Cyber Law Dynamics : Indian Challenge

– Santosh Khadsare
Scientist 'E' in CERT-In (Cyber Forensics), Ministry of Electronics and Information Technology
santoshkhadsare@gmail.com

"To deliver justice for the misadventures in the cyber domain, walls have to fall between nations and a consensus has to be built at any cost."

– @santkhad2

Introduction

Cybersecurity is an intrinsic part of human security and is inalienable from daily human lives. Cybercrimes are on the rise and have increased exponentially over the past few years. Cybersecurity has become a multifaceted issue and mere unilateral action will not suffice to meet cybersecurity needs of various stakeholders. The increased dependency on networks (local networks as well as the internet), sharing of information in Cyber domain and their inherent vulnerabilities which surface on a daily basis, lack of mutual consent between nation states on effective control of operations in Cyber domain and Cyber laws has brought a new type of threat : Cyber Warfare. Concept and definition of the term Cyber warfare is an interesting and never ending debate. Laws of armed Conflict (LOAC) cannot be applied as it is for cyber domain as not every attack can be treated as an act of war. Many countries and non-state actors are not only involved in Cyber Crimes, Cyber Espionage and Cyber Reconnaissance; they are effectively creating offensive Cyber Warfare capabilities and engaging in Cyber-attacks with increasing rate.

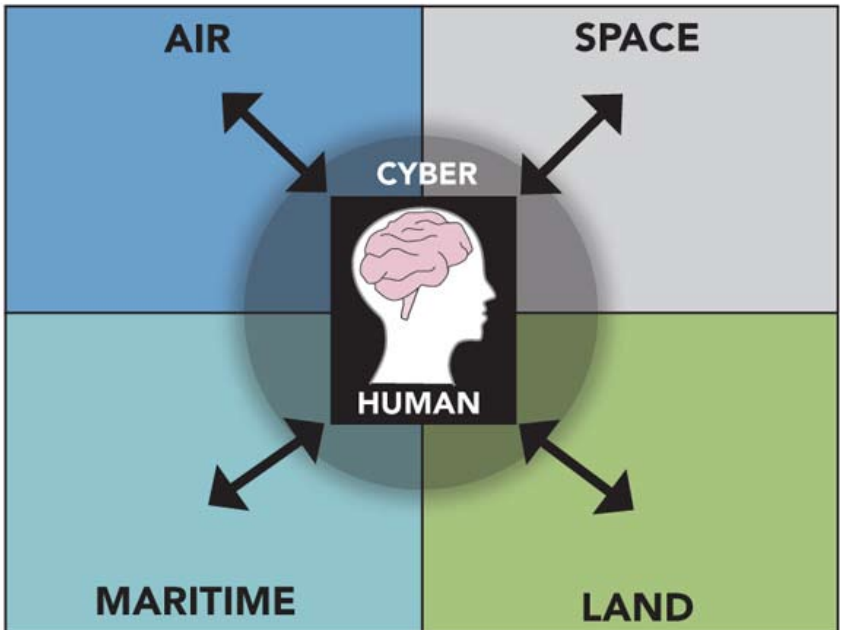
There are reports of cyber-attacks and network intrusions, especially the attacks on Critical Information Infrastructure (CII) that can be linked to nation states. What is more disturbing is that much financial aid and intellectual mind is being utilized by many countries on how to conduct Cyber Warfare rather than preventing it. In fact, there is a surprising lack of international dialogue and Cyber Laws with respect to the controlling Cyber space. Key issues in cyber domain such as attribution and role of every player (state or non- state) will be an important factor in decidingwhetherthe conflict is a cyber war. Paul J. Springer in this book "Cyber Warfare" has said "*Beauty is in the eye of the beholder, acts of war in the eye of the recipient*".

Cyber War

The aim of warfare for years was capture of territory. The medium which was used was land, sea,air and space. However, the use of force may be less applicable in a new battlefield made up of digital bits where the boundaries re blur, weapons used are difficult to detect and players can easily be hidden as non-state actors. The increased dependency on communication and data networks, storage of information in these networks and their vulnerabilities to outside world, perception management through ever present media and advances in electronic warfare technologies has forced countries to shift to fifth domain of warfare known as **'Cyber Domain'**. It is a volatile, mutable, manmade environment. Cyber-attacks on CII (military infrastructure, government, financial institutions, etc.) pose a rapidly growing threat to national security of our country.

Cyberspace. The term coined by William Gibson *'Cyberspace'* is the global, virtual, Information and Communication Technology (ICT) based environment, including the Internet, which directly or indirectly interconnects systems, networks and other infrastructures critical to the needs of society. Cyberspace exists across the other domains of land, sea, air, and space and connects these physical domains with the cognitive processes that use the data that is stored, modified, or exchanged.

