2nd International Conference on New Frontiers of Engineering, Management, Social Science and Humanities
Mahratta Chamber of Commerce, Industries and Agriculture, Pune (India) EMSSH-2018
27th May 2018 www.conferenceworld.in ISBN: 978-93-87793-28-6

COMPARISON OF CRIME OF DIFFERENT COUNTRIES—CYBER CRIME

Shruti Bajaj[1], Dr. Rajesh Kumar Singh[2]

1. *PHD STUDENT, PUNJAB TECHNICAL UNIVERSITY KAPURTHALA,*
2. *PRINCIPAL, SUSCET TANGORI MOHALI*

ABSTRACT:

Today's Global era needs laws governing fast paced cybercrime. The popularity of on-line transaction is on the rise thereby having attempts made by unscrupulous entities to defraud internet users. The modus operandi may be in the form of Hacking, Spoofing, Pornography, Scanners, Device, Fake card and the like. Here we are focusing on Cyber Crime. Cybercrime often has an international dimension. E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country. Within cybercrime investigations, close cooperation between the countries involved is very important. The paper is an analysis of the Cyber Crime of different countries with a comparative analysis with the India. The aim is to analyze the conviction rate in cybercrime with comparison to various countries and suggest various remedies.

Keywords: *Crime, Cybercrime, Cyber Security,*

I. INTRODUCTION

Cybercrime is defined as crimes committed on the Internet using the computer either as a tool or a targeted victim. However, some overlap occurs in many cases and it is difficult to have a clear cut classification system. We breakdown cybercrime along two dimensions. The first dimension classifies the computer as a tool and as a target. The second dimension is the classification of crime itself: Person, Property, and Victimless/Vice. In Simple ways we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a new age crimes that are addressed by the Information Technology Act, 2000. We can categorize Cybercrimes in two ways. The Computer as a Target:-using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc. The computer as a weapon:-using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc[1].

Cyber-law is also known as Cyber Law or Internet Law. Cyber-laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices. The increase in Internet traffic has led to a higher proportion of legal

issues worldwide. Because cyber-laws vary by jurisdiction and country, enforcement is challenging, and restitution ranges from fines to imprisonment [2].

Cyber Security is a complex and complicated branch to manage. Even Cyber Security Awareness in India and World Wide is not up to the mark. The rest of this paper is organized as follows. Section 2 explains country specific analysis of cybercrime in various countries. This section gives the detailed report of cybercrime and also the remedies and strategies to improve them.

II. COUNTRY SPECIFIC ANAYLSIS

This section of the report addresses the specific cybercrime of different countries and suggests remedies to improve them [3].

2.1 Australia

In 2012 Norton claimed that more than 5.4 million Australians were victims of cyber-crime – a quarter of the country's total population; those crimes cost Australia $1.65 billion over that year, and the Australian Government expected cyber-crime costs to stay above $1 billion a year for the foreseeable future.

2.1.1 Cyber-crime v. Cyber-warfare:

Both terms "cybercrime" and "cyber-attack" are mentioned in Australian policy documents in different contexts; thus, the distinction is apparent, even though there is no clear definition provided for either of the terms.

2.1.2 Where is the Focus?

Australian Government's Cyber Security Strategy was launched on 23 November 2009, as an outcome of the E-security Review 2008. The strategy articulates a number of strategic priorities, among which on the first place is "Threat Awareness and Response" set to "improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest". Other priorities include educating the Australians with information and practical tools to protect themselves online, cooperate with businesses to promote cyber security, promote the development of a skilled cyber security workforce, model best practice in the protection of government ICT systems, and promote a secure global electronic operating environment that supports Australia's national interests. "Legal and Law Enforcement" is one of the last objectives identified in Australian Cyber Security Strategy, and it is set to "maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime".

2.1.3 The Law and the need for Warrants:

The Ministry for Home Affairs and Justice and the Police are the authorities responsible for cyber-crime. The Ministry released the Protocol for Law Enforcement Agencies on Cybercrime Investigations in 2011. The protocol provides a cyber-crime investigation matrix that outlines the most appropriate agencies to deal with particular types of complaints, and provide specific arrangements for sharing information to cybercrime investigations between jurisdictions.

