Conflicts in International Cyber Crime and Methodologies of Cyberwar

Sameer Dasaka[1], Sarvani Gadiraju[2], Sandeep Dasaka[3]

ABSTRACT

Every day, a vast majority of computers and networks are getting hacked and it is important to maintain and manage incident response thoroughly. Cybercrimes are perilous issues which span over national and state borders easily where they are recognized as international issues. These issues are needed to be addressed quickly and meticulously.

Cybercrime and Incident Response Management can be handled by having an ideology of different types of cyber threats and cyber-crimes. The Digital Forensic Investigator needs to think outside the box and should have knowledge on various factors which trigger cyber-crime. At times, the psychology of the person also plays a very important role in identifying the root-cause of the cyber-attack.

This paper will present an outline into how conflicts in international cybercrime should be handled by identifying potential actors, and by developing excellentcyber security policies relating to cyberwarfare and cybercrime.

Key Terms: Cyber Crime, Cyberwar, Cyber Intelligence, Criminal Psychology, Cyber Security, Digital Forensics, International Cyber Laws, Internet Governance, Internet Infrastructure, Information Security, Incident Response Management, Threat.

Manuscript received July,2018

SAMEER DASAKA[1]: Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, Gujarat, India

SARVANI GADIRAJU[2]: Faculty of Computing and Mathematical Sciences, University of Waikato, Gate 1 Knighton Road, Private Bag 3105, Hamilton 3240, New Zealand.

SANDEEP DASAKA[3]: Department of Information Technology, Charles Sturt University, Quad 3, 1/01/102 Bennelong Pkwy, Sydney NSW 2127, Australia

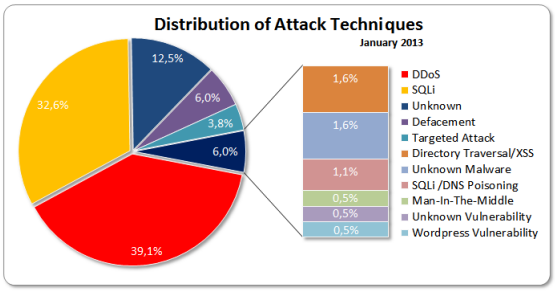
I. INTRODUCTION

Statistically, 3 out of 5 computers today are getting hacked in the world. Potential errors and bugs in software applications which lack proper security architecture and mechanisms are exploitable to various cyber-attacks like SQL Injection Attacks, XSS Attacks, CSRF Attacks, Input Validation Attacks and more. The lack of security also creates Zero-day vulnerabilities and are causing more damage and havoc to Individuals, Enterprises, Organizations, and also Governments. There are various number of threat actors who should be identified so that to understand and deal different types and effects of Cyber Crime. As discussed, it is quite important for a digital forensic investigator to perform psychological analysis on the attacker to understand the root-cause of an attack. Today internet plays a very important role for global messaging, social interactions and also business transactions as internet being completely integrated into the society and mankind. We know internet as a whole and there are few forces in the world who are fighting and attempting to split the internet and fragment it into pieces. When we talk about managing incident response and international cyber conflicts, there are usually two major issues we will have to face. The first, internet delivers anonymity to almost everyone who are using it. Which means, one can stay completely anonymous and maintain anonymity by spoofing their personal and business identities. With many businesses providing free and paid VPN services to users, it really gets difficult to track a user and validate his/her identity over the internet. Few of the famous VPN service providers are 'Proton VPN', 'Touch VPN', 'EasySurf VPN', 'ExpressVPN', 'HideMyAss VPN' and more. By using these services anyone can hide themselves and commit crime. The Second, Crime which takes place in two different locations or more which cross-national boundaries are difficult to bring to justice. Example, Alice while residing in United States hacks a computer in China, then it is gets difficult to know which law to be applied to bring the criminal to justice. Either cyber-laws in USA or cyber-laws in China. Cybercrime which crosses national boundaries are another major issue in the International Cyber Crime. Cyber Intelligence Agencies and Governments are trying to eradicate this issue by bringing common cyber laws

so that it may make jurisdiction more simple and efficient.

II. Advanced Persistent Threat (APT)& The Psychology of Criminal.

With the free flow of internet today, it makes an impact to political stability and political decisions. Many countries today have started viewing the internet as a threat to the society and have been promulgating censorship practices of the internet. Majority of the countries have concerns as the internet is advancing every day. There are international conflicts where issues like separation of the internet, espionage and the internet governance are to be addressed. Today, almost everything runs on the internet. Right from e-commerce, trading, stock exchange, global messaging, social communications, and more. Companies across the globe are investing billions of dollars in the internet as the mankind is very much dependent on it. Government agencies are using internet to develop more strategic pathways to fight different types of crime. After understanding the basic overview of how the society wants to censorship the internet, take control over, fight media piracy, and governments from different countries trying to bring laws which can help in solving cybercrimes which cross national and state borders, now let us see what the efforts should be necessary to keep information safe over the internet and on how to help nations maintain cooperation among each other to fight cybercrimes by updating internet strategic policies, improving incident response management, updating information security practices and more. When we try to understand the psychological factors which trigger cybercrimes, we should always keep in mind that psychology depends on two major factors. First, the psychology of the individual and second, the psychology of the government, institute, agency etc. At times a certain individual wants to hack into other individual or any institute system for his/her own personal or professional gain. The individual may also be heavily funded by any venture capitalists who would like to gain unauthorised access into their competitor's data and security infrastructure. This is where Advanced Persistent Threat also known as APT comes into the picture. This is where threat modelling is done, OS Fingerprinting is done and vulnerabilities are exploited. This is called as Advanced Persistent Threat because the process may take lot of time but sooner or later the attack will be successful. When we try to resolve these issues relating to cybercrime, it is important to look at the impediments which are on the way. For an example, if we want to look for Critical Security Infrastructure Weakness or Threats, it is necessary to know who our enemies are, what would be the business impact if they are successful in carrying out an attack, what would be the consequences, what would be their next major move and more. Today, companies and governments are trying to build more confidence among themselves before taking a step forward to build treaties. It is always important to know ourselves first, be confident about who we are and then take a step forward to change the world. People are trying to build cooperation among themselves first. At times, a cyber-warrior in one country who is assigned to hack into the systems of another country is recognized as a patriotic, but for the other country, he is a cyber terrorist. Attacks are distributed into many categories in the industry today ranging from SQL injection attack, exploiting WordPress vulnerabilities to Man-in-the-middle attack.



III. Transmogrification and Different Types of Cyber Crime.

Since ages, mankind had been experiencing different types of crimes on different levels every time and almost everywhere. From burglary to financial fraud, from murder to kidnapping, from capital crimes to organized crime, from espionage to cybercrime. In all these crimes, cybercrime and digital crime stands most important. Today, the internet is widely used and criminals use this as a sophisticated platform to carry on their attacks. It is possible for a person to start a riot in a city or a country simply by using the internet. Internet is a very powerful channel which can be both advantageous and deadly dangerous as well. Internet Crime or Cybercrime can be defined as a crime which has taken place with the help of computer systems, digital media and networks. Computers being easy to use, it can also be used for many different purposes. Computers can be used to target someone. It may be either an individual, business, or a government too. By using a standalone system as a target, hackers can use computers for Destruction of data, exploiting vulnerabilities in web applications, data forgery, identity theft and more. Then computers can be used as a weapon in the society where crimes like child pornography, cyber bullying, e-bomb, phishing attacks, e-spamming and more can be witnessed. In another scenario, computers can be used as an attack recruiter where hackers or other individuals use computer as a channel to recruit people who can finish the task for

them. This way, computers are used for many destructive purposes. Pathways to DeepWeb and Darknet give multiple access to drugs, illegal arms, prostitution, gambling, murder contracts, illegal organ transplantations and much more. Nowadays, police have set up their own websites in the deepweb and darknet sites to catch hold of criminals who perform illegal transactions over the hidden internet. In starting days, cybercrime was just a hobby for people to demonstrate their hacking abilities to the society, slowly, self-claimed hackers started joining into cyber groups and started performing to outrun each other. Then the competition begun. While challenging fellow hackers, hackers started attacking people in bulk to showcase their hacking abilities where majority of them were innocent victims. Though, another set of hackers called the White hat hackers came into existence, where they target companies which lack proper authentication mechanisms and security infrastructure. Hackers have been targeting companies who hold extremely sensitive data. Example, banks like Royal Bank of Scotland, UGS, Axis, ICICI and many more. These banks carry extremely sensitive data like credit card information, Net-Banking login credentials, OTP delivery systems, Debit card information and much more. Hackers have been targeting major companies and banks because, the dark web has major demand for stolen credit card information. Hackers breach data, steal account information's and sell them back again in the Deep and Dark Web platforms to make millions of dollars.

