The Exigency in Accretion of Cyber Warfare Legislation

Raman Solanki*
Ankit Verma**

Abstract

Recent advances of internet over the two decades of more than two billion users. The expansion resulted in developing applications for the cyber world, which bolster further expansion and more applications. To compute to the rise of a cyber-economy, commercial transactions and accentuating in the storing and sharing of hypersensitive information. Storing of sensitive information on networks eventuated to cyber espionage against the government and cyber economic warfare against the businesses and the need of the legislation dealing with newly developed cyber laws came into existence.

Keywords: Cyber Attacks, Web Vandalism, Legislation, laws, Disavowal of service

Introduction

Cyber warfare is delineated as a major interruption to critical infrastructure, despite it is the least liable-result. Assaulting an outland via the internet has an intense chain-reaction also a collateral global damage. Cyber warfare occurs continuously across cyberspace connections giving rise to minor disruptions, website vandalism, heist of national defense information, and rational property defraudment. We are on the point of a considerable bend in the attribute of warfare as military-competition bolsters into the cyber field. Characteristically, it reconnoiters concerns among senior-policy builder and leaders of the military in extensive cyber powers that their non-state and state adversaries to execute-prompt cyber defilement that could administer adversity on their rivals to give rise to catastrophic level of destruction on the cyberspace. The credible targets of cyber-attacks are the power grid, financial sector, energy reservoir (gas and oil pipelines) and communications [1]. The increasing dependence on information structure in generic and connections to the Internet in minute, hypercritical infrastructure is augmenting more liable to cyber-attacks. Leaders around the globe have embodied concerns of the exigency of cyber "Unforeseen Attacks" are developing. Cyber Weapons' possibility to oversee damage to that of Nuclear weapons is valid. The Legislations ought to safeguard its populace from these virtual weapons of mass-destruction of the economy and the information by enforcing and updating laws [2].

Raman Solanki*
Student (BCA)
IITM, Janakpuri, New Delhi-110058

Ankit Verma**
Assistant Professor
IITM, Janakpuri, New Delhi-110058

Types of Cyber Attacks

The use of Information-Technology and computers to complete acts of war on the government and large scale framework is the true delineation of cyber-attacks. The assailant of cyber-attacks can be a definite person, a formulation, or another government. There are many different forms of cyber-warfare from specialized-hacking jobs on an unambiguous server to the conventionally targeted denial of service attacks. The definitive in cyber-attack is a blitzkrieg that completely abstracts the dexterity for all of the members of the government and the organization to connect to the internet. The adversaries are so clever even when one method gets done then they are ready with their other method to add to the destruction. The most commonly used methods for Cyber Attacks are Web Vandalism and Disavowal of Service Attacks.

Web-Vandalism

Web-Vandalism is characterized by website disfigurement and denial of Service invasion. Website defacement is the most quotidian contour of web

Table 1: Webserver

	2005	2006	2007
Apache	308	486	319
IIS/6.0	72	181	114
IIS/5.0	100	66	24

Table 2: Operating System

	Linux	Windows
2009	276	180
2010	446	258
2011	306	140

vandalism; Website-defacement is an imperative threat to many internet-facilitated businesses. It hostilely affects the public image of the Organizations. Organizations may suffer from loss of important data, trust of people and business. The following are the steps on how website defacement works [4].

- The number one step would be to search for a username for instance strutting as administrator and calling an employee; the administrator information can also be fetched from a Whois database.
- Using various executions such as brute-force, the password can be salvaged.
- As one has the access to the administration access, the next step will be to annex administrative privileges.
- Ensconcing a backdoor; the defacing of the website may begin.

How to defend against website defacement?

- Avoid using the server as a client (e.g., web browser)
- Remove buffer overflow vulnerabilities in your programs.
- Use a different user(s) other than root for managing the website contents.
- Enable access logs.
- Update.

Web vandalism is not only present in the United States. It is also a problem in many other countries particularly Kyrgyz. The published statistics of registered website defacements every year is given in the table. The following tables are subset of those statistics:

How to recover from website Vandalism and avoid future defacements?

- Change all user passwords, if the web server provides user-authentication, and you have evidence/reasons to think the passwords may have been compromised. This can require a large user communication.
- If backup server has been used, restore the primary web server component as nominal

Disavowal of Service

The disavowal of service malicious deed is an attempt to exhaust all of an available contrivance in order to keep those resources from its contemplated end-users. The disavowal of service is one of the most banal blitz upon the internet done by the attackers. Its use is so outspread because it is comparably accessible to implement and it is very arduous to defend-against. Conventionally an assailant-builds an alluvion of ersatz requests to a service, scorning the results. The server is bogged-down by huge number of approaching requests, taking long times to haft both the fraudulent requests and any licit requests that come in during the attack. In supreme cases, the server will not be able to haft the strain of the approaching-connections and will

crash, enduringly breaking the server until it is manually renewed. A disavowal of service attack may subsist of an entreaty which is crafted to coup a specific vulnerability in the server, inciting it to crash without coercing a large number of requests. The assailant-sends request from more than one system making it a distributed disavowal of service attack (DDoS). A disavowal-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. A DoS attack can be perpetrated in a number of ways. Attacks can fundamentally be classified into five families:

- Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to:

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
- Crash the operating system itself.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address. Two types of DDoS attack networks have emerged: the Agent-Handler model and the Internet Relay Chat (IRC)-based model. The Agent-Handler model of a DDoS attack consists of clients, handlers, and agents (see Figure 1). The client is where the attacker communicates with the rest of the DDoS attack system. The handlers are software packages located throughout the Internet that the attacker's client uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack. The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. The owners and users of the agent systems typically have no knowledge that their system has been compromised and will be taking part in a DDoS attack. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. Usually, attackers will try to place the handler software on a compromised router or network server that handles large volumes of traffic. This makes it harder to identify messages between the client and handler and between the handler and agents. In descriptions of DDoS tools, the terms "handler" and "agents" are sometimes replaced with "master" and "daemons", respectively.

The IRC-based DDoS attack architecture is similar to the Agent-Handler model except that instead of using a handler program installed on a network server, an IRC (Internet Relay Chat) communication channel is used to connect the client to the agents. An IRC channel provides an attacker with additional benefits such as the use of "legitimate" IRC ports for sending commands to the agents [4]. This makes tracking the DDoS command packets more difficult. Additionally, IRC servers tend to have large volumes of traffic making it easier for the attacker to hide his presence. Another advantage is that the attacker does not need to maintain a list of the agents, since he can log on to the IRC server and see a list of all available agents [4]. The agent software installed in the IRC network usually communicates to the IRC channel and notifies the attacker when the agent is up and running. In an IRC-based DDoS attack architecture, the agents are