The Cybercrime Act states the following offences:

- Unauthorized modification of data to cause impairment: 10 years imprisonment.
- Unauthorized impairment of electronic communication: 10 years imprisonment.

- .Unauthorized access to, or modification of, restricted data: 2 years imprisonment.
- Unauthorized impairment of data held a computer disk: 2 years imprisonment.

Australia acceded to the Budapest Convention and new law enforcement measures had to be introduced as part of the joining the Convention, the Cybercrime Legislation Amendment Bill, which came into force in Fall 2012.31 One of those measures will allow other countries on the Council to serve notices to Australian ISPs requiring them to store 180 days of web data for targeted users, and at a later stage the foreign countries can obtain a warrant to take receipt of the recorded information.

The expected changes include extending the period of time between interception and obtaining a warrant, mandatory data retention, surveillance of social networks, and criminalization of encryption. Under the proposed law, ISPs, search engines and social networks, and other websites are required to store all the information for 2 years, which could be accessed without a warrant by the Australian Security Intelligence Organization (ASIO). ASIO will have a right to demand personal passwords to access this data and to deny providing this information would be illegal.

2.2 New Zealand

According to 2010 data, 70% of New Zealand adults have been the targets of some form of cyber-crime, with the most common complaints being computer scams, fraud and viruses/malware.

2.2.1 Cyber-crime v. Cyber-warfare:

The difference between "cyber-crime" and "cyber-attack" is defined in New Zealand's Cyber Security Strategy as follows:

Cyber-attack – An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.

Cyber-crime – Any crime where information and communication technology is:

1) Used as a tool in the commission of an offence;

2) The target of an offence;

3) A storage device in the commission of an offence.

2.2.2 Where is the Focus?

The distinction between cyber-crime and cyber-attacks was important in formulating the Cyber Security Strategy. A cyber-attack can be classified as a computer or cyber-crime, yet from New Zealand's Cyber Security Strategy it is evident that the following cyber threats require a special response and are more serious than domestic crimes: cyber-espionage, and terrorist use of the Internet. The highlighted difference from regular cyber-crimes is that the targets of these attacks are not individuals or private organizations, but government systems, critical national infrastructure and "businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets". Therefore, the Cyber Security Strategy is formulated particularly with the key objectives "to improve the level of cyber security across government and for critical national infrastructure and other business".

2.2.3 The Law and the need for Warrants

The following offences are identified as "crimes involving computers" and are subjected to punishment according to Crimes Act:

- Section 249 – Accessing computer system for dishonest purpose.
- Section 250- Specifies imprisonment for a term not exceeding 10 years to everyone who intentionally damages or alters any computer system "if he or she knows or ought to know that danger to life is likely to result". Any damage to computer system, interference with data without authorization, causing computer system to fail or deny service to any authorized user is punishable by imprisonment for up to 7 years.

.

In 2012 New Zealand passed the Search and Surveillance Act. 35 The Act unified the powers that previously were scattered across roughly 70 agencies. The Secret Intelligence Service and the Government Communications Security Bureau are still governed by their own legislation.

2.3 United Kingdom

2.3.1 Cyber-crime v. Cyber-warfare:

The policy documents reviewed do not offer explicit definitions for cyber-crime, cyber-attack or cyber warfare. However, the distinction is clearly present. In the Parliamentary Office of Science & Technology's report "Cyber Security in the UK" two types of cyber-attacks are discussed – attacks on information infrastructure and attacks on physical infrastructure; it is briefly explained that cyber-attacks are "aimed to steal sensitive information and data from financial, government and utilities infrastructure targets".

The Ministry of Defense comments on the emerging discussion about cyber war: "There is an ongoing and broad debate regarding what 'cyber warfare' might entail, but it is a point of consensus that with a growing dependence upon cyber space, the defense and exploitation of information systems are increasingly important issues for national security. The need to develop military and civil capabilities, both nationally and with allies, to ensure can defend against attack, and take steps against adversaries where necessary."

