Do laws of war apply to Cyberspace?
Dr. Karnika Seth

1. Conventional Principles of Law of war apply in Cyberspace

The 1899 and 1907 Hague Conventions created the primary body of the law of the War (with its foundations in the Oxford 1880 "Manual of Laws and Customs of War") and India is a signatory thereto. The key principles prescribed therein include principles of '*distinction*', '*military nece*ssity', '*proportionality*', and '*unnecessary suffering'*. These principles which apply to use of conventional weapons in armed conflicts also apply with equal force to cyber attacks. The ICJ has invoked "*the Martens Clause*", as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons.[1] Drawing an analogy therefrom, in the absence of explicit norms, the Martens Clause serves as a guide to assess the limits of freedom of action in domain of cyber attacks. The clause provides that -*"in cases not included in the [Hague] Regulations …. populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilised nations, from the laws of humanity and the requirements of the public*."

In November 2009, the International Committee of the Red Cross (ICRC) organised the conference "60 Years of the Geneva Conventions and the Decades Ahead" in Geneva, Switzerland. One of the issues under discussion in said conference was cyber attacks wherein the majority view was that the Geneva Convention, 1949 and its additional protocols and Hague Conventions provide guidance on these matters. Moreover, as per the *Tallinn Manual* in the cyberwarfare/cyber operations arena, the Tallinn Experts unanimously agreed *Jus ad bellum* (international law governing resort to force by a state as instrument of its national policy) and *Jus in bello* (International humanitarian law) apply to cyber operations[2]. Cyber attacks could be aimed at accessing a protected system of another country, collect, copy, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes or data controlled by the hacked computer system. As critical infrastructure of another country may be automating its industries such as power, telecom, or other industries, air traffic control systems, nuclear power plants, bridges, it can lead to serious physical harm or destruction aswell.

2. Cyber attacks v cyber attacks with violent consequences of damage to persons or property.

[1] Nuclear weapons, para 84
[2] Tallinn Manual, page 19

It is important to note that there is a pertinent different where a cyber attack can be said to cause disturbance or inconvenience as opposed to cause violent consequences such as tangible physical damage to persons and property.

The Geneva Conventions of 1949 and especially the Additional Protocol I of 1977 (AP I) defines violence through attacks as '*attacks are acts of violence against the adversary in offence or defence'*.[3] On one hand, cyber-attacks can cause damage to property or persons just as kinetic weapons, on the other hand , cyber-attacks such as cyber espionage, or disruption of a military or commercial intranet, downloading personal or other financial information, denial of access to internet may not produce direct tangible results as damage to persons or property. Thus, such cyberattacks may not necessarily have violent consequences and would not be covered in terms of Article 49(1) of Additional Protocol I. In cases where a critical information infrastructure of a country is attacked through cyber operations, Laws of Armed conflict could trigger application if it is foreseeable that it will bring physical damage to persons and property. When targeting dual-use systems, such as airports, railways, all Laws of Armed Conflict (LOAC) norms and principles regarding the conduct of hostilities such as distinction, proportionality are applicable.

The U.S already has a Strategy for operating in Cyberspace which designates cyberspace as an operational domain.[4]Similarly, India's *National Cyber security,* interalia, provides strategies to strengthen cybersecurity in India building National and Sectoral 24x7 information gathering & incident response mechanisms, crisis management through effective 'predictive, preventive, protective response and recovery actions'[5] and strategies to enhance the protection and resilience of the National Critical Information Infrastructure.

On the lines of the Hague Convention and in consonance with the UN charter, even as per Tallinn Manual , launching a cyber-attack against civilians is unlawful.[6] If cyber operations are intended to coerce a government (and not otherwise permitted by International law), it may amount to a prohibited intervention[7] or a prohibited use of Force (rules 10,12 of Tallinn Manual).A cyber-attack that qualifies as an armed attack brings with it right of self defense under Rule 13 of the Tallinn Manual. An armed attack is said to have occurred against a state when there is death, injury, damage or destruction, for example if a critical information such as power grid of a country is massively impaired or attacked. Article 51 of the UN Charter gives states the right to respond in self-defense to an "armed attack", until the time the Security Council takes steps to intervene. The right to use *interventionary*, pre-emptive armed force in the face of an imminent attack has not been ruled out by the ICJ.

