ROLE OF CYBER ATTACKS IN RELATION TO STATE'S PEACE AND SECURITY

*Written by **Anurag Mehta***

Law Graduate- 2017

INTRODUCTION

International law may well be described as the question of disciples which deal with global order. International law represents the essence of the progress of civilization towards a world ruled by law rather than a world ruled by force. It took thousands of years of effort, hundreds of wars and the sacrifice of millions of lives to achieve this. International tool is an essential tool for the abolition of war.

International law consists of rules and principles governing the conduct of states in their relations among themselves. Compliance with international law is the ordinary state of affairs. States normally follow the rules. Compliance is caused by the commonly shared expectation that governments and individuals will abide by the law; the disapproval and condemnation that result when rules are broken; the loss of standing suffered by a rule-breaking state, which can have adverse diplomatic and economic consequences; and the availability of sanctions including economic measures like trade embargoes and in extreme cases, the use of force directed by the Security Council.

The most authoritative statement on the sources of international law is contained in Article 38(1) of the Statute of the International Court of Justice (see end of lesson), an integral part of the UN Charter. The Statute identifies five sources:

1. Treaties (Conventions)

2. Customary International Law

3. General Principles of Law Recognized by All Nations

4. Judicial Decisions

5. Teachings of the Most Highly Qualified Jurists.

At the same time, military reliance on computer systems and networks has increased exponentially, thus opening a “fifth” domain of war-fighting next to the traditionally recognized domains of land, sea, air and outer space. Cyber security is considered to be a hot topic in international law today and very pertinent to international security discussions. It is crucially important that civil society have access to safe and secure internet. ‘Cyber mania’ is regarded as an overreaction to the threat of cyber-attacks. The major challenge to governments is to ensure that people are primarily protected from crime and espionage on the internet. The vast majority of cyber-attacks are not carried out by government sponsored hackers but by criminals intending to steal business secrets and financial information. Therefore, there have been strong attempts to discourage governments characterizing the internet as being seen a war-fighting problem. To fit the internet security problem into the war-fighting category has also led to flawed analysis of the relevant international law. There is appropriate international law relevant to supporting commerce and communication on the internet, but that law is not the law of international armed conflict.

Internet security concerns are as old as the internet itself. There was an attack in1998 by some 3000 Chinese hackers on Indonesian government sites. Since then, there have been tens of thousands of attempts to hack into major computer networks belonging to defence ministries, banks and the media. Such incidents are happening daily. Most of these cyber intrusions have espionage or theft as the purpose and are typically categorized as ‘computer network exploitation’ (CNE). A smaller group is being referred to as ‘computer network attacks’ (CNA). Perhaps these should better be referred to as ‘computer network interference’ (CNI), as opposed to CNE or CNA. CNI would be closer to the language of economic or trade injury than ‘attack’, which is a term more closely associated with the military category.

Georgia-Russia, 2008: This was the first known use of the internet during a conventional armed conflict to interfere with civilian use of the internet; it occurred in the 2008 conflict in the Georgian enclave of South Ossetia. Georgia triggered the conflict by attacking Russian soldiers who were part of a peacekeeping contingent in South Ossetia under the terms of a Georgia- Russia treaty of 1991. On the night of 7-8 August, Georgia staged a conventional military attack, killing approximately a dozen Russian soldiers and wounding many others. Russia conventionally counter-attacked pushing to within 35 miles of the Georgian capital, Tbilisi. Georgia claimed that Russia initiated distributed denial of service (DDoS) attacks against a number of Georgian websites, including government sites, media sites, and commercial sites. The interference last approximately a month. The physical fighting had lasted about a week.

Stuxnet, 2009-2010: A computer worm, dubbed Stuxnet, infected computers manufactured by Siemens and used in the Iranian nuclear programme. The worm is believed by experts to have been created by the United States military with assistance from Israel and scientists at Siemens. The effect of the worm in Iran was to cause centrifuges to turn far more rapidly than appropriate. In early 2011, officials in Israel and the US announced that Iran's nuclear programmes had been set back by 'several years.' The Stuxnet worm, however, affected computers in other countries as well, including India, Indonesia, and Russia. It is believed that 40 per cent of the computers affected were outside Iran. Stuxnet is said to be the 'first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.' Ralph Langner, a German computer security expert, was thought to be convinced that Stuxnet is a government produced worm: 'This is not some hacker sitting in the basement of his parents' house. To me, it seems that the resources needed to stage this attack point to a nation state.'