Innocent people are being targeted and are attacked by faking a persona and are lured with offers where they give away their OTP (One-Time Passwords) and other sensitive information to the attackers. This is one type of cybercrime where hackers use social engineering attacks and phishing attackers to lure the victim and then trap them. Another type of cybercrime is where cyber warriors or cyber criminals target employees of a company, hack into their personal and private data and then ask ransom to not publish their private information over the internet.

IV. Psychological Explanations of Cyber Crime.

Most of the hackers do not succeed in their initial attempts. Because technology being advancing every day, it is really tough to find new loopholes. Whenever there is a data breach, forensic investigators try to find and analyse the root-cause of the attack. Once successfully found, the loophole or the vulnerability which was exploited before is patched. Therefore, Secure Code Reviews came into existence to find the vulnerabilities in code which can be targeted and exploited. In situations like these, hackers or cyber criminals need more and more motivation and willpower to keep going. This motivation can come from one's self or from an individual. The impact of the motivation on the criminal will help him/her succeed. The major parameter for the criminal to be motivated always is, Who the target is, what impact does it create when the attack is initiated, what is the direction in which he/she is going, how much is the intensity of the attack. Sometimes, the criminal is self-motivated or has external motivational influence on him/her and at times, innocent victims are turned into cyber criminals where they are threatened and also motivated at the same time to pursue the attack. The major motive for hackers to hack into computers and networks is financial gain or profits. Then rest comes revenge, cyber bullying and more.

V. The Internet Infrastructure

For us to understand cybercrime and conflicts in cybercrime, it is first necessary to have an understanding about the infrastructure of the internet and the infrastructure of the Networks. The internet infrastructure is the basic yet eminent point of source where constant communications and end-to-end connections also known as nodes are made. In the cyber world, the internet architecture is where lot of issues are based on. The more we will be able to understand its architecture, the better. As we know, internet is the network of networks where almost each and every device today are inter-connected to each other to communicate. The internet acts as a backbone for all these inter-connected devices to have global communications where data is being constantly received and sent. To understand the infrastructure of the internet better, it is important to understand the concepts of 'packet-switching' and 'circuit-switching'. In the concept of circuit-switching, two devices are dedicatedly connected to each other via a medium to establish a connection to communicate to each other. Today, the internet exactly works on the process of

circuit-switching. Coming to the concept of packet-switching, whenever a sender sends a message over the internet, the message is broken down or separated into small packets and then transmits to the receiver. This way, the packets take the most desirable path to travel across and will use the mechanism of sequencing and reassembling to join the data together. Here, according to the OSI layers, the transport layer, which is the Heart of the OSI will take the initiative to transmit the data over. Here the transport layer is held responsible for end-to-end connectivity. The list of tasks which are performed by the Transport layer of the OSI are:

- Identifying Service
- Multiplexing and De-Multiplexing
- Segmentation
- Sequencing and Re-assembling
- Error Correction
- Flow Control.

If a message 'HELLO' is sent from Alice to Bob, then the message is fragmented into separate packets like 'H', 'E', 'L', 'L', 'O' and then sent. Once Bob receives the message to his system, then the transport layer sequences and re-assembles it the way it was sent.

When the packets are sent, they do not choose a single particular route to travel. Instead, they choose multiple pathways to transmit but reach at the same destination. The packets usually use the TCP which is known as 'Transmission Control Protocol' and UDP which is known as 'User Datagram Protocol' to transmit over the internet. So, these protocols are certain rules which are established for computers to understand how to transmit the data over the internet. Now, each computer with an internet connection is assigned an address called as 'IP Address' which is 'Internet Protocol Address' is a unique number which is used to identify that particular machine. When two different systems try to communicate with each other, the IP addresses of the systems have to ready. Where, the sender needs to know the receiver's IP to transmit the data and the receiver needs to know the IP address of the sender to receive/accept the data. This way, the transmission of data is done over the internet.

Since multiple computers and websites have different unique IP addresses, it has been quite difficult to remember those IP addresses. Therefore, DNS which is known as 'Domain Name System' came into existence. Then, a website can be reached either by its IP address or its domain name.

Amazon has its IP address as 172.168.1.23 and its domain name as www.amazon.com. Here a user can either reach amazon via its IP address or its domain directly.

VI. Advancement of Cyber Warfare

Worldwide, Nations are building their own cyberwarriors. Implementing sophisticated cyber strategies and programming powerful computer viruses which could bring any nation down in an instance with the help of internet. So far, we have seen how individuals hack into computer systems and networks of innocent people, institutes, governments but when a nation attacks another nation's cyber infrastructure, then it is known as Cyber Warfare.