[3] Additional Protocol I, Article 49(1).
[4] Department of Defense, Strategy for operating in Cyberspace (2011)
[5] National Cyber security Policy,2013 (India).
[6] Tallinn Manual, Rule 32, 37.
[7] UN Charter Art.2(1)

Actions which are not an armed attack but constitute a violation of International law gives right to adopt countermeasures.(Rule 9). Where an action is mandated or authorised by the Security Council, including a cyber operation it is not violation of target state's sovereignty (Rule 18). The fact that internet is borderless does not mean a state has waived its sovereignty over internet. States can therefore exercise jurisdiction vis a vis cybercrimes and cyber activities pursuant to base of jurisdiction recognised in international law. To this end, the Indian IT Act,2000 , Section 1(2) , prescribes, that the Act applies to India and also to any offence or contravention thereunder committed outside by any person. Section 75 of the IT Act,2000 states that the Act applies to any offence or contravention committed outside India by any person irrespective of his nationality. Section 75(2) further clarifies that the Act applies to an offence or contravention committed outside India by any person if the act or conduct constituting the contravention or offence involves a computer, computer system or computer network located in India.

As per Rule 5 of Tallinn Manual ,incase a cyber-attack is launched from a State's cyber infrastructure on a target state, target state may be entitled to exercising countermeasures including use of cyber countermeasures (rule 9) or use of force in self defense in case of armed conflict (rule 13).There is no consensus on matter of attribution of liability of a state where a state only had constructive knowledge (as opposed to actual knowledge) of a malware that infected its systems leading to attack on another state. Moreover countermeasures should be proportionate[8] and are only to effect compliance with international laws and ought not to employ threat or force (Rule 11) , and should not be an armed attack (Rule 13) unless the cyber-attack escalates in degree of harm to an armed conflict where the right of self defense triggers .

3. Private persons assisting armed forces

When a private entity is engaged by a government of a state to conduct cyber operations, law of state responsibility is attracted as it exercises governmental authority[9].This situation is different from patriotic hackers who engage in such activities on personal level without any government direction. As per rule 7 &8, if a cyber attack originates / is routed from a state cyber infrastructure it is indication of association of act with State but not sufficient evidence .[10]Incase a state was used as a transit state, for a cyber attack, the transit state must however prove that it took reasonable measures to prevent such attack on its systems.Incase exact nature and origin of a cyber incident is not clear, certain protective measures are justified on ground of necessity. [11]

Further,the International Court of Justice has stated Article 2(4) (rule 10-12) and 51(Rule 13-17) of the UN Charter regarding prohibition of use of force and self defense respectively apply to "any use of force, regardless of the weapons employed[12]" and therefore would include cyber weapons/attacks.

4. Cyber espionage is a cyber attack equal to use of force?

[8] Naulilaa Arbitration Award ,pg 1028
[9] Page 37 of Tallinn Manual
[10] Page 39 of Tallinn Manual
[11] Page 43 para 12 , Tallinn manual
[12] Nuclear weapons advisory opinion para 39

Cyber operations are generally deployed in an espionage capacity which is not in contravention to the above said principles of distinction, proportionality and by virtue of Rule 30 of the Tallinn Manual do not constitute an attack. Not all cyber interference is prohibited automatically or violates international law prohibition on intervention. Intervention is illegal when it uses coercion[13]. Examples of intervention and use of force is Stuxnet. Intervention is wrongful if it involves coercion[14]. According to the Tallinn Manual-

"It follows that Cyber espionage and cyber exploitation operation lacking a coercive element donot per se violate non intervention principle.Mere intrusion into another State's systems does not violate the non intervention principle. In view of the international Group of experts , this holds true even where such intrusion requires the breaching of protective virtual barriers(e.g breaching of firewalls or the cracking of passwords)."[15]

However, it is pertinent to note Coercive Political interference such as influencing elections/fake news through cyber means is prohibited intervention being inconsistent with purposes of UN as per rule 10. However, Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks.

The severity of attack, physical harm to persons and property qualify attack as use of force, its invasiveness, immediateness being other criteria. Use of force is defined under Article 2(4) of the UN Charter. The use of force or threat of force is understood to mean the physical effects the act shall have physical damage or corresponding negative physical effects is the determining factor for the applicability of this article. If degree of loss to persons and property is more , it is an armed attack. Exercise of right of self defense is subject to requirement of necessity, proportionality, imminence and immediacy[16].There should be a reasonable determination that an armed attack is about to occur or has occurred prior to acts of self-defense. When the self-defense right is exercised an immediate report must be sent to UN Security Council. (Rule 17). The Tallinn Manual- Although a soft code, it gives some guidance on interpreting legalities of cyber warfare.