Cyber-crime is a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and worldwide web. The Indian law has not given any definition to the term 'cyber-crime.' In fact, the Indian Penal Code does not use the term 'cyber-crime' at any point even after its amendment by the Information Technology (Amendment) Act, 2008. The IT (Amendment) Act, 2008 is known as cyber law. It has a separate chapter XI entitled 'offences' in which various cyber-crimes have been declared as penal offences punishable with imprisonment and fine. • Under the law of neutrality, the questions arise as to whether belligerents can lawfully use the telecommunications infrastructure of neutral states for the purpose of cyberattacks, and what the responsibilities of "neutral" states are with regard to non-state belligerents conducting attacks from within or through its territory or infrastructure.

Under the law governing the resort to force between states (jus ad bellum), it will have to be determined in what circumstances, if any, cyber operations can amount to (a) an internationally wrongful threat or use of "force", (b) an "armed attack" justifying the resort to necessary and

proportionate force in self-defense, or (c) a "threat to international peace and security" or "breach of the peace" subject to UN Security Council intervention
The term "attack" is an important technical term of IHL in that many of its fundamental rules on the conduct of hostilities are expressed in terms of attacks. For example, "the civilian population as such, as well as individual civilians, shall not be the object of attack" "civilian objects shall not be the object of attack", "indiscriminate attacks are forbidden" and "attacks shall be limited strictly to military objectives".
Most attacks on the Internet consist of opportunistic attacks rather than attacks targeted for some specific entity. An opportunistic attack is when an attacker targets various different parties by using one or various generic ways to attack such parties, in the hope that some of them will be vulnerable to attack. In an opportunistic attack, an attacker will have a large number of targets and will not care that much on who the victim is, but rather on how many victims there are.

An attacker will generally find it much easier to make use of an opportunistic attack then a targeted one, simply because a broad scope will probably have a better chance of success in gaining access to sensitive information. There is simply more money (and possibly less risk) in computers that are vulnerable to common attacks and not well guarded, than attacking a specific company or person which might be better protected against such attacks. In a test, which lasted two weeks (TechWeb, 2006), AvanteGarde concluded that on average, it takes four minutes for a new Windows machine exposed to the Internet to get hacked.

Offences like tampering with computer source documents, whoever knowledge or intentionally conceals, destroy or alters or intentionally or knowingly causes another to conceal destroy or alter any computer source code used for a computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment upto 3 years or with fine which may extend up to 2 lakh rupees or with both. Hacking with computer system, publishing of information which is obscene in electronic form, publication for fraudulent purpose, breach of confidentiality and privacy, data theft, spreading virus or worms, identity theft, e-mail spoofing.

Cyber-attacks can be controlled if certifying authorities take proper precaution while issuing certificates. The details of the person who is certified should be keeping confidential so that hacking, if any could be controlled by the control private key. Blocking of websites an explicit in IT Act, 2000 is available only in section 67, relating to pornographic content on the website. Section 69 of the IT Act, 2000 empowers the authorities to intercept any information transmitted through any computer source in relation only to the following five purposes, interest of the sovereignty, the security of the state, friendly relations with foreign states, public order, for preventing incitement to the commission of any cognizable offence.

Such websites promoting hate content, slander or defamation to others, promoting gambling, promoting racism, violence and terrorism and other such material in addition to promoting pornography, including child pornography and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Cyber-attacks causes' mass destruction to the society & nation. One of the tool of cyber-attack is virus. Virus which destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme data or instruction is executed or some other event takes place in that computer resource.

New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce. The UNCITRAL adopted the model law on electronic commerce in 1996.

Some factors of cyber-attacks are e-mail, network attack, instant messenger attacks, distributed denial of service attacks (DDoS), bypassing security mechanism, bypassing the traditional anti-virus, bypassing e-mail content filtering, bypassing the firewall, bypassing IDS/IPS. For this asymmetric crypto system should be followed.

Take appropriate steps to respond to a cyber-incident- assess the nature and scope of an incident and identify what information systems and types of information have been accessed or misused. Promptly notify your primary regulator when you become aware of an incident involving unauthorized access to or use of sensitive customer information, and generally, following any incident that could materially impact your institution. Comply with applicable suspicious activity reporting regulations and guidance. Ensure appropriate law enforcement authorities are notified in a timely manner. Take appropriate steps to contain and control the incident to prevent further unauthorized access to or misuse of information. Notify customers as soon as possible when it is determined that misuse of sensitive customer information has occurred or is reasonably possible.

The customary international law of countermeasures governs how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense—including, implicitly, cyber-attacks. The Draft Articles on State Responsibility define countermeasures as *"measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."*

The international law of countermeasures does not define when a cyber-attack is unlawful. Instead it simply provides that when a state commits an international law violation, an injured state may respond with a reciprocal act. As explained above, some cyber-attacks that do not rise to the level of an armed attack nonetheless violate the customary international law norm of nonintervention. These violations may entitle a harmed state to use countermeasures to bring the responsible state into compliance with the law. The Draft Articles lay out the basic customary international law principles regulating states' resort to countermeasures. The Draft Articles provide that countermeasures must be targeted at the state responsible for the prior wrongful act and must be temporary and instrumentally directed to induce the responsible state to cease its violation. Accordingly, countermeasures cannot be used if the international law violation has ceased. Countermeasures also can never justify the violation of fundamental human rights, humanitarian prohibitions on reprisals, or peremptory international norms, nor can they excuse failure to comply with dispute settlement procedures or to protect the inviolability of diplomats.[162] Before resorting to countermeasures, the injured state generally must call upon the responsible state to cease its wrongful conduct, notify it of the decision to employ countermeasures, and offer to negotiate a settlement. However, the injured state *"may take such urgent countermeasures as are necessary to preserve its rights."* Countermeasures need not necessarily be reciprocal, but reciprocal measures are favored over other types because they are more likely to comply with the requirements of necessity and proportionality.

In the cyber-attack context, an attacking state may violate its obligation not to intervene in another sovereign state through a harmful cyber-attack, and so the state that has been attacked may employ lawful countermeasures. The most important countermeasures in this context are so-called "active defenses," which attempt to disable the source of an attack; passive defenses, by contrast, such as firewalls, merely attempt to repel cyber-attacks.

While no comprehensive international legal framework currently governs all cyber-attacks, a patchwork of efforts provides some tools the United States and other countries can employ to control this growing threat. This Section surveys legal mechanisms created by the United Nations, NATO, the Council of Europe, the Organization of American States, and the Shanghai Cooperation Organization to directly regulate cyber-attacks. While both the Council of Europe and the Organization of American States have taken actions relating to cyber-crime—a category of activity that overlaps in part with cyber-attacks, as noted above—the increased computer network protection and regulations are also relevant to efforts to combat cyber-attacks. Collectively, these organizational measures demonstrate a growing interest in addressing this issue through common legal frameworks. Yet these efforts have fallen short of establishing a rigorous legal framework that can effectively govern all cyber-attacks.

Cyber-crime is considered one of the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cyber-criminal syndicate. The ''cybercrime industry'' operates exactly as legitimate businesses working on a global scale, with security researchers estimating the overall amount of losses to be quantified in the order of billions of dollars each year. In respect to other sectors, it has the capability to quickly react to new business opportunities, benefiting from the global crisis that-in many contexts- caused a significant reduction in spending on information security.

The prevention of cyber-criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concept of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their ''attack surface'' and mitigate the risks. Education and training are essential to create a culture of security that assumes a fundamental role in the workplace. Every member of an organization must be involved in the definition and deployment of a security policy and must be informed on the tactics, techniques and procedures (TTPs) belonging to the cybercriminal ecosystem.

Prevention means to secure every single resource involved in the business processes, including personnel and IT infrastructure. Every digital asset and network component must be examined through a continuous and an evolving assessment. Government entities and private companies must cooperate to identify the cyber threats and their actions-a challenging task that could be achieved through the information sharing between law enforcement, intelligence agencies and private industry. Additionally, sharing threat information is another fundamental pillar for prevention, allowing organizations and private users to access data related to the cyber menaces and to the threat actors behind them.

At the last INTERPOL- Europol conference in October, security experts and law enforcement officers highlighted the four fundamentals in combating cybercrime as:

- Prevention
- Information Exchange
- Investigation
- Capacity Building

In September 2014, Troels Oerting announced the born of the Joint Cybercrime Action Taskforce (J-CAT) with the following statements that remark the necessity of an efficient collaboration between the entities involved, not excluding the Internet Users. Prevention activities must be integrated by an effective incident response activity and by a recovery strategy to mitigate the effects of cyber incidents.