Sri Lanka Institute of Information Technology

Cyber Security Laws

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT19961118	W M J P WIJESEKARA

Date of submission

Table of Contents

Abstract

A cyber attack is an attack dispatched by cybercriminals utilizing at least one PCs against a solitary or different PCs or organizations. A cyber attack can vindictively cripple PCs, take information, or utilize a penetrated PC as a dispatch point for different attacks. Cybercriminals utilize an assortment of techniques to dispatch a digital assault, including malware, phishing, ransomware, refusal of administration, among different strategies.

Cybersecurity law provides the confidentiality, integrity, and availability of public and private data, frameworks, and organizations, using forward-looking strict guidelines and motivators, with the objective of ensuring singular rights and protection, financial interests, and national security.

Technology has become exponentially in the course of recent decades. As time passes by, we persistently advantage from and increment our reliance on innovation. Web applications, drones, versatile applications, modern mechanization, and AI applications, and different advancements have transformed us. Yet, there are enormous risks that these technologies bring us. Along these lines, governments have presented Cybersecurity laws.

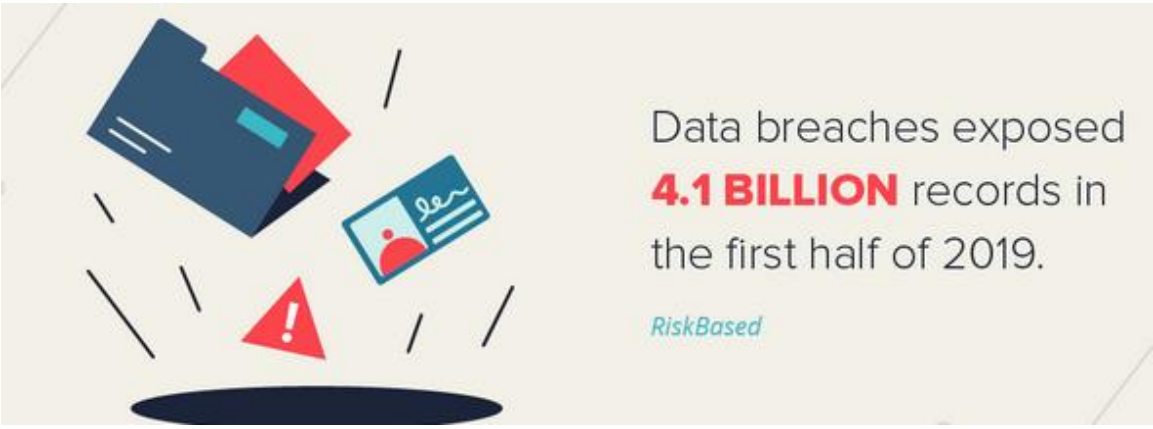
The last decade have seen a steady increase in these cyber crimes. This report contains some of the most serious of these cyber attacks. It further outlines the need for laws and regulations to prevent these crimes and the positive consequences of enforcing them.

1. Introduction

Secure their networks and information from cyberattacks such as viruses, worms, Trojan horses, phishing, attacks against denial of service (DOS), unauthorized access (theft of intellectual property or sensitive information) and attacks on the system.[1] There are various cyber - attack protection measures accessible.

Firewalls, anti-virus software, intrusion prevention systems, encryption, and login codes are included in cyber security measures.[2] In order to facilitate voluntary enhancements to cyber security, attempts have been made to enhance cybersecurity through legislation and joint efforts between the government and private sector.

Tensions are likely to continue to provide enhanced cybersecurity standards between domestic law enforcement efforts to conduct cross-border cyber-exfiltration operations and foreign jurisdiction.[2] Industry regulators, including banking regulators, have taken note of the cybersecurity risk and have either started or expected to begin to incorporate cybersecurity as an element of regulatory examinations.