Figure 1: Cyberspace as Fifth Domain of Warfare



Cyber Warfare. Cyber Warfare can be termed as a warlike confrontation or a peace time activity in virtual space called the Cyberspace with means of information and communication technology (ICT) and networks. Cyber Warfare aims at influencing the will and decision making capability of the enemy's political leadership, Armed Forces and population in the domain of Computer Network Operations (CNO). Three forms of CNO are highlighted in succeeding paragraphs:-

- **Computer Network Attack (CNA)**. Operations designed to disrupt, deny, degrade, or destroy information present in computers and computer networks.

- **Computer Network Exploitation (CNE)**. Computer Network Exploitation means retrieving intelligence-grade data and information from computers of Government, financial institutions, defense forces and critical infrastructures.

- **Computer Network Defense (CND)**. Consists of all measures necessary to protect own information and communication infrastructure against enemy or hostile Computer Network Attack and Computer Network Exploitation.

Why is Cyber Warfare Preferred?
Cyber Warfare is preferred mode of conduct of Operations in 21st century due to the following reasons:-

- **Attribution** Attribution of attacks in Cyberspace is difficult which gives advantage to the attacker to choose the location, timing and impact of Cyber-attacks.

- **Asymmetric Tool**. Cyberspace Operations acts as an asymmetric tool for nations with comparatively weaker Conventional force to gain military advantage.

- **Low Cost and High Impact**. Cyberspace is open to anyone who can afford low cost network infrastructure and expertise. Thereafter Cyberspace Operations can be launched against the Critical Information Infrastructures(CIIs) of a country which renders a substantial asymmetric advantage to the attacker.

- **Common Platform to Four Operational Domains.** Cyberspace domain acts as a common platform to orchestrate the battle in four operational domains (Land ,Sea, Air and Space).

Cyber Law

"Cyber space is a domain within which security, responsibility and accountability is incredibly essential. Cyber Laws provide a security backing to the digital society."

Internet has considerably modified he manner we predict, the manner we tend to govern, the manner we tend to do business and also the manner we tend to determine ourselves. Information technology is skirting everything in the present world. Ethical and criminal wrongdoings are the creation of the ubiquitous cyber domain. It has become the way to vent out criminal attributes of a person. Cyberspace is open and everyone can participate. "Information Technology" has brought transition to a paperless world helping in addressing resources initially used. Various activates are being carried out by us in cyberspace and the existing laws cannot be applied and interpreted in this light. Therefore, new cyber laws are required to govern the internet which should enable and accommodate legal infrastructure in line with present times. Cyber Law is the law governing cyber space. Cyber

space includes computers, iPods, networks, software's, data storage devices *(such as hard disks, USB disks etc.),* the Internet, websites, emails and even electronic devices such as smart phones, smart watches, ATM machines, etc.

Indian Cyber Laws

India parliament passed the Information Technology Act, 2000 on 17th October, 2000 which is applicable to whole of the country including Jammu and Kashmir and also is for acts committed outside India but having effects in India. It provided legal foundation for E-Commerce. The Act covers computer related crimes such hacking, cyber stalking, espionage, cyber terrorism, obscenity, identity theft, patent infringement, etc. but does not cover cyber warfare. The Information Technology Act when enacted brought about changed in existing acts such as Indian Penal Code (IPC), Indian Evidence Act and Bankers Books Evidence Act. Few provisions were added/amended to it after deliberations. The amended act is known as 'The Information Technology (amendment) Act, 2008'. Main objective of IT Act (Amendment) 2008 was providing security backing to the digital society.

Global Cyber Laws And Treaties

As on date there is no international law or treaty which has been accepted universally by all nation states. Every country has its own cyber law which is the final law of the land and supersedes laws of other nation states. There are bilateral and multilateral treaties which exist between two or more countries and are the only way the cyber related issues are being resolved. Budapest Convention and Tallinn Manual are two such positive attempts in this direction but they do not deal with cyber warfare.

NATO and US have concluded that International Humanitarian law applies to cyber law and nation states have a right to use kinetic force in the event of cyber war. But the most important thing is that cyber space sovereignty is what withholds all nations from enacting an agreeable cyber space treaty [1].

Budapest Convention (Convention on Cyber Crime)

This is the first international treaty related to internet and computer crimes which was signed on 23 November 2001 and is effective since 01 July 2004. At present there are 55 parties and 56 signatories(52 states have ratified the convention) to this treaty [2]. The signatories to this can share intelligence which assist in cyber-criminal investigations. Many influential countries which include India (Russia and Brazil too) have refused to sign the convention because of different reasons one of which supremacy of a few in amending and alteration of the rules of the convention.

Budapest Convention is addressing issues only related to cybercrime and nothing more. It does not address if a nation state is involved in a cyber war or cyber espionage kind of scenario. Cybercrimes such as IPR, frauds, sexual exploitation , etc. are important and the conventions main objective is to have mutually agreeable policy by adopting appropriate legislation and international cooperation.

