Service, Library of Congress.

Robinson, N. (2011). Comparative Study on Legislative and Non Legislative Identity theft rules. *RAND Europe,* 89.

Rosenzweig, P. (2016). *Cyber-security Act of 2012 Revised Cyber Bill Still Has Problems. The Heritage Foundation.* Retrieved 1 June 2017. from

http //www.heritage.org/defense/report/cyber-security -act-2012-revised-cyber-bill-still-has-problems

Roth, K. Implications for Virtual Worlds A Comparative Study of United Kingdom, United States and Australia on Network Readiness, Government Investment and Cyber-security. *Journal For Virtual Worlds Research,* 2010. **2**(5) p 2-13.

Salaün, A. (1999). Consumer protection - proposals for improving the protection of online consumers. *Computer Law & Security Review,* 15(3), 159-167.

http //dx.doi.org/10.1016/s0267-3649(99)80034-x

Samuel, C. (2017). *The Long Slog for Cyber-security in India. The Cipher Brief.* Retrieved 5 May 2017. from https //www.thecipherbrief.com/article/asia/long-slog-cyber-security -india-1092

Sarma, S. Cyber-security Mechanism in European Union. ICWA View Point. *Indian Council of World Affairs*. 2016.

Saxby, S. (1995).*Network-related law — recent decisions from USA.* Network Security, 1995(6), 18-19. http //dx.doi.org/10.1016/1353-4858(96)89728-5

Scapens, R. (2011). The Case Study as Research Method A Practical Handbook20111Yves-C. Gagnon. *Qualitative Research In Accounting & Management*, 8(2), 201-204. http //dx.doi.org/10.1108/11766091111137582

Scott J. Shackelford, J. P. (2016). A Comparison Of "Voluntary" Cyber-security Frameworks. *Cyber-security Research*, 2-50.

Segal, A. (2016). China, Encryption Policy. *Hoovers*, 1-78.

Shackelford, S., & Craig, A. (2014).*Beyond the New 'Digital Divide' Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber-security.*

Shalini, S. (2015). Cyber-security in the Indian Banking Sector. *Information Law and Policy Research at the Centre for Communication Governance,* 1-10.

Shankar, R. (2015). Criticism forces government to roll back its draft encryption policy. *Express News Service,* 1-10.

Shields, R. (2016).*What does the shake-up of EU data laws mean for marketers?.The Drum.* Retrieved 1 June 2017. from http //www.thedrum.com/news/2016/04/14/what-does-shake-eu-data-laws-mean-marketers-0

Singleton, S. (2003). *E-Commerce* (1st ed.). Aldershot, Hampshire, England Gower.

Skopik, F., & Smith, P. (2015). *Smart grid security* (1st ed.).

Ślęzak, D., Arnett, K., Fang, W., & Kim, T. (2009).*Security Technology* (1st ed.). Berlin, Heidelberg Springer-Verlag Berlin Heidelberg.

Sorebo, G., & Echols, M. (2012).*Smart grid security* (1st ed.). Boca Raton [FL] CRC Press.

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2016). EU and NATO cyber-security strategies and national cyber-security strategies a comparative analysis. *Security Journal*. http //dx.doi.org/10.1057/s41284-016-0083-9

Stoddart, K. (2016). UK cyber-security and critical national infrastructure protection. *International Affairs*, 92(5), 1079-1105. http //dx.doi.org/10.1111/1468-2346.12706

Stoddart, K. UK cyber-security and critical national infrastructure protection. International Affairs, 2016. 92(5) p 1079-1105.

Stroup, J. (2016). The Identity Theft and Assumption Deterrence Act of 1998. *The Balance*, 1-10.

Subsorn, P., & Limwiriyakul, S. A case study of internet banking security of Mainland Chinese Banks A customer perspective. *In Computational Intelligence, Communication Systems and Networks (CICSyN),* 2012 Fourth International Conference on p 189-195. IEEE.

Tajts, T. (2012).*Cloud computing security* (1st ed.). Lexington, KY Create Space.

Talbott, A. (2016). Privacy Laws How the US, EU and others protect IoT data (or don't). *Internet of Things The Security Challenge*, 1-10.

Kostadinov D., The Attribution Problem in cyber-attacks, (2013) http//resources.infosecinstitute.com/attribution-problem-in-cyber-attacks

Tim Scully (2016), Cyber-security and the 2016 Defense.

https //www.regionalsecurity.org.au/resources/Documents/SC%2012-1%20Scully.pdf

Trout, B (2007). *Cyber Law A Legal Arsenal for Online Business* (1st ed.). New York, NY World Audience.

Turner (2015). *Review of Australian Government Australia.* AIIA.

Van der Meulen, N., Jo, E., & Soesanto, S. Cyber-security in the European Union and Beyond Exploring the Threats and Policy Responses. *Rand Corporation.* 2005.

VEDA (2016). VEDA. An Equafix Company.

Voeller, J. (2014). *Cyber-security* (1st ed.). Wiley.

Wang, M., Zhang, Z., & Chen, C. (2015).Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme. *Concurrency And Computation Practice And Experience,* 28(4), 1237-1245.

http //dx.doi.org/10.1002/cpe.3623

Wang, X., Liang, Q., Mu, J., Wang, W., & Zhang, B. (2013). Physical layer security in wireless smart grid. *Security And Communication Networks,* 8(14), 2431-2439.

http //dx.doi.org/10.1002/sec.751

Weir, C., Douglas, G., Carruthers, M., & Jack, M. (2009).User perceptions of security, convenience and usability for E-banking authentication tokens. *Computers & Security,* 28(1-2), 47-62. http //dx.doi.org/10.1016/j.cose.2008.09.008

Weir, C., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security User preferences for authentication methods in E-Banking and the effects of experience. *Interacting With Computers,* 22(3), 153-164.

http //dx.doi.org/10.1016/j.intcom.2009.10.001

Wessing, T. (2016).Protecting the people China's Consumer Law. *Lexology,* 1-10.

Westby, J. (2004). *International Guide to Privacy* (1st ed.). American Bar Association. Section of Science & Technology Law.

White House, "Cyberspace Policy Review".

http //www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (2016).

Wilson, N. (2014). Australia's National Broadband Network – A cyber secure critical infrastructure?.*Computer Law & Security Review*, 30(6), 699-709.

http //dx.doi.org/10.1016/j.clsr.2014.09.003

Yee, G. (2006). *Privacy protection for e-services* (1st ed.). Hershey, Pa. Idea Group Pub.

Yeluri, R., & Castro-Leon, E. (2014). *Building the Infrastructure for Cloud Security* (1st ed.). Berkeley, CA Apress.

Zainal, Z. (2007) Case study as a research method, Jurnal Kemanusiaan bil.

Zhang, L. (2010). *Web services research for emerging applications* (1st ed.). Hershey, Pa. IGI Global (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA).

Zanders, J. P. (2009) "Cyber-security: What Role for the CFSP?" Institute Report - seminar organized jointly by General Secretariat of the Council of the EU & the EU Institute for Security Studies in cooperation with Estonia held in Brussels on 4 February 2009, European Union Institute for Security Studies