2. Evolution of the Cyber Attacks

We have been aware of the continuous process of transformation in the natural world ever since Charles Darwin presented the theory of evolution in 1859. In the world of crime, things are no different. Criminals used ingenuity and cunning to rob cash and valuables while money was stored in bank vaults. These were the days of safe crackers and criminal masterminds, cops and robbers, bombs and getaway vehicles. Yet change is inevitable, as we know. As our market activities shifted online, a new modus operandi was created by robbers, improving their abilities as cyber criminals.

The spyware inserted into a vulnerability inside WhatsApp was a recent instance of this. Although the gap was quickly fixed by WhatsApp, we saw a new threat: through a cleverly designed call, the spyware could be injected into individuals' smartphones, without even having to respond. The spyware might turn on the camera of a phone once installed, scan emails and messages and collect the location and data of the user.

The rise in phishing attacks has been another trend. Although automated tools search for threats in incoming emails, phishing attacks seldom contain anything that can be recognized. Phishing attacks actually leverage the human factor, lulling unsuspecting people into a false sense of security inside an organization and inducing them to split access information into network systems. These emails, messages or sites, claiming to be from trusted sources, may appear to be genuine at first glance. And just as soon as they appear, they can vanish, making it difficult to recognize or locate them. The first any realize is when they learn that their framework has been broken.

One especially inventive form of phishing attack first emerged in 2017 but is still being used since the unaware and (potentially) helpless are successfully preyed upon. These are fake work ads that get individuals to fill out application forms that reveal confidential personal details. These scams often trick people into calling premium rate telephone lines for interviews, engaging in money laundering through job-from-home scams, or paying extortionate fees for non-existent background checks, online training, visas, or insurance. SAFERjobs, a Metropolitan Police-created non-profit organization, reports that we have seen a 300 percent spike in recruitment-related fraud in the last two years.

So how do we protect against these ever-evolving threats? In order to defend us, patience and caution will go some way. Invaluable techniques are also workers understanding and preparation. Yet we need to think like them in order to really outsmart some of the brightest minds. We have to move from a step behind to a step forward. We need to assess our own processes for bugs, to monitor, monitor and continuously improve our business practices.

In addition, a comprehensive analysis of the Business Continuity and Incident Management plans requires a complete test and training strategy which can include policy assessments and a report complete of recommended remedial measures. In short, there are a lot of ways we will continue to grow in the same way as cyber criminals do today. And, going into the second half of 2019, it has become very clear that doing nothing is the most terrible thing.

3. Emerging Cyber attacks

- In 2022, the worldwide demand for information security is expected to hit $170.4 billion.
- In 2018, 62% of corporations witnessed phishing and social engineering assaults.
- 68 percent of business leaders believe their cybersecurity threats are rising.
- Just 5% of directories in businesses are adequately secured, on average.
- In the first half of 2019, data breaches revealed 4.1 billion documents.
- 71 percent of violations were financially motivated and 25 percent were spying-motivated.
- 52% of violations included hacking, 28% included malware and 32-33% included phishing or social engineering, respectively.
- There were 8,854 reported violations between January 1, 2005 and April 18, 2018.
- While total ransomware infections were down 52 percent, in 2018, enterprise infections increased by 12%.

4. Need of Rules and Regulations for Cyber Criminal Activities

1. Prevent the spread of false propaganda that could tarnish the reputation of a person or a public business and character assassination and take legal action against it.

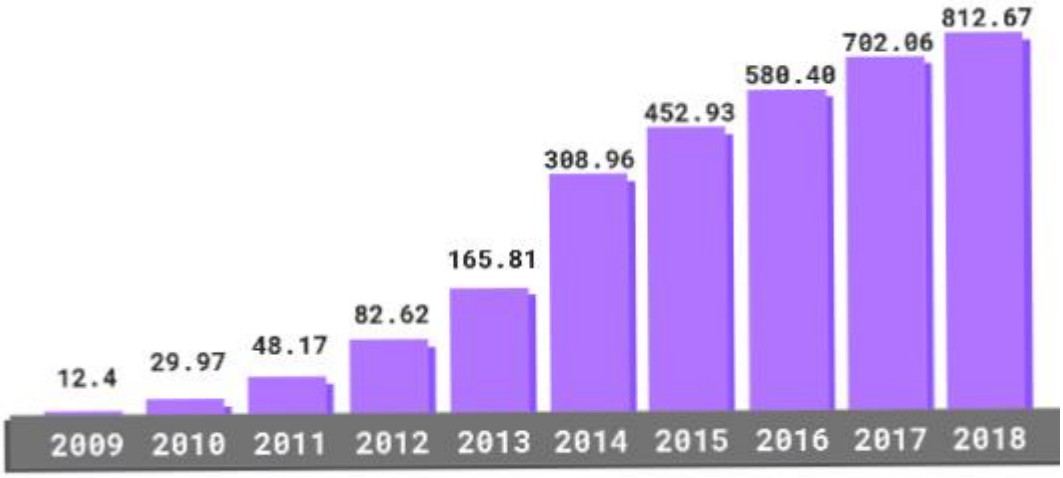
2. Protect the human rights of all people and take legal action against those who violate human rights through social media or the Internet.

3. Prevent crimes such as hacking into the database of a person or organization or stealing data or selling data to another entity or entity on a financial agreement or releasing sensitive data on the Internet that could harm the personal identity of that person or business company and Take appropriate legal action against such data fraudsters.

4. Prevent international fraud and bring criminals to justice by breaking into financial institutions and financial accounts, destroying usernames and passwords, and stealing money from those accounts.

5. Preventing crimes such as trespassing on the social media accounts of an individual or an organization, blocking access to the real owner of the account and doing various things that could tarnish his reputation and enforcing penalties on hackers.

6. To provide the opportunity to navigate cyberspace to ensure reliability in the use of the Internet.



Total Malware Infection Growth Rate (In Millions)

5. Content of the Laws

The Territoriality Rule

The information infrastructure situated within its territory is subject to the radical sovereignty of the states.

In view of the global nature of cyber attacks, there is ongoing debate about whether territorial legal structures can cope, but the lessons of Estonia, Georgia and other large - scale cyber incidents show that by fine-tuning their national regulations, nations can and must make better realistic use of legal remedies and concepts accessible under national law Through fine-tuning their national rules. The highest IPS and many key aspects of successful cyber defense depend on the quality of the National Law. Digital communications illegal function investigative authority Corporation. Until the possibilities for implementing and analyzing national legal methods are exhausted, it is hard to determine what remedies, if any, need to be agreed at the global scale.

Cyber infrastructure is subject to the jurisdiction of the Flag State and is subject to the nation's sovereign rights. For instance, every government can exercise effective control over the IT infrastructure located in its territory by ensuring the availability and quality of logs by keeping an overview of electronic communications providers by developing an understanding of the threats and capabilities that exist within its jurisdiction to deal with and organize incidents and maintaining the development of information society with the interests of national security.

The principle of territoriality empowers nations to impose their sovereignty on information infrastructure located within or otherwise subject to their jurisdiction within their territory. The state 's responsibility to preserve its own networks is supported by internationally recognized concepts of non-intervention and sovereign rights.[6]

The Responsibility Rule

The fact that a cyber attack was launched from an information system located in the territory of a state is evidence that state is responsible for the act.

If the cyber procedure was initiated or otherwise originated from governmental cyber infrastructure, there is a refutable presumption that the process is linked to the state in question. Therefore, countries need to consider the potential to be held liable for threats or other activities using their information infrastructure. They will face public condemnation and they will be expected to respond to investigations and help them. For countries whose infrastructure has been involved, information leading to the identification of the source of the attack or of the perpetrators, the methods and tools involved, and even active law enforcement measures such as confiscation, arrest and prosecution should reasonably be expected.