Tallinn Manual

After the Russia-Estonia crisis in 2007, the North Atlantic Treaty Organization (NATO) understood the significance of global cyber warfare. NATO Cooperative Cyber Defence Centre of Excellence set up at Tallinn (in Estonia) started a process that led to the preparation of guidelines to address Laws of Armed Conflict (LOAC) that could be applicable in cyberspace. These guidelines however did not supersede the existing LOAC which are very much applicable**.** It took almost four years for Professor Michael Schmitt (alumni United States Naval War College and his team (20 experts from various fields) before the first version of the manual was published in 2013. Numerous experts were consulted in their individual capacity including lawyers, academicians and technical experts who were the best in their field. The Tallinn Manual is considered as the first step towards illuminating the global law pertaining to cyber-attacks.

The Tallinn Manual is not a NATO directive. It clearly mentioned "Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence"[3]. The conclusions of the manual are the opinions of the authors/experts in their personal capacities, and not a statement of official policy by NATO, any of its member governments, or any other participating organization[4]. The inferences drawn are based on historical wars while cyber war is a continuous state of affair and going forward. The rules of engagement and interest of nation states in cyber war is different. Tallinn Manual falls short on illustrations and experience to articulate any laws to govern the cyber space.

Other Treaties

Bilateral treaty on data sharing between USA and UK exists but till

date we have not heard any success stories. China and Russia have crafted their own world cyber space treaty which the western world doesn't pay attention to. There are few more bilateral treaties signed between nation states but when it comes to execution there is a big question mark.

Role of International Community

- Data is the everything. Call it oil or gold mine. In cyberspace data should be the basis of sovereignty and the International community should consider it in a similar manner.
- Your goal should be my goal when it comes to protection of data in cyberspace. All nation states should come on the table and work towards understanding the concept of sovereignty, deterrence and attribution in cyber space so as to stop malicious actors from committing crimes which may lead to cyber war scenario.
- Legal complexities due to the complex characteristics of cyber space are posing a great challenge to all the countries around the globe. Now is the time when all should contribute in bringing to the table policy solutions that will help in dealing with the legal challenges presented by multiplicity of cyber security legislations covering various sectors.
- Digital trade needs to be addressed from legal perspective.
- Use of kinetic force in retaliation of a cyber-attack by nation state and the legal challenges posed by it is a worrying situation which needs to be addressed by the international community.
- Solutions should be a time bound manner and should not be left open ended as the challenges in cyber space are growing at a rapid pace.
- It is the responsibility of the international community to develop and introduce legislative frameworks and policies that can be used globally for sharing information in regard to violation of cyber sovereignty of any nation state and its jurisdictions.
- A clear regulatory roadmap has to be prepared by the international community by collaborating with each other to safeguard the Critical Information Infrastructure (CII) of all nation states.
- There is a need for defining and identifying rules on engagement for Cyber Operations being carried by nation states so that sovereignty of other states is protected.
- International coordination among nation states to analyze to address issues regarding cyber governance is the need of the hour. There is need to build trust and confidence in addition to building of cyber defences so that exchange on information takes place.
- Building of Safe and Secure cyberspace is a collective responsibility of the International community.

Recommendations to Indian Government

- Acknowledging itself as a growing superpower, India should spearhead and be a influencer in discussions related to cyber domain. Hence, it has the onus to present an integrated strategic view to the international community on cyber related issues.
- India should map important trends in cyber domain and cyber law with a perspective to collborating with different thinkers and global stakeholders, including the International Commission on Cyber Security Law, on principles of cyber security law jurisprudence and establishing minimum standards.
- India should generate more possibilities for governments, the private sector, civil society, the technical community and academia from different areas of the globe to participate in and develop creative and efficient legal frameworks to tackle the genuinely worldwide challenge.
- It is time for India to continue to be at the center of the evolving debate on cyber domain problems and associated legalities in the digital environment, as well as assisting global organizations toprepare, manage and forecast prospective occurrences in cyber space.
- India requires to work towards defining the legal and policy foundation for regulating cyber safety on the Internet of Things(IoT) at a worldwide level and working with numerous international stakeholders in this respect.
- We must contribute to global discussions on problems linked to the attribution of acts in

cyberspace. Contribute also to the global discussion on the evolution by state and non-state actors of behavioral norms in cyberspace.

