Page 689 - 696

DOI: *http://doi.one/10.1732/IJLMH.25227*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 6

2020

International Consensus on Cyber Warfare: Challenges and Implications

DR.CH.LAKSHMI[1]

ABSTRACT

The International community emphasized State sovereignty with an object to promote the norms set forth in the United Nations Charter. Accordingly, each State has sovereign power and will have to protect their nation includes people and property. With this concept, number of international conventions was drafted including International Humanitarian Law or Law of Armed Conflicts or Law of War which emphasized on traditional warfare. On contemporary, the modern era is the evident of drastic changes in technology. It has a great impact in each and every walk of the life of the people includes in warzone. The current system of technology paves a new platform to a modern warfare through sophisticated equipment which is available to every human being. Now, not only conventional military weapons such as tracked and directed by computer, computer itself is a weapon to target the military and entire system of the enemy State. Globalization makes everything be globalized including the safe guards and security aspects of the nations too. It is a known fact, technology not only dominates the human activities and it also plays a vital role in dominating State activities without observing the principle of State Sovereignty. This paper aims to understand the impact, use of technology in warfare and its impact on the society.

Keywords: *State Sovereignty, Armed Conflicts, Globalization, Cyber War and Cyber Crime*

I. INTRODUCTION

In 1945, after math of two great world wars, with a great consensus the International community had arrived to a conclusion and thereby promoted United Nations Charter to save succeeding generations from scourge of the war.[2] To this extent, they wanted to unite their strength to maintain international peace and security and to ensure by acceptance of the principles and the institution of methods, that armed force shall not be used. The International community emphasized State sovereignty with an object to promote the norms set forth in the

[1] Author is a Asst.Professor at Damodaram Sanjivayya National Law University, Visakhapatnam, India.

[2] Preamble to the United Nations Charter

[ISSN 2581-5369]

United Nations Charter. Accordingly, each State has sovereign power and will have to protect their nation includes people and property. Public International law is very clear in all aspects of States' responsibility in protecting and promoting peace on one hand and conversely imposes an obligation not to intervene in others' sovereignty except under certain necessary conditions. Art.2 (4) of the United Nations' Charter Strictly prohibited the use or threat of use of force against other State and conversely, the United Nations' Charter shall not impair the inherent right of the States where there is a threat to their nation and security. State's sovereignty had been emphasized by the international community with an object to promote the norms set forth in the Charter of United Nations. Accordingly, each State has Sovereign power and they shall protect their nation. With this concept, number of international conventions was drafted with a view to protect and promote rights of the human beings and on the other hand, they imposed an obligation on nations with a view to promote the world peace but not into pieces. Unfortunately, the drafts men of the international documents, especially all the four Geneva Conventions which places severe obligation on the parties to the armed conflict in resorting the use of force but whereas it shall not provide any specific room for cyber warfare which is the current day quandary facing by many States due to the advent of technology. Everyone knows about the repercussions of the war fare on the societies. The entire world is the evident of the last two major world wars.

Even the word 'War' is a single monosyllable but it has a great impact on the society. If war takes in any place it could not be impossible to re-establish the society to its normal stage. It's not only effects on military and military objectives, it has a great impact on the day to day life of the civilians. War inevitably results in immeasurable suffering among people and in severe damage to objects. Second World War catastrophe had a great impact on the society and many people lost their lives, War has such a great disaster in any place and caused to violation of fundamental freedoms and human rights. Hence, States with all the support of other States decided to Unite to defeat these situations by the reason of saving younger or future generation from the scourge of war. Accordingly, the Charter of the United Nations recognized the principle of sovereign equality of all its Members. Further it has as its central concern reaffirms its faith in the fundamental human rights and the dignity of human personality and in the equal rights of men and women and of nations large and small. Due to these reasons, to achieve its goal, and to protect the rights of human beings with the effects of warfare, it puts its utmost effort by bringing the rules relating to warfare. The Second World War which was the major verity to promote Geneva Conventions by the International Community was a memorable impetus in the world's history to protect the rights of succeeding generations from the scourge of warfare. But, there are still some gaps in the four Geneva Conventions, such as the rules governing aerial bombings are not stipulated in the Conventions. To overcome those loopholes and to include some new circumstances, International community was felt as an urgent necessity in the reaffirmation and development of rules in conducting the hostilities activities. With that result, governments adopted Protocol s I and II additional to the Geneva Conventions, which combine elements of Hague and Geneva Law in the year 1977 which had a great impact on the society. The Protocols have very broad acceptance and their provisions are considered as customary law. The Geneva Conventions and their Additional Protocols are at the foundation of Modern International Humanitarian Law. The aim of international law is to regulate the conduct of warfare and seeks to minimize its effect on the society. They specifically protect people who are not taking part in the hostilities (civilians, health workers and aid workers) and those who are no longer participating in the hostilities, such as wounded, sick and shipwrecked soldiers and prisoners of war. The Conventions and its two Protocols emphasized certain measures to be taken to prevent or put an end to all breaches. They contain stringent rules to deal with what are known as "grave breaches". Those responsible for grave breaches must be sought, tried or extradited, whatever nationality they may hold.

On contemporary, the modern era is the evident of drastic changes in technology. It has a great impact in each and every walk of the life of the people and without which one cannot sustain in the society. Not only individuals and Society, to maximum extent State also dependent upon such technology to carry out their manifold activities. People are acquainted with the word malware[3] which causes damage to computer without the knowledge of the owner and technological advancement in communication corroding the boundaries which are necessary for autonomous states' policy and sovereignty of the State, which has been recognized by the international community. Technology has such a powerful weapon and more dangerous rather than nuclear bomb.

In reality, cyber space as the global digital communication can deliver vast benefits to individuals and societies. Due to this reason, cyber technology and cyber security has become much importance to everywhere where as a lack of such security resulted into many threats and leads to terrorism. Perhaps one of the most serious threats facing by States is the use of cyber capabilities to conduct military style operations with the aim of degrading, denying or destroying information resident on computers or computer networks. Such threats fall under

[3] This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of **malware** including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer.

the banner of cyber war.[4] The current system of technology paves a new platform to a modern warfare through sophisticated equipment which is available to every human being. Now, not only conventional military weapons such as tracked and directed by computer, computer itself is a weapon to target the military and entire system of the enemy State. An attack could eventually make the entire technology with deadly equipment against its controllers. An attack launched across the globe could massive damage. Globalization makes everything be globalized including the safe guards and security aspects of the nations too. Cyber crimes, Cyber attacks and cyber warfare have been rapidly increasing in the recent years with the advent of technology. At the outset, these attacks similar to be armed attack which is the subject matter of the law of warfare.

Despite the fact, that Geneva Conventions and Additional Protocols have had a great impact on States to its foster respect and enhancement of International Humanitarian Law, conversely it does not encompass any specific rules for prohibition of threat to use of force by using technology. It only prohibits and limits the use of force by belligerent States (jus in bello) under the principles of law. But at international level, there is no specific law or treaties to prohibit the use of force through technologically even the consequences of the technology are higher in its volume. Any act which caused to kill or injure persons or destroy or damage objects are unambiguously uses of force without observing the fundamental principles of international humanitarian law are said to be violation under international law. Though, the International community recognized the principles of Jus ad bellum[5] and jus in bello,[6] but in practice, these are not undoubtedly observed by the International community.

In the contemporary situations, the advent of technology on human society is incredible. It is a known fact, technology not only dominates the human activities and it also plays a vital role in dominating State activities without observing the principle of State Sovereignty. Due to this reason, it’s a high time to the international community to identify the contemporary situation and take necessary measures to achieve the goals of the United Nations Charter.

II. What is cyber warfare?

Cyber warfare refers to an unauthorized intrusion into a computer or a network, in order to commit crimes like hackers. It is organized by governments, and is incredibly sophisticated. The internet touches almost every part of our modern infrastructure from the power grid to the machines that produce our goods even our internet itself can be taken down. Cyber war

[4] Russell Buchan; Nicholas Tsagourias, Cyber War and International Law, 17 J. Conflict & Sec. L. 183 (2012)

[5] Right to war

[6] Right uses of forces in war

isn’t just an attack on a government, it can stop the entire nation dead and further it also targets the military directly. An attack could prevent missiles from finding targets or launching communications could be disrupted or cut off completely. After the first ‘Stuxnet attack’ on Iran in 2010, many international legal experts who helped to draw up a Non Atlantic Treaty Organizations (NATO), commented that ‘the Stuxnet[7] attack against Iran was an illegal act of force’ and it might have been ‘Armed Attack’ or ‘Cyber War’’.

WHAT IS STUXNET ATTACK: It’s a type of 500-kilobyte sophisticated computer virus/worm that infiltrated numerous computer systems and exploits the entire infrastructure of the nation. This virus physically destroys bomb making machines. This is a digital virus which has been developed as a tool to derail or at least delay the computer programs in developing nuclear weapons. This virus operated in three steps such as----

- Firstly, it analyzed and targeted Windows networks and computer systems. The worm, having infiltrated these machines, began to continually replicate itself.
- Secondly, the machine infiltrated the Windows-based Siemens Step7 software. This Siemens software system was and continues to be prevalent in industrial computing networks, such as nuclear enrichment facilities.
- Lastly, by compromising the Step7 software, the worm gained access to the industrial program logic controllers. This final step gave the worm's creators access to crucial industrial information as well as giving them the ability to operate various machinery at the individual industrial sites.[8] Through this method, one State can attack on other States Technology (including computer programs) which plays a pivotal role for its nation.