Tallinn, for instance, accused Moscow of cyber targeting vital Estonian government and private infrastructure networks in 2007. Among other items, this attribution was built on Russia's reluctance to assist in efforts to reveal the specifics of the attacks. Russia has also been linked to the cyber attacks against Georgia and Lithuania in 2008.[7] China is equally responsible for launching cyber-espionage attempts against the information networks of the united states and other countries.[8]

Through having greater control over the use and misuse of the information infrastructure under their authority, countries can also be required to increase their own stages of cyber security. Of course, on a case - by - case basis, the balance between economics and interests would have to be stuck.

There is no support for the Attribution principle in current international law on state liability. Efficient monitoring and overall regulation are the two main norms. According to the Nicaragua case of 1986, successful control (financing, coordination, supply and equipment preparation, target selection and planning of the whole operation) is not sufficient to meet the threshold.[9] It was concluded in the Tadic case of 2003 that overall influence goes beyond planning and managing military operations.[10] Constructs for attribution are recognized in international environmental law where evidence of immediate intervention is absent**.**

The Cooperation Rule

The point that a cyber attack has been carried out by information systems located in the territory of a state induces a obligation to comply with the victim state.

The interconnectedness of the global information networks makes it impossible for any country, without cooperating with nations whose infrastructure can be used to navigate such an attack, to defend itself against a cyber attack. There is also a need for more successful collaboration between public and private institutions and between legal , political, military and technologists.

If the vast majority of the information infrastructure is privately owned and controlled, the reliance on public information systems and networks funded by the private sector on a contractual basis is considerable. Cooperation can take the form of consultation, sharing of information, and resource reallocation. As well as supporting the under assault programs. The legal structure for cooperation will be enabled by national laws concerning ISP cooperation, data sharing and alliances, as well as coalition agreements. The Cybercrime Convention encourages parties to collaborate to the maximum extent possible for the purposes of inquiries or prosecutions involving criminal offences related to information systems and computer networks, through the implementation of relevant international treaties on international cooperation in criminal matters, agreements decided on the basis of uniform or mutual legislation, and domestic laws.[11] The principle of cooperation can also be identified in the Treaty on the North Atlantic. Whereby the parties shall consult jointly whenever the territorial integrity, political independence or protection of either of the parties is threatened, in the opinion of each of them.[12]

The Self-Defense Rule

Everyone has the right to defend themselves.

Both criminal and international law are part of the principle of self-defence. In theory, everybody, subject to the proportionality and necessity of such operation, has the right to self-defence.

In criminal law, there is no responsibility for what would otherwise be illegal acts of self-defence if the victim reasonably suspects that excessive force is about to be used against him. This is not to suggest that the principle will explain any cyber 'hack-back'; it should be a last resort solution.

The conditions for invoking individual and collective self-defence at the international level are based on customs, the Charter of the United Nations and international case law. If it rises to the level of a 'armed attack', a cyber attack invokes individual and collective self-defence. National authorities or, for joint action, international partners (for example, the North Atlantic Council depending on Article V of the NATO Treaty) would be responsible for deciding whether a cyber-attack is equal to such an attack by virtue of its impact, implications or existence. Under Article V, an armed attack against one or more of the parties in Europe or North America shall be treated as an attack against all of them and, where such an armed attack occurs, each of them shall assist the attacked party or parties in the exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations.[13]

So far, this threshold has not been reached by a cyber attack and there has been no military response to a cyber attack yet. If it is appropriate to put an end to the attack and the response is proportionate to the method and effect of the attack, a kinetic response in self-defence against a cyber attack might be legitimate.

The Data Protection Rule

It is important to carefully monitoring the need for network surveillance and sharing of information against the right of individuals to privacy. Currently, there is a significant difference between legal and technological data approaches and their protection.[14] Although monitoring of network data in technical communications appears to be well-established and routine, it poses important concerns among legal experts.