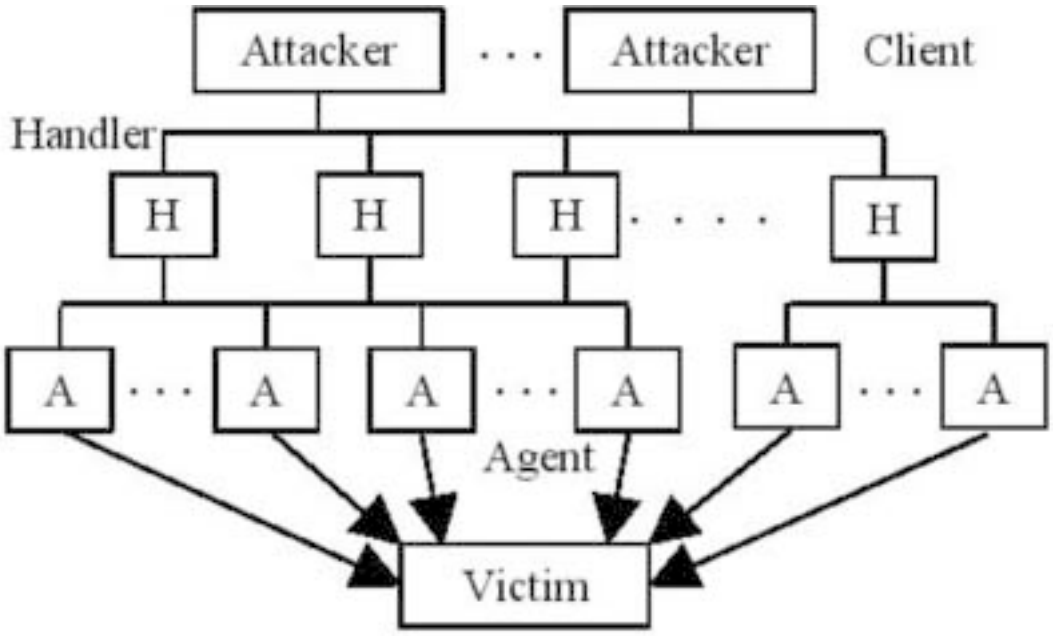

Figure 1: DDoS Agent-Handler Attack Model

often referred to as "Zombie Bots" or "Bots". In both IRC-based and Agent-Handler DDoS attack models, we refer to the agents as "secondary victims" or "zombies", and the target of the DDoS attack as the "primary victim". Well-designed agent software uses only a small proportion of resources (memory and bandwidth) so that the users of secondary-victim systems experience minimal performance impact when their system participates in a DDoS attack.

The following pie-graph represents the top source countries for Distributed Denial of Service Attacks [6].

Cyber Warfare Legislature

Various countries use various legislatures for protecting or advancing Cyber Warfare. It varies from enrooting, maturating a stratagem, to be oblivious to certain attacks. Disparate nations affiliate different approaches

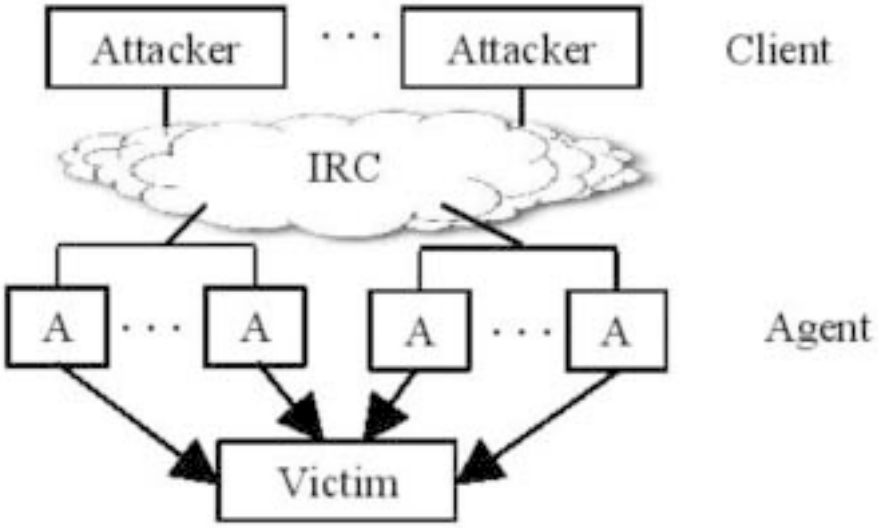

Figure 2: DDoS IRC-Based Attack Model

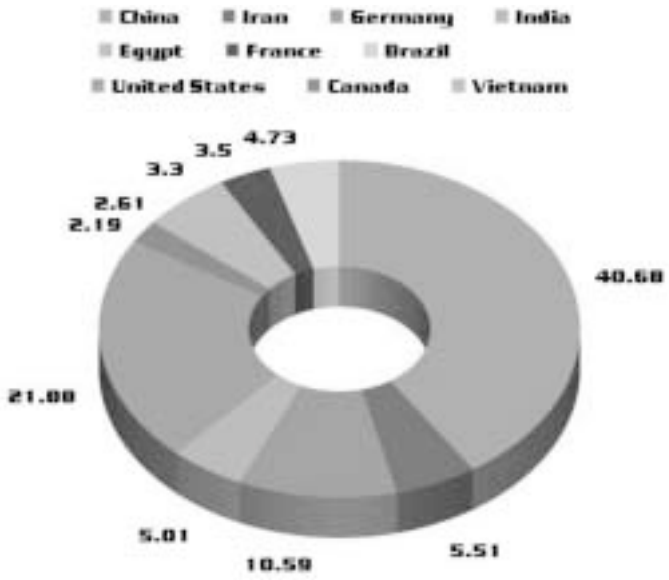

Figure 3: Top Sources for Distributed Denial of Service Attacks

to the cyber espionage and sabotage conducted by the assailants' government-forces; Myriad nations don't have a legislature to hedge their populace from these cyber-war and attacks by their assailants' government forces. Different zones in the world have different laws to treat and react against/for Cyber-attacks and the laws are necessary to safeguard people from various techniques of cyber-attacks.

EMEA

The Middle East, Africa and Europe, the cyber-warfare attacks have been comparably less than the other two time zones. Various Countries in this time zone don't even have a legislature to guide or bulwark from cyber warfare or attacks, The United Kingdom of Great Britain and Northern Ireland, to foster their networks also ordained cyber war games dubbed 'Waking Shark 2' to hedge their financial-organizations followed by the Wall-street. Britain has also endowed up a cyber-security and "operations-center" based in Government Communication Headquarters (GCHQ). The Police and Justice Act 2006, of the United Kingdom, amended the Computer Misuse Act 1990 and specifically outlawed disavowal-of-service attacks and set a maximum penalty of 10 years in prison Germany; the German Law gives the right to the German agencies to cyber scrutiny capability to twenty percent of total internet traffic [8]. Netherlands has various centers to support scrutinizing eye on the other networks ranging from National Cyber Security enter (NCSC), Joint IT branch (JIVC), Joint Signet Cyber Unit (JSCU) and Defensive Cyber Command (DCC), these clutch of various agencies have been set up by many other countries of this time zone.[9] The Europe has also entrenched ENISA (European Union Agency for Network and Information Security) The governmental agencies in this time zone have opened up to protect themselves from these unforeseen- cyber-attacks than just military [8-9].

APAC

The Asia-Pacific region has been the origin or the most cyber-attack-bearer than any other time zone because of its size and new developing economy and rivalries; this has been the major hotspot for Cyber Attacks also the inducement of these acts of war. China has been the most controversial country when referring to the origin of Cyber Attacks, China is gripped culpable for a twine of Cyber-attacks on numerous private and public institutions in countries ranging from France, Russia, Canada, India and the United States of America; the Chinese government disclaim any involvement in these campaigns and they believe that they are not the hazard but rather the victim of an rapid increasing number of Cyber-Attacks. The Chinese government uses-New space based intelligence

gathering systems and surveillance systems, infrared decoys, false target generators and anti-satellite systems. They have been information zing their military through increase educations of military person in Cyber Warfare, developing the information network for military training and have digital campuses and libraries for advancement [10]. Under Section 27A and section 161, the Chinese government is protecting and also includes imprisonment against unauthorized access to computer by telecommunication extended by Article 285,286,287. The Korean Peninsula has also been the victim and the impel of Cyber Attacks, North Korea is aggrandizing its workers through military academics specializing in hacking and other forms of Cyber-Warfare. During the military dictatorships of Park Chung-hee and Chun Doo-hwan (1961-1987), anti-government speech was frequently suppressed with reference to the National Security Act (NSA, 1948) and the Basic Press Law (1980). Although the Basic Press Law was abolished in 1987, the NSA remains in effect. The government has used other "dictatorship-era" laws in order to prosecute critics in contemporary contexts; [11] India is also-the sufferer and antecedent of various sponsored Cyber Attacks and has been late like many other developing nations around the globe in perceiving the Cyber Attacks, The government of India has taken various steps in developing a safe and resilient cyberspace for its citizens, businesses and government and have a National Cyber Security Policy 2013 also addressed by the Information Technology Act, 2000 to safeguard itself. Many nations in this time zone are not alert and have no legislature to safeguard its populace and economy [12].