2.3.2 Where is the Focus?

The UK's Cyber Security Strategy 2011 provides the action plan for the country to meet these objectives by 2015, in the order of importance:

1) The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace.

2) The UK to be more resilient to cyber-attacks and able to protect the UK's interests in cyberspace. 3) The UK to have helped shape an open, stable and vibrant cyberspace, which the UK public can use safely and that supports open societies.

British government puts greater emphasis on combating cybercrime, while the objective to protect the country from cyber-attacks comes second. The objective to secure the UK from cyber-attacks is also taken seriously. In 2010 the Government invested £650 million in a four-year National Cyber Security Programme (NCSP). Around half of this funding was assigned towards enhancing the UK's core capability to detect and counter cyber-attacks.

2.3.3 The Law and the need for Warrants

The Computer Misuse Act (1990) describes different computer misuse offences and outlines penalties for them:

(1) Unauthorized access to computer material;

(2) Unauthorized access with intent to commit or facilitate commission of further offences; and (3)Unauthorized modification of computer material. The penalties vary from a fine to imprisonment from six months to ten years

depending on nature of the crime. The Act was expanded in 2006. The Regulation of Investigatory Powers Act 2000 provides a whole chapter on communications interception, including the section on "Lawful interception without an interception warrant" According to this section, communication may be intercepted without a warrant if just one person involved in the communication has consented to the interception; surveillance by means of this interception is authorized as well; communication interception is also authorized if it's related to "the prevention or detection of anything which constitutes interference with wireless telegraphy".

In 2012 the Home Office drafted a new Communications Data Bill, which would authorize the state to monitor internet communications and require communications companies to store users.

2.4 United States of America

The United States ratified the Council of Europe Convention on Cybercrime in 2006.

2.4.1 Cyber-crime v. Cyber-warfare:

In various legal, strategic and academic documents of United States the terms cyber-crime, cyber-attack, computer attack, electronic attack, and cyber-terrorism are coined and defined.

2.4.2 Where is the Focus?

The Department of Homeland Security operates the National Cyber Alert System and the National Cyber Response Coordination Group – two important programs in protecting U.S. from cyber threats. In addition, Homeland Security oversees an ongoing security exercise Cyber Storm.

The National Cyber Security Division (NCSD) is a Department of Homeland Security responsible for protecting cyber infrastructure. To secure cyberspace, NCSD identified two objectives:

1) To build and maintain an effective national cyberspace response system.

2) To implement a cyber-risk management program for protection of critical infrastructure.

The Cyber security Strategy for the Homeland Security Enterprise identified two strategic focus areas for the future of cyberspace security: "Protecting Critical Information Infrastructure," and "Strengthening the Cyber Ecosystem". Additionally, the Department of Defense in its Strategy for Operating in Cyberspace described the following five strategic initiatives for U.S. in cyberspace:

- Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
- Initiative 2: Employ new defense operating concepts to protect DoD networks and systems.
- Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.

2.4.3 The Law and the need for Warrants:

Cybercrime laws are covered in the Title 18 of the United States Code (18 U.S.C.), which is the Criminal and Penal Code of the United States. The Electronic Communications Privacy Act of 1986 and describes requirements for disclosures of data, conditions for mobile tracking devices and surveillance, and interception of communication data. It covers interception of wire, oral, or electronic communication and the preservation and disclosure of stored wire and electronic communication. In 1994 the US further modernized its lawful intercept

capabilities by passing the Communications Assistance for Law Enforcement Act. However, since 2001 the US has engaged in warrantless intercepts under its Foreign Intelligence Surveillance Act.

2.5 Federal Republic of Germany

Germany ratified the Council of Europe Cybercrime Convention in 2009.

2.5.1 Cyber-crime v. Cyber-warfare:

The penalties for cyber-crimes are highlighted in the Criminal Code, but there is no direct mention or definition of the term "cyber-crime" there. However, cyber-crime is discussed in the German Cyber Security Strategy of 2011. It is mentioned there that national capabilities to combat cyber-crime "must be strengthened" and in order to do it the government "will make a major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention.