This is to gain political and economical advantage over the other nation. Different types of wars had been fought including air, sea, land, and also bio war. Now, it is time to Cyber war.

Cyber war is a process of implementing a systematic and sequential attacks on a nation's computer or cyber infrastructure where, it is possible to take down the nation's financial markets, crash shares of companies, manipulate share values and more. Then, cyber warfare can be used to create havoc to the public by hacking into public railway systems, turn down electricity, disable public support systems and more. Then comes disabling satellite and telecommunications of the country. Restoring all these takes lot of time and sometimes cannot be restored again. It is only recognized when the damage has been occurred and is very difficult to detect this in an earlier stage. Terrorists today are attacking a nation from the cyber front. These incidents are increasing all the time. Usually, Government websites are targeted and hacked to gain political advantage and superiority. Destruction of a nation's telecommunications and information systems are the major goals for implementing cyber warfare. This is because, communication is the most basic source to discuss, understand and mitigate issues. Without communication, it will be almost impossible to restore the peace back. Cyber warfare can also be called as Cyber Terrorism or hacktivism. The motive plays an important role in cyberwar. Is it to gain political or economic advantage. Is it to disrupt peace and create inconvenience to the public by hacking into and shutting down public support and resources like water, electricity, financial transactions and more. The other motive is to gain financial benefit from the country. The tools andtechnologies which are used to create havoc

are also the tools used to hack an individual or a government.

Cyberwar can also be due to resources. Today, there is a severe shortage of resources everywhere around the world. What one country needs is being sold in extreme expenses by another country, in such cases, different countries plan and attempt different cyber strategies which would cause severe havoc to the nation and in return to restore stability, resources are given without any expense. Whenever cyber war takes place, managing incident response gets real tough as cyber war just not focus one certain field or domain to hack into. Cyber war targets multiple fields like financial markets, healthcare, railways, airport systems and many more. Detection of the attack, collection of data, analysis of the collected data, chronology determination, incident response, havoc assessment, detection of vulnerabilities which were exploited and remediation of vulnerabilities are the sequential steps to be follow when cyber war has taken place on a nation.

VII. Cyber Warfare Threat Actors and Intelligence

In the field of Cyber Security, it is always important to know who our enemy is, what would be the impact if a cyberattack is carried on us, and how will the enemy probably plan or threat model the attack on us. Having knowledge on these parameters will help an individual or an organization to safeguard themselves from any cyber-attacks. Few threat actors who can be recognised are:

- The Government Funded: Certain hacking groups are very well-funded or sponsored by their government to design sophisticated cyber strategies and implement them. These groups are not detected at an early stage as they are constantly under radar and design threat modelling in a very clever way. These groups are used to collect information about a specified target for mostly political advantage.

- An Insider Threat: Typically, employees in an organisation who sell internal secret access codes, who share internal confidential information to the outside people, who give unauthorised access into their networks for the benefit of others. These types of attacks are said to be known as insider attacks. Employees who are involved in insider attacks are rewarded heavily for they're illegal assistance to successfully carryout the crime.

Sometimes, when a new software update is released, or when a functionality is upgraded, then there are chances that there might be a leak in the security architecture which can be used to exploit the web application and gain unauthorised access into the organisation. Therefore, there is always a constant pressure for organisations to deploy secure code reviewers to thoroughly check the source code of the websites or web applications to review the code. Once we are able to identify our enemies, the next stage is to maintain Secure Threat Intelligence Systems where the governments or institutes are alerted whenever their networks are scanned to perform a cyber-attack. Once threat intelligence reports are consumed by the governments, this external information is used to create and implement internal defensive cyber policies and strategies. Threat Intelligence or SIEM is also used to let an organization know if anyone is planning to engage a cyber war on them by analysing and cross-referencing their network security systems and network logs. This will be very helpful to strategize an operational & defensive approach to counter-attack the enemy.

VIII. International Humanitarian Law and its relation with Cyber Warfare.

Before we get to know what, International Humanitarian Law is, and how it is cyber warfare is related to it, it is important to understand the principles of just war. These laws of war are important to understand as cyber warfare relates deeply with the laws of just war. With this understanding, it is possible to resolve the crimes and conflicts which are happening over the internet or in the cyber zone.

