CRITICAL RESEARCH STUDY ON PREVENTING CYBER CRIMES THROUGH EFFECTIVE CYBER LAW CONCEPTS AND POLICIES FROM GLOBAL .PERSPECTIVES

BY

ANSAM QASIM HACHIM

Imam Kadhim(a) collage for Islamic science

Email; ansam2hachim@gmail.com

ABSTRACT

Cybercrimes has continued to grow over the years with new crimes been introduced into the deep web. The trend in recent attacks across the globe has shown the versatility of the perpetrators and what they are capable of doing. The impact, effect and reality is has on organisations worldwide cannot be over emphasized. Cyber laws have also been incorporated over the years, to be implemented at various level and jurisdiction. The trend of attacks and growing urge among perpetrators has called for concerns on what the incorporated cyber laws have done to curb the growing crime. This paper examines cybercrimes and cyber laws in order to be able to make the laws effective and further implement it in preventing more cybercrimes

Keywords: Cybercrimes, Cybercriminals, Cyber Laws, Cyberspace, Deep Web, Cyber Attacks, Cybersecurity, Network Access, Denial of Service, International laws

الملخص

استمرت الجرائم السيبرانية في النمو على مر السنين حيث تم إدخال جرائم جديدة في شبكة الإنترنت العميقة. وقد أظهر الاتجاه في الهجمات الأخيرة في جميع أنحاء العالم مدى تنوع مرتكبي الجرائم وما يستطيعون فعله. لا يمكن التأكيد على التأثير والأثر والواقع على المنظمات في جميع أنحاء العالم. كما تم دمج القوانين السيبرانية على مر السنين ، ليتم تنفيذها على مختلف المستويات والاختصاص القضائي. وقد دعا اتجاه الهجمات والحاجة المتزايدة بين الجناة إلى مخاوف بشأن ما قامت به القوانين السيبرانية المدمجة للحد من الجريمة المتنامية. تبحث هذه الورقة في جرائم الإنترنت والقوانين الإلكترونية من أجل أن تكون قادرة على جعل القوانين أكثر فاعلية وتطبيقها في منع المزيد من الجرائم السيبرانية

الكلمات المفتاحية: جرائم الإنترنت ، مجرمو الإنترنت ، القوانين السيبرانية ، الفضاء السيبراني ، الشبكة العنكبوتية ، الهجمات السيبرانية ، الأمن السيبراني ، الوصول إلى الشبكة ، رفض الخدمة ، القوانين الدولية

INTRODUCTION

Cybercrimes is not a new phenomenon but perpetrators might have discovered a lot more new approaches of committing cybercrime. By definition, as described by Margaret (2010) "*Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone*".

The Council of European Convention on Cybercrimes (CECC) described cybercrime in a more detailed manner stating "*cybercrime is a wide range of malicious activities including the illegal interception of data, system interferences that compromise network integrity and availability and copyright infringements*"

In view of these numerous activities across the globe, cyber laws have been incorporated to help tackle the rise in cybercrimes. A deeper examination reveals that most countries have their respective cyber laws constituted and integrated based on the types of crimes they experience most. All countries have their cyber laws with the ultimate goal, to curb, suppress and minimise cybercrimes. An examination shows a high increases in cybercrimes and attacks in recent years has called for questioning as to the kind of cyber laws that have been incorporated, their effectiveness in actually preventing cybercrimes. In order to be able to actually determine the impact and the role cyber laws have played, there is a need to critically examine categories of cybercrime, types of cybercrime, preventive measures as well as cyber laws that are incorporated to combat these crime. There is a need to also examine the effect as well as reality.