2.5.2 Where is the Focus?

The clear definition of cyber-attacks is important in the formulation of Germany's Cyber Security Strategy, according to which, the government of Germany recognizes that cyber-attacks "may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines" and acknowledge that the threat may come not only from abroad (foreign/external cyber threat) but also from within the country (internal threat), and that it is very difficult to track the origin of a cyber-attack. The German strategic approach is focused on coordination and information sharing between private and public sectors of the country, and also on coordination with foreign and international security policies in particular, cooperation with the United Nations, EU, the Council of Europe, and NATO, the G8, the OSCE and other multinational organizations. In general, both Criminal Code and the Cyber Security Strategy pay special attention to espionage and sabotage, which are identified as types of cyber-attacks in the Cyber Security Strategy.

2.5.3 The Law and the need for Warrants

The German Criminal Code (as amended in 2009) lists the following:

Section 202a – Data espionage: Imprisonment not exceeding three years or a fine for unlawfully obtaining data or for unauthorized access to data (Subsection 202a(2) specifies in this and further presented in this report Sections from the Criminal Code that the implied data is "stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable"). • Section 202b – Phishing: Imprisonment not exceeding two years or a fine for data interception. • Section 202c – Acts preparatory to data espionage and phishing: Imprisonment not exceeding one year or a fine.

• Section 303a – Data tampering (unlawfully deleting, suppressing, rendering unusable or altering data): imprisonment not exceeding two years or a fine. The attempt is punishable too.

• Section 303b – Computer sabotage: imprisonment not exceeding three years or a fine if the damage is done to another person.

In 2010 the Constitutional court of Germany overturned a law from 2008 that required telecom companies to keep communications data (logs of calls, faxes, SMS messages, e-mails and history of internet use) for six

months. The law wasn't overturned completely though, despite that it's not allowed anymore to record telephone calls or read electronic communication messages, the retention of data is still permitted. The records would include evidence of who got in touch with whom, for how long and how often – without requiring any evidence of wrongdoing. A new amendment to Telecommunication Act will oblige service providers with more than 100,000 customers to allow the Federal Network Agency to automatically access data on behalf of investigative agencies without the knowledge of providers, while smaller providers will have to answer such requests within six hours.

2.6 French Republic

The increase of cybercrime in France is most often explained with the constant increase of internet users and with the observable fact that cybercriminals are continuously evolving from being single individuals to becoming a complex interconnected network, forming communities to exchange expertise and knowledge on how to conduct cybercrimes and attacks efficiently. France ratified the Council of Europe Convention on Cybercrime on January 10, 2006.

2.6.1 Cyber-crime v. Cyber-warfare:

Cybercrime is defined in France's Information Systems Defense and Security Strategy (2011) as "Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime."

"Cyber-attack" is defined in the 2008 French White Paper on Defense and National Security as a major attack, external or internal, against information systems.

Cyber terrorism and cyber warfare are also mentioned in the White Paper as major threats that need to be not only prevented, but also a response to such actions should be designed.

2.6.2 Where is the Focus?

France's Information Systems Defense and Security Strategy lists and explains four strategic objectives of the county in cyberspace:

1) Become a cyber-defense world power in cyber-defense.

2) Safeguard France's ability to make decisions through the protection of information related to its sovereignty.

3) Strengthen the cyber-security of critical national infrastructures.

The strategic focus of the country is clearly directed on retaining France's areas of sovereignty, protecting important businesses and government from espionage on the scientific, economic and commercial assets, protecting the nation from computer attacks. The 2008 French White Paper on Defense and National Security explains that "large-scale cyber-attacks on national infrastructures" is the biggest threat France would face over the next 15 years, which led to the development of the Information Systems Defense and Security Strategy specifically focused on the national defense capabilities and measures to be taken to strengthen cyber-defense.

2.6.3 The Law and the need for Warrants

The Penal Code of France (amended 2005) outlines the following crimes:

- Unauthorized Access to Automated Data Processing Systems – Article 323.
- Violations of Personal Rights Resulting from Computer Files or Processes – Article 226.

- Child pornography – Article 227.