Under the EU Data Protection Directive,[15] any information relating to a natural person known or identifiable shall be considered as personal data. In enforcing the Guideline, the prevailing view is that IP addresses are personal data and are subject to processing restrictions under national legislation.[16] Such restrictions include requiring the data subject 's consent to the processing of such data, prohibitions on the transfer of such data subjects to third countries for the processing of such data, and possible inadmissibility as proof of Pursuant to the EU Data Protection Directive, the transfer of personal data to a third country can take place only if an acceptable level of pre-protection is maintained by the third country.[17]

These prohibitions can prevent attempts at national level to recognize, attribute or avoid cyber-attacks, but exceptions in the public interest and for national security are allowed by the Directive. Exceptions still occur for criminal trials. It will help to create the right balance between privacy and surveillance by clearly defining the need and methods for data and packet inspection.

The Duty of Care Rule

Everyone has the duty to ensure that their information infrastructure has an acceptable level of protection.

The concept of duty of care is well known in many areas of law: an individual is obliged to ensure the security of the personal data processed by him or her and due diligence responsibilities derive from the legal framework of data security , information society systems, worker protection, etc.

Under the EU Data Protection Directive, for instance, the controller of personal data must take reasonable technical and organizational measures to protect such data against accidental or malicious destruction or accidental loss, adjustment, unauthorized disclosure or control, in particular where the transmission of data over the network and against any other unlawful form of processing is required. These measures shall ensure a standard of security suitable to the risks posed by the manufacturing process and the quality of the data to be obtained, taking into account the state of the art and the cost of implementation.

The Council of Europe Convention for the Security of Persons in relation to Automated Processing of Personal Data (1981) is a similar floating norm. In order to protect personal data contained in automated data files against accidental or unwanted destruction or accidental loss, as well as against unauthorised access, modification or distribution, Article 7 requires adequate security measures to be taken.

The duty of care definition can be applied to establish security standards for sensitive information infrastructure and governmental or military information services as cyber threats with political dimensions become more prevalent.

The Early Warning Rule

There is a responsibility to alert possible victims of known cyber threats that are coming.

In 2008, after the Lithuanian Parliament adopted a law preventing (among other things) the use of Soviet symbols, 300 Lithuanian websites were defaced with the hammer and sickle symbol. A single, easily patched ISP vulnerability was involved in the attack itself, but the response had wider ramifications: having learned of the impending attacks, the ISP gave an early alert to its clients and notified them of the incident.[18] If broadly applied, cyber security could be greatly enhanced by this strategy.

The fact that government entities were given advance notice of the attacks highlights the requirements for government information technology service-level agreements (SLAs) and the need for a non-discriminatory responsibility to alert both public and private sector internet service providers and web hosts of known threats.

To a great extent, the question of SLAs is a matter of national legislation or touch. The responsibilities of service providers to ensure the protection of services emerge from the ePrivacy Directive EC/2002/58.[19] For Lithuania and other members of the European Union, this Directive invokes a general duty to take effective technical and organizational steps to safeguard the protection of the services of the provider. The service provider could, if possible, coordinate further action with the public communications network provider to which it links. Member stats can, in compliance with the E-Commerce Directive, create obligations for information society service providers to notify the competent public authorities promptly of suspected illegal activities.[20]

The Access to Information Rule

The public has a right to be informed about threats to their life, security and well-being.

There is strong trend in Europe towards transparency of governmental acts and records, giving the public the right to be informed about threats and decisions related to their life and well-being. A holder of information is required to disclose existing information to danger to the life, health and property od persons.[21]

The presumption is that public-sector information should be publicly accessible unless there are compelling reasons otherwise. While access to information can allow the public to learn of threats and attacks and can raise awareness about cyber security, it may also result in unwanted publicity.

Private-sector organisations worry that disclosure of cyber attacks against them, and their results, might reduce trust in their business model or services. But government responses politically motivated cyber attacks often require publication of such information. A balance needs to be stuck between these public and private-sector interests. Open discussion of the details of methods, targets and effects of an attack may also increase vulnerability, as it can tell the attackers things they would not otherwise know.

The legal framework for access to information will be an important aspect of cyber security in the context of strategic communication and public awareness.

The Criminality Rule

Every nation has the responsibility to include the most common cyber offences in its substantive criminal law.

Instead of something qualitatively new, the criminality rule is a reminder. In criminal law, it is well known that only if such activities count as criminal offences will cyber attacks be investigated and prosecuted.

Therefore, unless the particular action or consequence is defined as a crime under national law, it is virtually impossible for the state to punish anyone involved in a cyber attack. Cyber crime that is politically motivated is, for the most part, a threat to society in general rather than to particular individuals or organizations, and could involve a different approach than cyber crime that is economically motivated.

As a result of political tensions, the Lithuanian case showed that random private-sector targets can come under cyber attack. The Estonian case showed that politically motivated distributed-denial-service-attacks can nonetheless effectively disrupt communications inside and with the government in a country with a very low rate of cyber crime and leave national law enforcement agencies empty-handed, even though they have ample investigative powers. The Georgian case shows how conducting kinetic warfare with no meaningful legal redress would contribute to the military effort.

A strong starting point for improving and harmonizing national legal responses to cybercrime is the current international agreements, such as the Council of Europe Convention on Cybercrime,[22]. Each Party shall take such legislative and other steps as may be appropriate to constitute, as a criminal offense under its domestic law, access to all or any portion of the computer system without right when committed internationally.[23]

The Mandate Rule

The capacity of an agency to act (and regulate) comes from its mandate.

For the concept and coordination of international efforts in global cyber security, the mandate rule is important. Its basic functional significance lies in the creation of new or revision of existing agendas for cyber security.
Examination of current cybersecurity-related legal and policy instruments shows overlaps and discrepancies in international coordination.[24] For example, at least six major international bodies have been working on international harmonisation of cyber crime. This poses the issue of the required input of each State Party to a national cyber security system for a variety of such organisations.

International organizations should make use of and develop the efforts of other organisations to justify governmental investments in their cyber capabilities. Although, for example, NATO's primary focus in the field may be on collective self-defense measures, it also needs a structure for dealing with cyber incidents below the threshold of a cyber-armed attack, whether aimed against the organization itself or individual member states. Cyber security is always closer to mounting a cyber attack, and improving national and foreign technologies will become an investment concern as government information technology becomes a more frequent goal. NATO's niche may be the selection, sharing and implementation of best practices to deal with cyber attacks with national security implications or cooperative defense and security concerns.

* * *

These ten rules outline key concepts and areas that must be included or addressed in a comprehensive legal approach to cyber security.

6. Future Trending Attacks

This is a selection of emerging and current threats to cybersecurity that you will possibly learn more about this year.

1. Deepfakes

Deepfakes is a mixture of the terms "deep learning" and "fake." Deepfakes occur when fake images and sounds that appear real are created by artificial intelligence technology.

A deepfake may generate a video in which the words of a politician are distorted, making it look like a political leader said something they never did.
The images of famous actors or other celebrities are superimposed on the bodies of other people by other deepfakes.

2.Deep fake voice technology

This technology enables individuals to use artificial intelligence to spoof the voices of other individuals, often politicians, celebrities or CEOs.

3.Synthetic identities

Synthetic identities are a type of identity fraud in which scammers use a mix of credentials that are real and fake to construct a real person's illusion.
A criminal may, for example, construct a synthetic identity that requires a valid physical address. However, the Social Security number and birth date linked to that address may not be valid.

4.Cyberattacks powered by AI

Evolving Artificial Intelligence. However, it is most prone to cyberattacks when studying a new model or system.

Cybercriminals will inject bad data into an AI program in such attacks, known as poisoning attacks. This bad knowledge can then lead the AI system to learn something that it is not supposed to do.

An illustration? To get around spam detectors, some cybercriminals have used poisoning attacks on AI devices.

5. Social media misinformation

You have undoubtedly used the word "fake news." This is often referred to as misinformation, the intentional distribution of news reports and false facts intended to convince individuals, often voters, to take certain actions or hold certain beliefs.

Via social media like Facebook and Twitter, social misinformation is also distributed. During and after the 2016 presidential election, "fake news" became a hot subject.

6. New cybersecurity challenges created by 5G networks

Tech experts worry that 5G would generate new obstacles for corporations and policymakers in terms of cybersecurity.

Information Risk Management's 2019 report, entitled Risky Business, said survey respondents were concerned that 5G technology will lead to a higher risk of cyber attacks on Internet of Things (IoT) networks.

They also cited a lack of 5G hardware and firmware protection as a problem.

7. Quantum computer advances pose a challenge to cryptographic systems

The principle of quantum computing is still recent, but this is a method of computing at its most fundamental, which can use some elements of quantum mechanics.

For cybersecurity, what's important is that these computers are fast and strong. The risk is that quantum computers can decode cryptographic codes that, if they ever did, would take conventional computers even longer to crack.

8. Cyberattacks on cars

The threat of vehicle-based cyber attacks is growing as more cars and trucks are linked to the Internet.

The fear is that cybercriminals would be able to hack vehicles to steal personal data , monitor these vehicles' location or driving history, or even disable or take over security functions.

9. Cloud jacking

Cloud jacking is a type of cyberattack in which hackers infiltrate, store in the cloud, enterprise programs and systems, and use these tools for cryptocurrency mining.

10. Cyberattacks on less-developed countries

In developing countries, people may be more vulnerable to cyberattacks.

People also perform financial transactions over unsecured cell phone lines in these countries, rendering them more vulnerable to attacks.

11. Security of elections

The U.S. government fears that hackers from other countries could target state and local government voter registration databases with the purpose of either destroying or disrupting this information. This might discourage individuals from being able to vote.

The U.S. government, therefore, has improved efforts to safeguard this election data from criminals.

12. Attacks on the public sector with ransomware

Hackers enter the computer systems of an end user in a ransomware attack, normally freezing them. Only if the victim pays a ransom will these attackers activate the infected systems.

Today, hackers also attack government bodies' computer systems, including counties, public utilities, and fire and police departments, hijacking their computer systems before a ransom is paid by these government agencies.

13. Privacy of data

A vast amount of essential data is kept by businesses, care professionals and government departments, ranging from patients' Social Security numbers to clients' bank account numbers.

Data privacy refers to a security division based on how this information can be secured and kept away from hackers and cybercriminals.

14. Breaches in hospitals and medical networks.

For cybercriminals, hospitals and other medical facilitators are prime targets. That's because the personal and financial details of so many patients are accessible to these media providers. This data, which hackers can then sell on the dark web, can be exposed through data breaches.

7. Conclusion

In today's society many people have increased knowledge about IT or computer literacy but very little knowledge about cyber security. therefore; Cybercrimes such as ransomwares, spywares and data breaching are on the rise. According to my point of view, knowledge on basic topics such as cyberspace, cyber-attack and prevention methods etc. should be socialized. We can do this in a few steps.

- School education related to information technology should include a basic analysis of these cyber-attacks and hackers.
- Awareness of what an individual can do to avoid these cyber-attacks and hackers.
- As a third step, higher education on cyber security should be significantly improve through the television, radio, social networks, conference and seminar.

What is a cyber-attack? How can we avoid this? How to set a very strong password? Etc. The basics should be constantly socialized.

Finally, this project aims to create a law-abiding society aware of cyber security strategies.

* * *

8. References

1. For details about the 2007 attacks and the legal considerations involved,Cyber Incidents: Legal Considerationms (Tallinn: CCD COE Publishing, 2010).