STATISTICS

Statistics shows the past, the current and future trends and for cybercrimes, it will only get worse, except new drastic cyber laws are put in places to curb the rising trend. According to Steve (2018) and Briana (2017):

- Cybercrime damage in terms of cost is expected to hit about $6 trillion annually by 2021
- Cyber security spending is expected to exceed #1 trillion from 2017 to 2012
- Cybercrime will be more than triple the number of unfilled cybersecurity jobs, this is expected to reach 3.5 million by 2021
- Human attack surface is expected to reach 6 billion people by 2022
- Global ransomware damage in terms of cost is expected to exceed $5 billion as at end of 2017
- Growth of new malware is a trend expected to rise
- Ransomware is expected to be on the rise

A critical examination of the statistics clearly shows that the implementation of the cyber laws has not really made much impact in curbing cybercrime and related activities. In order to be able to actually examine why cyber laws haven't made much impact and what could be done to improve its effect, there is a need to examine categories of cybercrimes. The ability to be able to identify the categories will help in enacting laws that would help address a particular category

CATEGORIES OF CYBERCRIME

There are basically three main categories of cybercrime that is usually taken into consideration whenever dealing with cybercrime issues. These are:

- **Crimes Against People (Individuals)**

These are crimes committed against a group of people or individuals and most of them occur online. The effect is that it literarily affect the lives of the individuals involved in one way or the other. Typical examples are identity theft, human trafficking, various types of spoofing, credit card fraud and related issues and offences, distribution and re-distribution of child pornography, cyber bullying as well as cyber harassment and stalking.

- **Crime Against Property**
  These are crimes committed against properties which could belong to an individual, a group of people or small, medium and large organisations. The properties might include computers, servers or mobile phones or even personal devices. The attacks usually come in form malfunction or virus attacks. Typical examples include, hacking, Dos Attacks, IPR violations, virus transmission, computer vandalism, copyright infringement as well as cyber-squatting.
- **Crime Against Government (Authority)**
  This is a crime usually target against government offices, parastatals or agencies. This is also considered an attack on the nation's sovereignty, usually considered an act of war. Typical examples of piracy or pirating software, cyber warfare, cyber terrorism, illegal access of confidential files as well as hacking of highly classified documents

The different categories of cybercrimes have been examined, there has been laws created to curb these crimes but it's as if the effect of these laws haven't been that much of an impact as presumed. In order to be able to know how to successfully implement these laws to get the desired result, there is a need to critically examine the crimes related to the different categories in order to be able to come up with effective implementation strategies using already created law or further create new laws to that effect. But first, the need to understand how these crimes are committed as well as who cyber criminals might be to as to raise the awareness for easy identification.

HOW CYBERCRIMES ARE COMMITTED

Cybercrimes are committed using computers in three main ways which are

- **Target**
  Cyber criminals can attack other people's computer without the knowledge whatsoever and carry out very devastating activities. These activities can include virus spreading, identity theft, as well as other related crimes that would in one way or the other cause damages to the individual that owns the computer.
- **Weapon**
  Cybercrimes can be committed by criminals using other people's computer as their weapon without them knowing their tools has been compromised. Crimes in this regards can include spam, fraud as well as illegal gambling. The result of this is that the owner of the computer been used as weapon is the one that would eventually get into trouble.
- **Accessory**
  Cybercrimes can be committed by criminals when they use other people's computers as an accessory without their knowledge whatsoever to save stolen

or illegal data. This is common especially when a government agency has been attacked, in order to make identification difficult, perpetrators decide to use other people's computer as accessories

WHO COULD BE A CYBER CRIMINAL?

Cybercriminal could be anyone of any professional in any organisation with bad intentions towards the organisations they work for as they work in organised group and can be:

- Programmers who write code or programs that are eventually used by cybercriminal organisations
- Distributors who distribute or sell stolen data and goods from cybercriminals
- Hackers who constantly exploit organisational systems and networks as well as applications
- IT experts that maintains organisation's IT infrastructure such as servers, databases and other integrated technologies
- System hosts and provides that host websites and server that possess illegal content such as child pornography
- Leaders that are connected to big bosses of huge criminal organisations that assemble as well as direct cybercriminal teams.
- Money mules that manage bank account and wire transfers

CYBER CRIMES TYPES

There are a lot of cybercrimes but in recent times, some have become used more than other and have had devastating effect on its targets. In all one cannot count the number of cybercrimes that are in existence. The recommendation is there are some everyone must know because of the effect it has on any target. Here are 10 cybercrimes people need to be aware of

Malware/Malvertising: Malware explains the use of malicious software to either harm or totally compromise a computer, mobile device or cloud based solutions that receive, stores and transmits data. it can also be used to monitor a lot of online activities, track vital information in the process collecting the details and sent back to the criminals who eventually exploit that data. The most common are spyware and bots. Malvertising is used to refer to different kinds of harmful software such as viruses, Trojan and worms that latch of a computer without their presence ben known

Identity Theft: This is also referred to as internet theft, it is a family name used to categorise any kind of theft that takes place over the internet. Identity theft is achieved when personal data of an individual is intercepted and used in malicious activities such as online mass shopping, to act if it is the actual person.

Phishing: Phishing involves a cybercriminal that tries to trick individuals into giving out their personal information such as bank account numbers, account passwords as well as credit card number. They usually contact intended target via email, text messages, phone calls or even through social media pretending to be legitimate registered business like internet provided, bank or even Telephone Company.

Child Soliciting and Abuse: This is a type of cybercrime where criminals solicit children through chat rooms for the sole purpose of pornography. It can also come in a way or form that shows, explains or describes sexual abuse and content towards children. The definition of a child is someone below the age of 16. This has grown a lot in the last 20 years especially in Eastern-Europe

Online Scam: Just as the name implies, any scam that is done or happens online is an online scam. Perpetrators do this by tricking individuals into giving out their personal details using an ad pop up saying they have won something and then ask for card details to pay for shipping. Weird transactions from your bank account confirms that you have been scammed.

Virus Dissemination: Virus is a program that maliciously infects a computer and makes it to malfunction. Viruses also carry a piece of malware with them and spreads it across to softwares installed on the computer system. Full quarantine and safe environment to test is usually the only way to remove a virus totally from a computer system.

Electronic Money Laundering: Large sums of money that are generated illegally definitely would be laundered first before it can be accessed to be spent on invested. Electronic money laundering involves movement of large sums of illegally generated money through bank to bank transfers usually called "wire transfer"

Cyber Bullying: this is similar to cyber stalking but in the case the messages sent across can be very harmful, abusive as well as offensive. This can also be done when videos or picture posted offends the victims. This is another trend that has been on the rise lately and authorities of different countries have shown concerns of the future effect

Hacking: Hacking is the term used to describe the process whereby a stranger access your computer system without your permission and knowledge. This could be for a number of reasons such as greed, to test expertise and fame. However, in as much as it is an illegal access, it is considered hacking. Some may gain access in order to steal personal information and use it to commit another offence. Most hackers are computer programmer who have deep understand of how computer system works and how they can be manipulated to that effect.

Cyber Stalking: This involves monitoring from someone that knows the victim as the victim is subjected to online harassment in different forms such as email and messages. The sole aim of this is usually to make the victim miserable and to exert a form of control on the victim.

With all these been identified, so many questions comes to one's mind. Such questions such as: What laws have been put in place to curb this trend? How are these laws implemented? What are the various jurisdictions of these law? Answering these questions would help in understanding how cybercrimes can be prevented with effective cyber laws globally.

CYBER LAWS

Cyber laws are also referred to as the Law of the Internet and it is described as the overall legal system which deals with the Internet, cyberspace as well as related legal issues. It also cover broad area including, freedom of expression, access to the Internet as well as its usage and online privacy. There are basic terms that needs to be understood. There are basically three basic terms that needs to be made clear which are:

- **Information Technology Law:** The laws that constitute this refers to digital information and it further describe how information is gathered, stored and transmitted.
- **Cyber/Internet Law:** The laws in this categories focuses on how the internet is used.
- **Computer Law:** This cover a large area as it includes the internet as well as computer IP laws

In as much as these terms have been understand, the questions that comes to one’s mind are numerous at this stage. They include: Why Cyber Laws? What are the International Cyber Laws currently in place? How can the implementation be more effective? The answer to these questions would further enhance the understand and create a framework that can help implement effective implementation of the cyber laws I

WHY CYBER LAWS?

It is interesting to know that the reason for creation of cyber laws cannot overemphasized as the rate at which internet spread was second to none, thereby slowly giving rise to cybercrimes to also grow. Just as there are international laws governing air space, there should be international laws governing the cyber space or cyber world. This is because there is a critical need to have a framework that controls the way the internet is accessed and used otherwise, users will definitely take advantage and misuse to their own selfish benefits and to other people’s detriment. Cyber laws are needed because of the following reasons:

1. A critical examination of the way the internet spread is phenomenal and is due to the fact that there is no centralised regulatory agency controlling it. The uncontrollable growth calls for strict regulation
2. Anyone can be hooked to the internet as long as they have a computer system and internet connection, this brings a very high level of flexibility for users which has also constituted the misuse or improper user conduct
3. Cyber laws are needed in order for system administrator to have the ease of checking and tracking down crimes such as frauds, vandalism as well as abuse which has made life miserable for a lot of online users

4. The misuse of the internet by online users may have direct destructive effect on physical businesses and also spread element of distrust which also has negative effect of the growth of online business such as e-commerce.

CURRENT INTERNATIONAL CYBER LAWS

Overview

The issue of international laws at present cannot be overemphasized. This is because there is no standard international law that is drafted to be universal recognised cyber law, but each country have their own list of cyber laws that are have been put together to curb cybercrimes in each distinct country. Though a critical examination shows that most cyber laws enacted by different countries are very similar because most of these countries deal with similar threats and attack, there is that loophole of allowing of not been able to curb or punish crime committed by someone from another country. In this case, except the person is extradited to the country where the effect of the crime is felt, the person may never be punished.

In order to combat the challenges posed by the rising cybercrimes including new ones, many countries such as e USA,Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland,Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore have been forced to review their domestic criminal laws so as to drastically curb computer related crimes. However, the reality is that no country has been able to resolve all issues such as legal, enforcement as well as crime prevention because the legislation by these countries cover only few classification of computer related crimes.

Standard International Cyber Laws (SICL)

This call for a centralised international law whereby by countries can be a member. Becoming a member means irrespective of where the effect of a cybercrime is felt, the perpetrators can be punished anywhere. With the rate at which cybercrime and attacks have increased and the fact that there are new type of cybercrimes, the dire need for the creation of Standard International Cyber Laws that will curb, stop and further punish cybercrimes and cybercriminals irrespective of location. The Standard International Cyber Laws (SICL) should be able to do two main things:

- Create as well as implement guiding rules and conduct which will further facilitate efficient communication and secured reliable transactions through the electronic medium
- Define, punish and also prevent possible actions that leads to attack on the electronic medium with the potential of harming others

To further enhance the creation of Standard International Cyber Laws (SICL) that will protect individuals, government agencies as well as hardware and infrastructure, 4 main areas are tagged to be covered in the Standard International Cyber Laws that would be eventually created. It includes:

1. **Internet Government:** this includes legal and technical aspect, content regulation and free expression as well as technical standard
2. **Cyber Crimes, Warfare and Terrorism:** this includes cybercrimes of different categories and laws applicable to cyber conflicts
3. **Data Protection and Privacy:** this includes treaties and international agreements on data privacy as well as its protection and access
4. **E-Commerce:** this includes treaty and model laws on E-Commerce as well as intellectual property

ENHANCING EFFECTIVE IMPLEMENTATION OF CYBER LAWS

It is no doubt that implementation of the existing laws as well as the news ones that would be created is crucial in the fight to prevent cybercrimes. This is because its effective implementation will reduce cybercrime rate, further reduce the likelihood of cyber dangers posed by cybercriminals as enhance free, crime-free deep web platform. All these are the benefits that government agencies and individuals want to enjoy while using the internet which brings the issue of how this level of cybercrime free platform can be achieved.

Critical examination, evaluation with assumptions suggest that this could be achieved by 4 main processes and methods:

1. By creating a suitable environment that further induces self-compliance by the immediate society as well as environment
2. By regularly monitoring different scenarios that comes with very reliable feedbacks
3. By acknowledging the fact that incorporation of modifications can be made at any time offering openness as well as flexibility.
4. By establishing guidelines for the implementing agency that is authority-responsible

These four processes ensures one thing: A simple and fair law that is clearly defined. In the case where the law is misused to harass individuals, corporate agencies or government entities resulting in the defiance, then the agency responsible for implementation is compelled to take actions that are deemed corrective.

ARE NEW CYBER LAWS NEEDED

There is no doubt that the new trends of cybercrimes in recent years has reached a stage where the existing laws can no longer cover all cyber related crimes and as such, new laws that would help tackle new emerging cybercrimes needs to be created and enacted. This is done or can be done in two folds:

- By modifying some laws to cover other areas that may have been left out or not taking so serious

- By totally creating new laws that cover new areas especially with emerging trends of cybercrimes

By modification, some laws will be covered and by totally creating new ones, emerging crimes would be tackled and the perpetrators can be tried irrespective of location as well as the jurisdiction

CONCLUSION

Cybercrimes are on the rise with new deadly crimes emerging from places people never thought could be home to cyber criminals. The need for more efficient implementation has become priority couple with the need to establish Standard International Cyber Laws (SICL) that would serve as the global governing body for cybercrimes as well as related issues.

Preventing cybercrimes through effective cyber law concepts and policies from global perspectives can only be achieved through this furthermore an integration of many local laws enacted from different countries using it to tackle cybercrimes.

Cybercrimes should be taken seriously and treated with high sensitivity. Drastic actions should be taken against perpetrators in order to be able to set the desired standard that is needed to create a conducive environment especially for corporate organisations and government agencies that mostly depends on online presence to carry out their designated tasks as well as processes

REFERENCES

Briana. G (2017) 6 Must-Know Cybersecurity Statistics for 2017 | Barkly Blog. Available at: https://blog.barkly.com/cyber-security-statistics-2017. Accessed on the 2nd of March, 2018

John. G (2018) 2017 Security Breaches: Frequency and Severity on the Rise. Available at: https://revisionlegal.com/data-breach/2017-security-breaches/. Accessed on the 2nd of March, 2018

John. M (2018) Cyber Security Statistics. Available at: https://thebestvpn.com/cyber-security-statistics-2018/. Accessed on the 5th of March, 2018

Kobra. M, Saeideh. Y (2014) A global perspective on cybercrime. Available at: http://article.sciencepublishinggroup.com/pdf/10.11648.j.hss.20140202.14.pdf. Accessed on the 17th of March, 2018

Manish. L (2012) Cyber Laws: A Global Perspective. Available at: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005846.pdf. Accessed on the 17th of March, 2018

Marco. G (2012) Understanding Cybercrime: Phenomena, Challenges and Legal Response. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Accessed on the 14th of March, 2018

Margaret. R (2010) Cybercrime. Available at: http://searchsecurity.techtarget.com/definition/cybercrime. Accessed on the 1st of March, 2018

Mary. O (2012) Cyber Security andInternational Law. Available at: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf. Accessed on the 16th of March, 2018

Samanjeet. K, Sukhwinder. S, Amanjot. S (2015) Cyber Security: Attacks, Implications and Legitimationsacross the Globe. Available at: http://research.ijcaonline.org/volume114/number6/pxc3901932.pdf. Accessed on the 15th of March, 2018

Sanjana. R (2016) 4 types of cybercrime that everyone should know about available at: https://yourstory.com/2016/12/4-types-of-cybercrime/. Accessed on the 12th of March, 2018

Scott. S (2016) 6 most common types of cybercrimes business leaders should understand. Available at: https://mobilebusinessinsights.com/2016/11/6-most-common-types-of-cybercrimes-business-leaders-should-understand/. Accessed on the 12th of March, 2016

Silverbug (2017) 10 Types of Cyber Crimes... And Another 10 You've Never Heard Of. Available at: https://www.silverbug.it/blog/10-types-of-cyber-crimes...-and-another-10-youve-never-heard-of. Accessed on the 10th of March, 2018

Stephen. N (2012) The 10 Most Common Internet Crimes. Available at: http://www.complex.com/pop-culture/2012/11/the-10-most-common-internet-crimes/. Accessed on the 13th of March, 2018

Steve. M (2017) 2017 Cybercrime Report: Cybersecurity VenturesCybercrime damages will cost the world$6 trillion annually by 2021. Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf. Accessed on the 18th of March, 2018

Steve. M (2018) Top 5 cybersecurity facts, figures and statistics for 2018. Available at: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html. Accessed on the 2nd of March, 2018

UpCounsel (2018) Cyber Law: Everything You Need to know. Available at: https://www.upcounsel.com/cyber-law. Accessed on the 5th of March, 2018