The Manual defines an international armed conflict as –

"An international armed conflict exists whenever there are hostilities which may include or be limited to cyber operations, occurring between two or more state"[17].

It may be noted herein Espionage per se is not illegal (rule 66). Intrusion by military may be per se regarded as use of force. Whether a cyber operation becomes an armed attack depends on its scale and effects. All states that develop cyber weapons ought to ensure these comply with law of armed conflict

[13] Tallinn Manual page 45 para 8,9,10
[14] Nicargua judgemnet, para 205
[15] Tallinn manual , page 47 para 8
[16] Rule 14,15 of Tallinn manual
[17] Tallinn Manual , pg .71

applicable to the state.(Rule 48). Attacks in international armed conflict in Russia and Georgia in 2008 are armed conflict.

5. Attribution of liability & Bot attacks

Under article 49 (1) of Additional Protocol I, "attacks" means acts of violence against the adversary, whether in offence or in defence. The term "acts of violence" denotes physical force. Based on that interpretation, which the ICRC shares, cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as "acts of violence", i.e. as an attack from perspective of IHL.

A detailed legal analysis needs to be made as regards attribution of liability and an attack in cyberspace. Many bot attacks arise from infected computers and owners of such computers may be unaware that their systems have been infected . Incase a state was used as a transit state, for a cyber attack, the transit state must prove that it took reasonable measures to prevent such attack on its systems. Incase exact nature and origin of a cyber incident is not clear, certain protective measures are justified as a countermeasure on ground of necessity. [18]

6. Other relevant laws/ documents require consideration in India/abroad

For the purposes of the study, besides the law of armed conflict, India's national cybersecurity policy, bilateral agreements with other countries, Mutual legal assistance treaties will need to be studied and MOU signed by India with other countries on issues of cybersecurity will also be relevant . This will clarify India's legal prowess, policy direction and capabilities to effect cyberwar operations as part of attack or self defense. The study of Multilateral and bilateral treaty arrangements /MOU on cybersecurity will also throw light on India's position to receive international cooperation from law enforcement authorities abroad .

For formulation of an effective cyber action strategy, additional laws applicable in domestic jurisdiction of India will be relevant as both in case of a cyber attack or self defense certain civil organisations and personnel may get affected directly affecting their personal rights to data or privacy or otherwise. Statutes such as Information Technology Act,2000, particularly,(Section 66F- prohibiting Cyberterrorism), Section 69A (empowering Central Government to block websites), Section 69B (empowering Central Government to intercept & monitor Internet Traffic data) , Section 70 (Protected system),Section 70 A (National nodal agency), Section 70-B (CERT to serve as national agency for incident response) together with Section 5 of the Indian Telegraph Act,1885 (Power for Government to take possession of licensed telegraphs and to order interception of messages) and Rule 419-A of Indian Telegraph (Amendment) Rules will require important consideration. Also, the procedure and safeguards for interception have been prescribed / notified vide the Information Technology (Procedure and Safeguards for interception, Monitoring and Decryption of Information) Rules, 2009 will define legally prescribed methods of interception within India.

[18] Page 43 para 12 , Tallinn manual

The IT Act,2000 also contemplates the National Critical Information Infrastructure Protection Centre, which was established by a Gazette of India notification on January 16, 2014. The NCIIPC Rules under the IT Act lay down the manner in which the NCIIPC should perform its functions. As per the NCIIPC charter, its function is to "take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders." The Guidelines recognise national security, economy, public health and safety, as the key considerations in assessing whether the object of protection is critical. Currently, the following sectors have been identified as CII - banking and financial sector; ICT and telecommunication; transportation; power; energy; the Ministries of Home Affairs, External Affairs and Heavy Industries; and Niti Ayog. While devising a cyber security strategy for India the role of Indian CERT and NCIIPC , Nodal offices, and its intelligence gathering and incident response capabilities ought to be aligned with agencies such as NTRO, and other such bodies for an effective and coordinated action.

For analysing effects of cyber espionage/surveillance conducted in other countries, legal frameworks of relevant target countries will be required to be analysed to study implications of possible violation of its laws prior to any cyber operations such as the *General Data Protection Directive* in the European Union.

Pronouncements of Landmark judgements on surveillance, ***PUCL v UOI*** (1997) 1 SCC 301 and the recent ***K.S Puttaswamy*** judgement declaring Right to privacy as the fundamental right of citizens of India, and the *Personal Data Protection Bill* will be relevant for detailed analysis