2. For Operation Aurora http:// www.damballa.com/research/ aurora/; for Conficker http://www. Confickerworkinggroup.org/wiki/ pmwiki.php/Main/HomePage; W32.Stuxnet Dossier, Version 1.3 (November 2010), http://www.symantec.com/ content/en/us/enterprise/media/ security_response/whitepapers/w32 stuxnet_dossier.pdf, p. 4.

3. For details about the Estonian legal lessons learned and amendments to national laws, Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007, International Cyber Security Legal and Policy Proceedings (Tallinn: CCD COE Publishing, 2010), pp. 40-67.

4. the 2009 Cyber Conflict Legal and Policy Conference organised by CCD COE. The agenda of the Conference is available at http://www.ccdcoe.org/ legalconference/.

5. At the 2010 CCD COE Cyber Conflict exchange, state responsibility, criminal cooperation and the applicability of international law - were addressed by legal experts from at least two key areas (data exchange from the cyber law and criminal law perspective, criminal cooperation from the criminal law and national-security law perspective, and so on), with the intent to identify gaps between these areas of law and come up proposals on how to improve the existing legal framework. The agenda of the conference is available at http://www.ccdcoe. org/conference2010/agenda.html.

6. UN General Assembly Resolution 1514, at 67, UN GAO R, 15th Sess., Supp. No. 16, UN Doc. A/4684A, 14 December 1960.

7. International Cyber Incidents.

8. for example, Dan Goodin, "India and Belgium Decry Chinese Cyber Attacks', The Register, 8 May 2008, http://www.theregister. co.uk/2008/05/08/belgium_india_ china_warnings; John Leyden, 'France Blames China for Hack Attacks', The Register, 12 September 2007, http:// www.theregister.co.uk/2007/09/12/ french_cyberattacks; Rhys Blakely, Jonathan Richards, James Rossiter and Richard Beeston, 'MI5 Alert on China's Cyberspace Spy Threat', Times, 1 December 2007, http://business.timesonline.co.uk/tol/business/industry sectors/technology/ article2980250.ece.

6. 1984 ICJ REP. 392, 27 June 1986.

7. Case No. IT-94-1 (International Criminal Tribunal for the former Yugoslavia, 1995).

8. Cyber Crime Convention, Article 23.

9. Article IV of the North Atlantic Treaty.

10. Article V of the North Atlantic Treaty.

11. 14 IP Addresses Subject to Personal Data Regulation, International Cyber Security Legal and Policy Proceedings (Tallinn: CCD COE Publishing 2010), pp. 24-39.

12. Directive 95(46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 - 0050. Available at http:l/eurlex.europa.eu/ LexUriServ/LexUriServ.do?uri-CELEX:31995LO046:en:HTML.

13. IP Addresses Subject to Personal Data Regulation.

14. EU Data Protection Directive 95/46/ EC. Article 25(1).

15. For an overview and legal assessment of the Lithuanian incident, International Cyber Incidents.

16. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002 P. 0037 0047. Available at http://eur-ex. europa.eu/LexUriServ/LexUriServ.do? uri-CELEX.32002L0058 EN:HTML

17. EU E-Commerce Directive, Article 15 (2).

18. Estonian Public Information Act, para. 28(1)7.

19. The Council of Europe Convention on Cybercrime (ETS 185, signed on 23 November 20001, entry into force on i July 2004), aiming to facilitate international cooperation, detection, Investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction, is open for signature by the member states and the non-member states which have participated in its elaboration and for accession by other non-member states. As of December 2010 the total number of signatures not followed by ratifications was 17; the total number of ratifications/ accessions was 30 (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Macedonia, Ukraine and, as a non-

member, the United Statesj. Available at http://conventions.coe. int/Treaty/Commun/QueVoulezVous. asp?NT-185&CL-ENG.

20. Council of Europe Cyber Crime Convention, Article 2.

21. For an overview of current international legal and policy instruments on cyber security Frameworks for International Cyber Security, Law and Policy Instruments (Tallinn: CCD COE Publishing, 2010).