2.7 Norway

The Budapest Convention on Cybercrime was ratified by Norway in 2006. 45,000 cyber-crimes were committed in Norway during 2012. The most targeted sectors in 2012 were military defence, oil and gas, energy, government and hi-tech industry. It's been estimated that Norwegian companies lost about NOK 20 billion because of cyber-crimes. However, not all of the cyber-crimes are being reported, because companies are often unaware of the attacks on their businesses.

2.7.1 Cyber-crime v. Cyber-warfare:

Does the Distinction Exist? The terms "cyber-crime" and "cyber-attack" are not defined in Norwegian law or in Norway's National Strategy for Information Security (Nasjonalstrategi for informasjonssikkerhet). However, the term "computer crime" appears in the National Strategy for Information Security, and "warfare against critical infrastructure" is discussed.

2.7.2 Where is the Focus?

The second chapter of the Strategy discusses the importance of ICT infrastructure and the challenges in protecting ICT systems from breaches and unlawful use. One of the paragraphs mentions that "warfare against critical infrastructure" is being developed in many countries, and that it must be assumed that this warfare is sophisticated enough to pose a major threat to the national critical infrastructure. It must be assumed that the attack will be directed against information resources, including computer systems that control critical infrastructure and industrial processes.

Other measures include continuing support for the Norwegian National Security Authority (Nasjonalsikkerhetsmyndighet or NSM), which is a "cross-sectorial professional and supervisory authority within the protective security services in Norway" that defines protective security as actions that are aimed "to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism". The NSM was established in 2003 and is responsible for the Security Act; Defense Secrets Act; Defense Inventions Act; the certification of information systems and products (SERTIT); coordinating role in preventative work and responses against IT security breaches aimed at vital infrastructure in Norway (NorCERT); and, developing the Norwegian Computer Network Defense (CND) strategy.

2.7.3 The Law and the need for Warrants:

The Norwegian General Civil Penal Code (2005) does not define cyber or computer crimes and the word "computer" does not even appear in the Code. Instead, the terms "electronic means", "technical devices" and "technical equipment or software" are used. Below are the sections from the Civil Penal Code that can be interpreted as applying to cybercrime:

Section 145. Unlawfully obtaining data or software (fines and/or imprisonment for up to 6 months).

Section 145b. Making available to others someone else's passwords or other data that can provide access to a data system (fines and/or imprisonment for up to 6 months).

Section 151b. Any person who by destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, electronic communication, or transport causes comprehensive

disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years.

2.8 Russian Federation

The authority in charge of solving cyber-crimes in Russia is Department "K" of the Ministry of Internal Affairs of the Russian Federation (Russian: Minister Delhi or MVD). In late 2012 MVD published their latest report with statistical data on crimes in high technologies (covering the first half of the 2012). The data indicates that for that period 5696 cyber-crimes were detected in Russia, up by almost 11% compared to the same period from 2011.

The leading Russian computer security company Group-IB states two reasons for the rapid and continuous increase in cybercrimes in Russia. First, the legislative system to combat cybercrimes is ineffective and the punishment for cyber-crimes in Russia is very mild: the sentences for computer related crimes are either very short or suspended. Second, different hacker organizations try to cooperate with each other to get higher profits and support their criminal enterprises.

The most popular cyber-crimes in Russia are:

1) Various online fraud activities (stealing funds from bank accounts, phishing, SMS text messages scams, stealing payroll records using viruses, etc.),

2) Spam distribution

3) DDoS-attacks.

Cyber-crime related to child pornography is a topic of special attention in Russia. In 2011 the government launched a nationwide program "Sornyak"93 to combat with this particular type of crime.

2.8.1 Cyber-crime v. Cyber-warfare:

Russian and Chinese authorities often use the term informationization in their strategic and policy documents, which means "the intensive exploration and use of information resources for social and economic development". In Russia, the word "cyber" is generally used only in media and academic publications. In the official policy documents the words "information" or "informational" are most often used instead as in information security, informational resistance, information space (instead of cyberspace), etc.

Even though the terms "cyber-crime" and "cyber-warfare" or "cyber-attack" do not appear in any of the official public documents, the use of terms such as "information security", "computer information crime" or "computer crime", and "informational resistance", makes it clear that the government distinguishes between regular cybercrimes and cyber-warfare.