It has been proved that over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random worker's USB drive. One of the affected industrial facilities was the Natanz nuclear facility. The fist signs that an issue existed in the nuclear facility's computer system in 2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. The cause of these failures was unknown at the time. Later in 2010, Iran technicians contracted computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered

[7] A malicious computer worm

[8] Stuxnet Worm Attack on Iranian Nuclear Facilities, Michael Holloway, July 16, 2015, submitted as coursework for PH241 Stanford University, Winter 2015

multiple malicious files on the Iranian computer systems. It has subsequently revealed that these malicious files were the Stuxnet worm. Although Iran has not released specific details regarding the effects of the attack, it was estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. With these estimations, this constituded a 30% decrease in enrichment efficiency.[9]

According to the sources, firstly it was found in Iran, Indonesia and India and nearly 85% of their technology which was severely infected. Its aim was not just cause damage to the computers but to cause handicapped the entire nation without having any physical effects. The worm is often said to have been first discovered in 2009 or 2010 but was actually found to have attacked Iranian's nuclear program as early as 2007. This attack targets Supervisory Control and Data Acquisition (SCADA) control systems for large infrastructures.Iran and Indonesia were the first two countries which were affected by the cyber war. However, due to a 'flaw' in coding, the virus spread to other parts of the world. India and several other countries were caught in the aftermath of the world's most sophisticated cyber war. Some reports claim that India is the third most infected country.[10] The reason is On July 7, 2010, a power glitch in the solar panels of India's INSAT-4B satellite resulted in 12 of its 24 transponders shutting down. As a result, an estimated 70% of India's Direct-To-Home (DTH) companies' customers were without service. Once it became apparent that INSAT-4B was effectively dead, many people from international community said that India also one of the effected party of ' Stuxnet' worm. Many international law experts declared that cyber attack that sabotaged Iran's uranium enrichment program was an "act of force" and was likely illegal. Any act of force which destroy or damage objects or uses force without a reasonable cause could termed as the violations of the international principles of peace and security.

III. CYBER WORLD AND ITS PHASES

Today, the entire world is in virtual reality. Computers, the data networks that interconnect them and the services available over the networks make up this cyberspace. As cyberspace invades almost all areas of modern day living, playing, and working, it is becoming more important that people understand its technical and political underpinnings and operations, as well as its capabilities, threats, and weaknesses. There are three phase of cyber actions at present prevails in everywhere. They are as Cyber crime; Cyber attack; and Cyber war are the major phases in cyber world. In fact, each phase is inter linked with other phase and could

[9] ibid

[10] http://stsfor.org/content/stuxnet-vulnerability-scada-systems-and-india

indirectly effect without knowing the other side. Each phase has a severe impact on individuals, society and States too.

What is a Cyber Crime? It may be also referred as computer crime. Here, a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

With the development of the technology and its intrusion in the other fields,

"Just as the Fourth Geneva Convention has long protected civilians in times of war, International Community now desires to have a Digital Geneva Convention that forces governments in protecting the rights of civilians from Nation-State attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against Nation-State cyber attacks requires the active assistance of technology companies. The technology sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a 'Neutral Digital Switzerland, that assists customers everywhere and retains the world's trust."[11]

IV. CYBER WAR AND ITS IMPACT ON THE SOCIETY

Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes. Kinetic cyber attacks are a real and growing threat that is generally being ignored as unrealistic or alarmist. Kinetic is nothing but a force applied by unknown people against unknown persons. For example-- Dropping bombs , shooting bullets , any form of violent behavior.

In the 21st-century military is exploring less violent and more high-tech means of warfare, such as messing electronically with the enemy's communications equipment or wiping out its bank accounts. These are "non-kinetic." Kinetic military action is a euphemism for military action involving active warfare, usually including lethal force. "Kinetic" was used as a retronymic euphemism for military action in Bush at War, a book by Bob Woodward in 2002.

[11] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#_ftn1

In the light of the hacking of the website of the Indian Space Agency's commercial arm in 2015, Antrix Corporation and government's Digital India programme, a cyber law expert and advocate at the Supreme Court of India, Pavan Duggal, stated that "a dedicated cyber security legislation as a key requirement for India. It is not sufficient to merely put cyber security as a part of the Information Technology Act. We have to see cyber security not only from the sectoral perspective, but also from the national perspective." Hence, there is a heavy need for a Digital Geneva Convention. Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell or exploit them. In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries. All these could be possible only with the best efforts of International consensus only.

*****