'**jus ad bellum**' and **'jus in bello'** are two distinct and significant domains which are necessary to understand the actions of proceeding to a war. Since a war can also be fought over the internet, these domains relate a lot to cyber warfare. 'jus ad bellum' is where laws of armed conflict apply while going to a war and the principles which administrate or direct the right to go to war are known as jus ad bellum and the principles which administrate the action of war in known as jus in bello.

Certain laws are regulated regarding the conduct while in war. These laws are known as '**International Humanitarian Law**'.There are many countries in the world who have signed this treaty where the laws of armed conflict are regulated.

Now, talking about cyber warfare we need to know who the legitimate ruling classes of cyber warfare are. Generally, many proxies of different countries conduct cyber warfare as a covert act or maneuver. The question here arises that are the proxies of all these different nations truly recognizable or not. According to the laws of just war, one should know that a war should only be held or conducted with proper and rightful intentions

only which are generally motivated or inspired by or for a cause. This cause should be a public cause where majority of the people residing in a country benefit from the war keeping in mind that the war should be waged with rightful intentions. When a war is conducted, it should fulfil the term '**Just Cause**'. Just Cause Law means that there has to be legally supported and sufficient reason to conduct a war while keeping in mind that it should be conducted only for a good cause.

As we know that there is a significant improvement in the advancement of technologies every day, it is difficult to measure or assess the amount of success one can gain through implementing a cyber-attack. When a cyber-attack is taking place, it is very uncertain and unclear if the defensive strategy which is going to be implemented would work or not. When a war is conducted, the benefits of the war should be proportional to the cost of expenses encountered. This can be measured with the impact or extent of damage and in the field of cyber warfare, it takes lot of time to assess the impact of damage. When a cyberattack happens, till date, there were no direct causalities.

A war should only be conducted, when all the diplomatic meetings fail. Therefore, it is really difficult to apply international humanitarian laws on cyber warfare.

IX. Trust among Nations and issues with Information Security over Cyber Space.

It is very important to maintain trust and confidence among nations while making sure the sentiments, opinions, conceptions, speculations, considerations and contemplation of another nation are not directly or indirectly affected. The major problem among nations is not being able to trust each other. It is important to address this issue to settle issues related to cyber security and information security among nations while using cyber space. It is necessary to let other nations know if any exercise related to cyberattacks are being implemented to minimize the anxiety which exists. The key to minimize or stop the conflicts among nations in the cyber space is to maintain good trust with each other. When a country is vulnerable to cyber-attacks, it is obvious that the country would feel very vulnerable as their people and countries resources are at a stake. It is important for other countries to help them grow powerful without exploiting their vulnerabilities in their cyber space. This will increase the confidence in a country on other countries.

X. Conclusion

We have presented a formal strategy on how conflicts between two or more nations in the field of cyber security can be handled and mitigated. We have concluded that if two or more nations work harder to establish a healthy communication and relationships between each other, this will help to build more confidence among themselves. Trust can only be build if countries start exploring their significant vulnerabilities in their cyber space and help other nations overcome their fear and anxiety by strengthening them. Our work introduces an end-to-end methodology where countries can be safe while exploring and experimenting their advancements over the internet and the cyber space without triggering fear and anxiety in other countries. The proposed framework is efficient and beneficial if the intelligence agencies or the governments of different nations together work to enhance their technologies in the cyber space.

XI. References

[1] Lawrence A. Gordon Martin P. Loeb WilliamLucyshyn Lei Zhou, Journal of cyber security, volume 1, Issue 1, 1 September 2015, page3-17, https://doi.org/10.1093/cybsec/tyv011 Published:27, November 2015.

[2] Langner R. Stuxnet: dissecting a cyberwarfareweapon.Secur Priv IEEE 2011 ; 9: 49–51 .

[3] Symantec Corporation. Internet security threatreport.2015. (9 November 2015, last accessed date).

[4] Cyber Crime – A Growing Challenge for Governments, July 2011.

[5] https://legal-dictionary.thefreedictionary.com/Just+Cause

[6] https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html

[7] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010.
Available: http://www.microsoft.com/security/sir/

[8] http://www.experian.com/decision-analytics/fraud-and-identity.html

[9] Open Web Application Security Project. The ten most critical Web application security vulnerabilitieshttp://umn.dl.sourceforge.net

[10] https://www.civilserviceindia.com/subject/General-Studies/notes/basics-of-cyber-security.html

[11] https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[12] http://www.vssut.ac.in/lecture_notes/lecture1423183198.pdf