2.8.2 Where is the Focus?

The Doctrine on Information Security of the Russian Federation (2000) is the main document that outlines Russia's national interests in the information area, which are:

1) Protection of the individual constitutional rights and freedoms related to information.

2) Raising awareness (international and within the country) about Russia's information policy.

3) Protection of information resources from unauthorized access, ensuring the security of information and telecommunication systems that are already deployed or being set up in Russia.

In 2010 a new Military Doctrine was published in which great importance was assigned to information security. It states that cyber security is the responsibility of the military. The Military Doctrine defines different types of the modern military conflicts and states that information resistance is one of the characteristics of such conflicts.

2.8.3.The Law and the need for Warrants

The laws related to criminal offences in cyberspace are outlined in the Criminal Code (1996) and in the Criminal-Procedural Code (2001). Chapter 28, "Computer Information Offences", of the Criminal Code includes:

- Article 272. Illegal access to computer information.
- Article 273. The creation, use and distribution of malicious software.
- Article 274. Misuse of means of storage, processing or transmission of computer information and telecommunications networks.

2.9 China:

Recent reports by UK and US-based private information security companies and government intelligence agencies suggest that China and Russia invest their resources in industrial espionage, and that the risks of cyber-attacks from these two countries are very high. Law firms have been identified as high-risk targets. Indeed, the international fear about the threat of cyber-attacks from People's Republic of China is growing rapidly. However, China also has its own internal concerns about protecting their cyberspace and fighting cybercrimes within the country.

2.9.1 Cyber-crime v.s Cyber-warfare:

Chinese laws and policies do not provide a clear distinction between cyber-crime and cyber warfare, or clear definitions. Over the past few years, a heated discussion has been raised between academics, private organizations and the public regarding the impact of cyber-warfare in China. In 2009, the state journal People's Tribune surveyed the public awareness of cyber warfare.

2.9.2 Where is the Focus?

The Chinese government appears to pay more attention to cyber-crimes that involve damaging the political stability and state unity rather than other cyber-criminal behaviors, such as online fraud. We have not uncovered public documents that discuss cyber-warfare or cyber-attacks by foreign interests.

2.9.3 The Law and the need for Warrants:

Several Ministries regulate cyber-crime and cyber-security in China. Among them are the Ministry of Information Industry, the Ministry of Public Security, responsible for internal security, and the Ministry of State Security, which handles external security. China's Criminal Law was amended in 1997, 2000, 2009 and 2011 to refer to cyber-crimes. The main provisions are as follows:

- Article 285a – Accessing [hacking] of computer systems in the areas of State affairs, national defense or sophisticated science and technology
- Article 285b – Obtaining of computer data and controlling of computer systems
- Article 285c – Provision of programs or tools used to access or control computer systems
- Article 286 – Sabotaging computer systems or data, that results in systems failure.

III. CONCLUSION

Interestingly, we have observed that most often the terms "cyber-crime" or "computer crime" are not defined, but only inferred in the laws of some countries. However, these terms, as well as the more explicit definitions of "cyber-attack" as an act distinct and more serious than a cyber-crime, can be found in the national strategic documents that usually serve as guidelines for government and sometimes the private sector. Based on the legal documents, governments are particularly concerned with such cyber-crimes as financial fraud, child pornography and illegal access to computer data every country reviewed in this report has introduced penalties for these offences. All of the countries covered in this report are currently drafting or discussing some changes in their legislation against cyber-crime and developing new units or agencies to address the issue of cyber-attacks. From the reviewed policies, strategic acts and agreements, there is a striking correlation to differentiate cyber-attacks from cyber-crimes, the strategic focus in cyber security approach shifts from simply detecting and combating criminal offences in cyberspace locally to a more complex efforts including protecting national infrastructure from cyber-attacks, either foreign or within the country.

REFERENCES

[1]. Available.[Online].https://en.wikipedia.org/wiki/Cybercrime.

[2]. Available.[Online].https://www.techopedia.com/definition/25600/cyberlaw.

[3].http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf.