CYBER WARFARE : A SERIOUS THREAT TO GLOBAL SECURITY

Pushp Lata Verma

Assistant Professor,

Department of Education in Science and Mathematics (DESM), NCERT, New Delhi.

The fast-changing pace of information and communication technology has changed the way how we communicate, collaborate, share information and do business. In this age, wherein online communication has become the norm, Internet users and governments face increased risks of becoming the targets of cyber attacks. The new information technologies have posed threats in the form of transnational terrorism, international organised crime, cybercrime or hostile information operations directed against national or global interests. For the individual, the risks include confidentiality of their personal and private communications and use of their personal information for unlawful activities. At national levels, cyber war has the potential to paralyse crucial government installations and institutions having serious social and financial ramifications..

Introduction

The advent and global expansion of the Internet may prove to become the fastest and most powerful technological revolution in the history of mankind. Over the years, the number of individuals actively using the Internet has increased everywhere in the world. Today, states, non-state communities, business, academia and individuals have become interconnected and interdependent to a point never imaginable before. The fast-changing pace of information and communication technology has changed the manner in which information was disseminated prior to this technological revolution. It offered opportunities for corporates, academia, professionals and the governments to expand their networking activities for further economic growth and development. Along with opportunities, it also poses a serious threat to peace and security of the world. As businesses and societies in general ever more rely on computers and Internet-based networking, cyber crime and digital attack incidents have increased around the world. It gave transnational terrorism, international organised crime, cross-border criminal gangs, cyber crime, or hostile information operations the opportunity to create financial scams, computer hacking, downloading pornographic images from the Internet, virus attacks, e-mail stalking and creating websites that promote racial hatred, etc. Many countries are ill-equipped to defend themselves against cyber attacks. This has left countries of the world under-defended against sustained, damaging state-level attacks. Some countries have cyber armies and also use a network of patriotic and mercenary hackers that allow the state to deny responsibility. For the individual, the risks include confidentiality of their personal and private communications, and their personal information being compromised. These also include misuse of their personal information

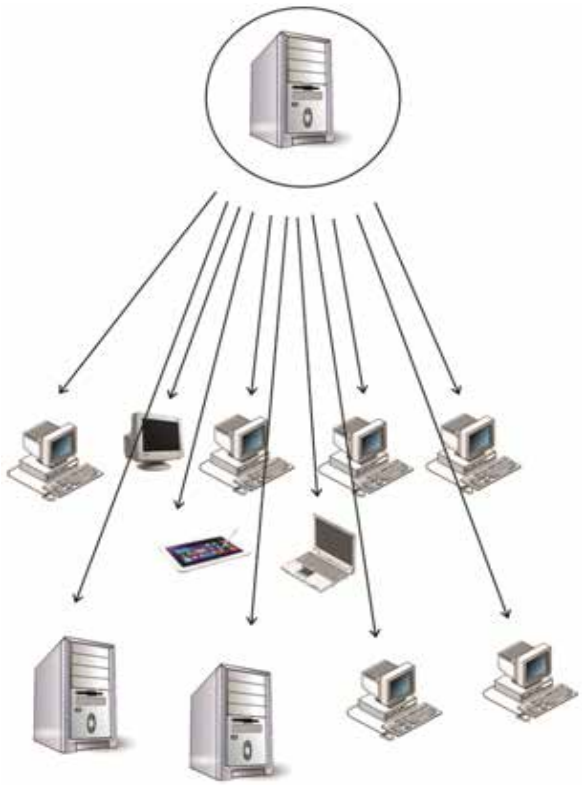

Fig. 1. Scanning Attack Single attack host scans a large number of victims

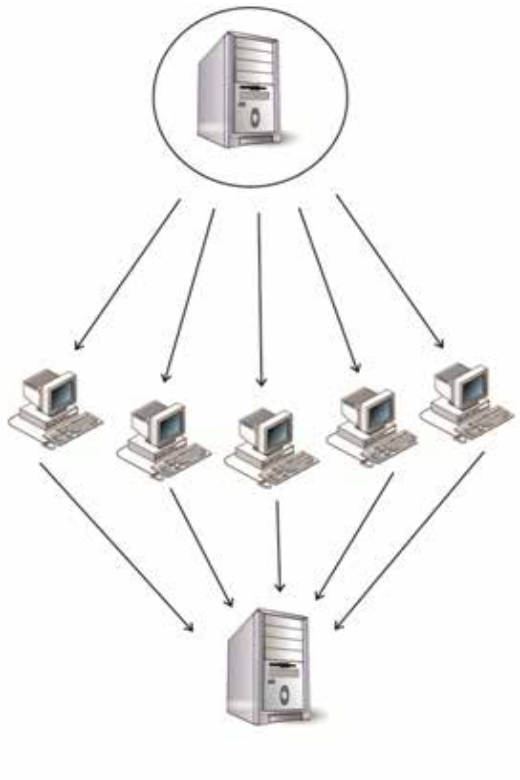

Fig. 2. Denial of Services Attacker uses a number of bots to attack a victim

and additional privacy issues of the smartphone applications and also from mobile operators and service providers.

Cyber Warfare

When interpreting and applying existing international law to cyber warfare, due consideration must be given to the specific characteristics of cyberspace. Most notably, cyberspace is the only domain which is entirely man-made. It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation. Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum. These travel in the form of multiple digitised fragments through unpredictable routings before being reconstituted at their destination. While cyberspace is readily accessible to governments, non-state organisations, private enterprises

and individuals alike, IP spoofing and the use of botnets, for example, make it easy to disguise the origin of an operation, thus, rendering the reliable identification and attribution of cyber activities particularly difficult.

Cyber war refers to conducting operations which impact national security using information as key means of weapon. It means disrupting or destroying information and communication systems of critical infrastructure installations. It also means trying to know everything about an adversary and subverting information flow to either deny or modify information to gain advantage. Thus, cyber war is a war like conflict in virtual space with means of Information and Communication Technology (ICT) and networks. As other forms of warfare, cyber war aims at psychological manipulation of population and influencing the will and decision making capability of the enemy's political leadership and armed forces in the Operations of Computer Networks. Some examples of cyber attacks are the cyber attack on Estonia in April-May 2007, coordinated South Korean – US attacks in July 2009, Stuxnet Computer Worm Attack on Iran's Nuclear facilities in June 2010, etc.

Key Features of Cyber Warfare

With the exponential growth in the ICTs, some proponents think that cyber war will sooner or later replace kinetic war or at least act as a precursor to a physical attack. More frequently, cyber war is presented as a new kind of war option that is cheaper and attractive with less or no bloodshed, and less risky for an attacker than other forms of armed conflict. There are various factors that make cyber attack an attractive option for potential enemy to unleash the cyber war.

i. Cyber war is cheaper since it does not require large number of troops and weapons.

ii. Cyber war is easy to deliver by stealth via global connectivity from anywhere.

iii. Cyberspace offers the attacker anonymity because it is so difficult to trace the origin of an attack. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.

iv. Cyber war may help to avoid the need to engage in combat operations, and thus, results in minimum causalities for the aggressor.

v. Cyber war leads to the ability to disrupt the adversary rather than the risky means of destroying his forces.

vi. Blurs traditional boundaries: Cyber warfare creates its own 'fog and friction of war'.

vii. Cyber war skips the battlefield. Systems that people rely upon such as banks, the electric power grid, air defence radars are accessible worldwide from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defences.

viii. Cyber war happens at almost the speed of light. As photons of attack packets stream down fiber-optic cables, the time between the launch of an attack and its effects is barely measurable, thus, creating more risks for decision makers, particularly in a crisis.

ix. The victim of an attack has to invest considerable resources into neutralizing the threat, which requires teams of dedicated software and hardware experts with specific skill sets. Such persons are difficult to recruit and to retain as private industry offers more attractive terms for their talent.

x. The vulnerabilities of countries increasingly dependent on complex, interconnected, and networked information systems increase over time, thus providing adversaries with a target rich environment and varied attack opportunities.

xi. Cyber war may overwhelm the government, public and private sector resources and services by disrupting functiong of critical information systems. Some of the examples of cyber war threats to individuals, businesses and government are identity theft, phishing, hactivism, compound threats targeting mobile devices and smart phone, compromised digital certificates, denial of services, botnets, and data leakage, etc.

Impacts on Individual Freedom from the Threat of Cyber Warfare

There is often tension between protecting civil liberties and enforcing laws to maintain public safety and order. A new area of such tension has evolved recently from the field of information and communication technology. As cyber space continues to expand in nations as well as globally, so does the increasing cyber attack. Threats in cyber space emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and governments alike. Their effects carry significant risk for personal freedom, privacy, public safety, the security of nations and the stability of the globally linked international community as a whole. Cyber crime and cyber attacks have resulted in changing the dimension of conflict of individual freedoms and national security to a new height. The fear of real or perceived threat of cyber space and of terrorist attack has made easy for government of many nations to pass harsher policies ranging from arrest without warrant, preventive detention and snooping on citizens in various ways. This has become one of the serious threats to individual freedoms and rule of law which serves as the pillar of democracy.

UN Initiatives

Considering the increasing possibility of threat to international peace and security arising from misuse of information and communication technologies (ICTs), the UN General Assembly in 2002 had directed UN Secretary General (UNSG) to constitute a Group of Governmental Experts to consider existing and potential threats in the sphere of information security and recommend possible cooperative measures to address them. In pursuance of the Resolution, UNSG constituted the first UN Group of Governmental Experts (UNGGE) on International Information Security in 2004. So far four Groups have been constituted and India has been a Member in first three Groups. The UNGGE report of June, 2013 underscores that international cooperation is essential to reduce risk of misperception and enhance security in the cyber domain. It contains recommendations to promote peace and stability in State use of ICTs. It provides that international law is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. It also provides for voluntary measures to build trust, transparency and confidence, as well as capacity building for ICT security, especially in developing countries.

Present Scenario

Cyber warfare assumes a significant position in the present scenario owing to some of the parameters that the domain specifically possesses.

a. The omnipresent nature of the warrior is exclusive to this domain wherein the warrior could be present at several locations while carrying out an attack. In fact, the warrior could be digitally present at several locations simultaneously yet be present nowhere.
b. Warrior cloning is yet another exclusive form in this domain of cyber war. Multiplication of systems and innumerable number of instances that can be created at the time of war renders this domain extremely lethal.
c. Geographical spread of a single message may span across several continents.
d. Identity assumptions are so very easy and common in this domain that false flags can be raised easily during conduct of such wars.
e. The entry barriers are so low that the most juvenile nation could enter the domain and start making a difference in the global equations and create assymetries. Cyber attacks have been observed to be originating from cyber space of a number of countries; however, it is difficult to attribute cyber attacks to a particular country. This is because cyber space is virtual, borderless and anonymous due to which it becomes difficult to actually trace the origin of a cyber attack. It has been observed that attackers compromise computer systems located in different parts of the world and user masquerading techniques and hidden servers to hide the identity of the actual system from which the attacks are being launched.

Need for International Cooperation

Cyber warfare is not merely a further technological development in waging war as it represents a completely new category of warfare. The fundamental difference with conventional warfare means that cyber warfare cannot be entirely governed by the current framework of International Humanitarian Law. The regulation of cyber warfare requires an international treaty with global applicability. Focusing on attempts to reconcile cyber warfare within the present Humanitarian Laws needs a relook and requires rectification in the new context of cyber domain. There is an urgent need to regulate the conduct of Nation States in Cyber Space particularly Cyber Weaponization.

Further, threats emanating from the borderless cyber domain necessitate international cooperation amongst States to reduce risk and enhance security. Cooperation in areas such as information sharing and mutual assistance may become essential in responding to a cyber crisis and cyber crimes. These developments show that, in recent years, wider debate has intensified on the development of possible norms of State behaviour and a set of confidence-building measures in the cyber security domain. The challenge is to develop multilaterally agreed principles in areas related to cyber security.

In order to address the problem of Cyber War, there should be a Cyber War Limitation Accord (CWLA) involving all member countries of the United Nations. To start with, CWLA should focus on:

- Establishment of a Cyber Risk Mitigation Centre (CRMC) for sharing information and providing assistance to nations at risk.
- Create international law concepts like obligation to assist and national cyber accountability.
- Limiting cyber attacks to military infrastructure only in case of conflicts and imposing a ban on cyber attacks against civilian infrastructure.

- Impose a ban on usage of Cyber Espionage against rival countries to gather intelligence.
- Prohibit the preparation of the battlefield in peacetime by the deployment of trapdoors, logic bombs on civilian and financial infrastructure.