- Working towards recognizing the legal difficulties presented by Darknet / Deepweb and helping to define prospective legal strategies for mounting efficient legal responses is another significant element.
- Legal issues related to blockchain technology can also be taken up at international level so that India as a responsible player is there from the word go. Issues related in its application such as cryptocurrencies and its legal fallout also needs to be discussed.
- The fundamental legal principles underlying cyber sovereignty should also be examined and worked on.
- We should call on thinkers from all over the globe to discuss, discuss and deliberate on the harmonization and regulation of Cyberlaw's legal framework. The aim should be to work towards a global harmonization of Cyberlaw principles by incorporating ethical values, virtues and balancing conflicting perceptions of value in all tools to enhance cyber legislation in line with global cooperation.
- As a accountable country, we should continue to work towards convergence of views on cyber-law, cyber-crime and cyber-security so that we can adapt to fast technological innovations and keep shaping our societies, making them more cyber-capable, cyber-conscious and cyber-safe. India should continue to identify and address the implications of cyberspace in capability development and at operational planning, especially regards to public awareness.
- India should cooperate with global stakeholders and collate global best practices on emerging cyber-domain jurisprudence and participate in separate discussions with stakeholders to assist in the collapse of prevalent universally accepted values.
- Conducting Global Cyberlaw, Cybercrime & Cyber Security Conferences and Workshops.

Indian Challenge

There is a surge of new National Cybersecurity legislations around the globe but there are numerous inconsistencies in them. An international legal framework integrating the varied features and nuances of the interconnected fields of Cyberlaw, Cybercrime and Cybersecurity needs to be established which shall promote the development of the Internet and technologies and also aid in the development and peace building amongst the world community. India a nation of younger population are the cyber warriors of the future and are ready to contribute in making the nation cyber safe. We need a policy to harness this untapped power and make concerted efforts to reward these unsung cyber warriors. Massive economy, young workforce, and technological developments have forced the world to look towards India as a lucrative marketplace for their finished products. With internet reaching remote places, digital gadgets in every household and booming e-Commerce industry India's present and future looks more promising and interconnected to the cyber mesh.

National cyber laws of all nation states are becoming an issue. Internet jurisdiction is the biggest problem as there are no fixed boundaries and the problem of attribution worsens it.Attempts to hold a rogue nation state accountable for its cyber intrusions is always met with denials and veiled threats [5].International Humanitarian Law could be used as a reference point for creating an acceptable global cyber law but it would only evolve when cases related to cyber war are argued and settled in Hague international Court. Some common points can be filtered out from Budapest Convention, Tallinn manual, International Space Treaty etc. and agreed upon to start with.

India may be an IT super power but it needs a long term strategic plan for governing cyber space with the help of civilian and defence establishments. It also has to take lead in getting other nation states to sit across the table and formulate common international cyber law or treaty which will help everyone and make the cyber space more secure.

Special Mention : Adv Pavan Duggal (Lawyer, Supreme Court of India) for his Inputs

References

- Cyber Warfare and International Cyber laws: An Interview with Advocate Prashant Mali published in Digital 4n6 Journal (Aug 2017).
- Wikipedia, the free Encyclopedia.
- Tallinn Manual – General Editor Micheal N. Schmitt

- Applying International Law to Cyber Warfare- a presentation by Jason Thelen, Associate Director of the Cyber Statecraft Initiative (Atlantic Council) at RSA Conference 2014.
- Cyber Warfare by Paul J. Springer
- A Review of International Legal Framework to Combat Cybercrime by Sandeep Mittal IPS and Prof. Priyanka Sharma. Research paper published in International Journal of Advanced Research in Computer Science (May-Jun 2017)
- The Intersection of Law and Ethics inCyberwar:Some Reflections byMajor General Charles J. Dunlap, Jr., USAF (Ret.)*.
- Cyberwarfare and International Law byNils Melzer
- Outcome document of International Conference on Cyberlaw, Cybercrime & Cybersecurity Organized by Cyberlaws.Net & Pavan Duggal Associates, Advocates, Supreme Court of India.

Santosh Khadsare is an Information security professional who specializes in Digital Forensics. He is a Scientist 'E' in CERT-In (Cyber Forensics), Ministry of Electronics and Information Technology (MeitY), (Government of India) and heading the Cyber Forensics Lab at CERT-In. The author is B.E (Electronics and Telecommunications) and possesses additional qualifications such as CHFI, CEH, RHCSA, Advance Cyber Forensic Course (CDAC), Cyber Crime Investigator, and Access Data Certified Professional. Santosh has 19+ years plus of rich experience in the field of Information Security, Digital Forensics, Cyber Audit, Cyber Laws and Incident Response. Speaker in various international conferences such as CII Conference on Cyber Security, CSI Conference, It-sa Conference on Cyber Security, International Conference on Cyber Law, Cybercrime & Cyber Security, C0C0N, HAKON, National Cyber Defense Summit and GovInfoSec Summit Asia. Authored various articles on information security and Digital Forensics in national and international publications Won the COMMUNITY STAR award at NULLCON International Cyber Security Conference 2017:

santoshkhadsare@gmail.com
https://www.linkedin.com/in/santosh-khadsare-3539a818/
@santkhad2