The Americas

The New world in the western hemisphere of North and South America has dealt with various and the oldest forms of Cyber Attacks. The United States of America has the uttermost organized military for such cyber-attacks. Cyber warfare is a constituent of the American military-strategy of spirited Cyber defense and the use of Cyber-Warfare as a platform to attack. The United States Department of Defense has formally recognized cyberspace as a new sphere in warfare and has set up a new Cyber Command (USCYBERCOM) to shield America Military Networks and attack other countries systems. In the US, denial-of-service attacks may be considered a federal crime under the Computer Fraud and Abuse Act with penalties that include years of imprisonment and fine. The Computer Crime and Intellectual Property Section of the US Department of Justice handles cases of (D)DoS. The Canadian Armed Forces have also revealed to entrench a new systems; the executives of Cybernetics, guided by Chief Administrative Officer, the director General Cyber (DG Cyber). Within that cabinet the newly stationed CAF Cyber Task Force charged to design and construct Cyber Warfare proficiencies for the Canadian Armed forces. The Sub-continent of America, the South America has also risen up and understood the severity of the situation in the Cyber World and has an urge for all the countries in South America to form a joint cyber Shield to protect them from their adversaries and protect the vital data and growing economy however they have not made any law to protect themselves [7] [13] [14].

Conclusion and Suggestions

The Cyber World has only given the nations another more advanced "Field in Warfare" in which the assailant and rivals are not sending rockets and missiles to annihilate cities. They are not landing on the oceanfront for armed warfare. They are attacking with suave attacks by virtue of Internet borders away. With very little investments and wearing the cloak of invisibility/anonymity harming the national interests. The Cyber Space is confronting in both traditional and irregular conflicts. It will expanse from an artless novice to a highly schooled polished hacker, Through Cyberspace rivals will point academia, industry, government, military on land, maritime, and space empire. The exigency in accretion on cyber warfare legislation is vital and needed to develop by each and every nation around the planet as the current laws have failed to prevent the number of the victims from increasing at an escalating rate. The identification of source of Cyber-Attacks is nugatory as the assumed country's government may deny any involvement in these acts of war; With the current trends in rise of the Cyber Warfare; the nation's may choose to develop an exceptionally protected networks or choose to go back to the traditional ways to connect. In many countries, changes in legislation have resulted in the arrest of

computer virus writers. With widespread press coverage, these arrests have probably deterred many youths from developing malicious code. The governmental body has to foresee their own country's networks for any allusion of starting the Cyber Attacks, an intergovernmental organization to promote international co-operation in cyber space must be established and developed. The Cyber Space is only giving another field for antagonistic people to channel their cynicism which has to be disciplined, counseled and stopped by a regulatory organization common around the world. The years of imprisonment and fines imposed on people breaking the law must increase and laws common around the world should be come into existence as laws of some countries may be illegal to use in another countries.

References

1. ANDREW F. KREPINEVICH, Cyber Warfare, a "Nuclear Option"? Defense policy analyst Center for Strategic and Budgetary Assessments. 2012.
2. The Whitehouse National Cyber security Communications Integration Center Arlington, Virginia January 13, 2015, 3:10 P.M. EST.
3. WHITE HOUSE CYBERSPACE STRATEGY, Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel November 16, 2011.
4. Zener Bayudan, Brandon Pitman, John Oleynik, CS4235 at the Georgia Institute of Technology.
5. McAfee, local content white papers hollanderdefacement.
6. Source Country for DDoS Attackwww.foxbusiness.com/technology/2013/04/17/intensity-ddos-attacks-explode-in-firstquarter-average-bandwidth-surges-61/, access on 10th Jan'14.
7. Dancho Danchey's Blog, Security consultant "trends and fads, tactics and strategies, intersecting with third-party research, real time CYBERINT assessments"
8. Cyber Security Strategy for Germany Federal Ministry of the Interior Alt-Moabit 101 D 10559 Berlin, February 2011.
9. Minister of Security and Justice, Ivo Opstelten, Opening NCSC One Conference 2014, World Forum, the Hague, 3 June 2014.
10. Gorman, Siobhan (April 8, 2009). "Electricity Grid in U.S. Penetrated By Spies". The Wall Street Journal. Retrieved November 2, 2010.
11. Kim, Eun-jung. "S. Korean military to prepare with U.S. for cyber warfare scenarios". Yonhap News Agency. Retrieved 6 April 2013.
12. "National Cyber Security Policy of India 2013 (NCSP 2013)". Centre of Excellence for Cyber Security Research and Development in India (CECSRDI). Retrieved 14 August 2014.
13. Khang Pham, Cyber Security: Do Your Part, The Maple Leaf, Vol. 15, No. 2, February 2012.
14. Dilanian, Ken. "Cyber-attacks a bigger threat than Al Qaeda, officials say", Los Angeles Times, 12 March 2013.