India and Cyberspace

India ranks third in terms of number of Internet users after USA and China. This number is projected to grow six-fold during the period 2012-2017 with a CAGR (Compound Annual Growth Rate) of 44 per cent. It is worth noting that there are over 381 million mobile phone subscriptions with Internet connectivity in India. As more and more citizens become net savvy, incidences of cyber crime are also expected to increase. These figures confirm that the use of the Internet and ICT – enabled services are becoming more and more an indispensible part of our everyday life. With increasing dependency on technology – be it mobile phones, laptops or tablets, a new breed of tech-savvy fraudsters is coming out with new and more innovative ways of carrying out cyber attacks. According to the Indian Computer Emergency Response Team (CERT-In) there were 8,266 instances of cyber security breaches in 2009. This shot up to 13,201 in 2011. It should be noted that these are reported cases only. As per available reports around 63 per cent of smart-phone users in India have experienced some form of cyber crime. In 2012, the number of cyber crime cases that were registered under the IT Act 2002 in India was 2,876. This number rose by 61 per cent compared to 1,791 cases registered in 2011.

India's Response to Threats in Cyber Space

In India, CERT–In (the Indian Computer Emergency Response Team) has been created as a government-mandated Information Technology (IT) security organization and operates under the Department of Information Technology. Keeping in view the need for a stringent legal regime to deal with cyber crimes and cyber attack, the Parliament of India has enacted the Indian Information Technology Amendment Act, 2008. The Act mandates CERT–In to oversee and ensure that the provision of the legislation are implemented and fully adhered to. Further, CERT–In is also the national nodal agency to respond to computer security incidents. It reports on vulnerabilities and promotes effective IT security practices throughout the country. In 2008, the Indian Information Technology Act was amended to define Cyber Terrorism as an Act punishable with life imprisonment. Taking cognizance of the significant growth in cyber breach instances in India, the Government came out with the National Cyber Security Policy (NCSP) in July 2013. It covers a wide range of topics, from institutional frameworks for emergency response to indigenous capacity building. Also, the Government of India has proposed a cyber-security architecture which envisages a multi-layered approach for ensuring defense in-depth.

Cyber-crime and cyber attacks have resulted in changing the dimension of conflict of individual freedoms and national security to a new height. The fear of real or perceived threat of cyber space and of terrorist attack has made easy for government of many nations to pursue policies ranging from arrest without warrant, preventive detention, snooping on citizens,

etc. This has raised concerns about individual freedoms and rule of law which serves as the pillar of democracy. However, the government of India is profoundly concerned about human rights violations.

India is aware that terrorism in all its forms poses a major threat to national security, human security and individual freedoms all over the world. India's anti-terrorism legislations are in line with the relevant international instruments and commitments including the United Nations Global Counter-Terrorism Strategy. Such legislations are assessed at regular intervals so as to ensure that it is fully compatible with national security and individual freedom.

Conclusions

The phenomenon of cyber warfare does not exist in a legal vacuum, but is subject to well-established rules and principles. That being said, transposing these pre-existing rules and principles to the new domain of cyberspace encounters certain difficulties and raises a number of important questions. Some of these questions can be resolved through classic treaty interpretation in conjunction with a good measure of common sense, whereas others require a unanimous policy decision by the international legislator, the international community of states. For the time being, cyber warfare has not had dramatic humanitarian consequences, and it is to be hoped that this state of affairs will not change in the future. The potential for human tragedy, however, is already enormous, it is likely to increase with our growing dependence on computer-controlled systems to sustain our daily lives. It is all the more important, therefore, that states be aware not only of their legal duty to examine whether new weapons and methods employed in cyber warfare would be compatible with their obligations under existing law, but also of their moral responsibility towards generations to come.

References

Annual Report 2013-2014. Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India.

Barua, Yogesh. 2005. *Criminal Activities in Cyberworld*.

Brenner, Susan W. 2012. *Cyber Crime*.

Cahill, Kevin. 1986. *Trade War*.

Dasgupta, M. 2009. *Cyber Crime in India: A Comparative Study*.

Singh, Capt. Mithlesh Kumar. 2009. *Cyber War and Terrorism*.

Thomas, Douglas. 2000. *Cyber Crime*.