Himachal Pradesh National Law University, Shimla (India)

Journal Articles *ISSN:2582-1903* *Shimla Law Review*

.

Volume-IV (2021)

EMERGING NORMS OF INTERNATIONAL LAW AND CYBER-WARFARE: A Critical Analysis

Veer Mayank & Nidhi Saxena

This article can be downloaded from: http://www.hpnlu.ac.in/journal-level-3.aspx?ref-id=18.

Recommended Citation:
Veer Mayank & Nidhi Saxena, *EMERGING NORMS OF INTERNATIONAL LAW AND CYBER-WARFARE: A Critical Analysis* IV SML. L. REV. 130 (2021).

This Article is published and brought to you for free and open access by Himachal Pradesh National Law University, Shimla. For more information, please contact editorslr@hpnlu.ac.in

Contents

Volume IV | *ISSN: 2582-1903* | April 2020 - March 2021

Special Article *Page*

1. GENEALOGICAL AND ANALYTICAL CRITIQUE OF THE NATIONAL EDUCATION POLICY, 2020: The Rich Heritage of Indian Knowledge, Social Traditions, and the Problem of Social Order
   Chanchal Kumar Singh & Mritunjay Kumar 1

Articles

2. RECHTSTAAT OF POPULIST AUTHORITARIANISM: Paradoxes of the Constitution in Authoritarian Regimes
   Niraj Kumar 41
3. THE IMPERATIVE OF EMPRICAL RESEARCH METHODOLOGY IN LEGISLATIVE DRAFTING AND CONDUCT OF RESEARCH IN LAW
   Tonye Clinton Jaja & Chukwuka Onyeaku 59
4. EXORCISING THE COLONIAL GHOST IN CLASSROOMS: Contextualising Teaching of International Law in the Geographical South
   Manwendra K. Tiwari & Swati Singh Parmar 77
5. DIGITAL MARKET, DATA ANALYSIS AND THE SUBSEQUENT: Competition Law Challenges in Cyberspace in India
   Anand Pawar 97
6. CONSTITUTIONAL MORALITY IN INDIA: A Brief Analysis & Contextualising its (De)Limitations
   Vibhuti Jaswal & Aayush Raj 113
7. EMERGING NORMS OF INTERNATIONAL LAW AND CYBER-WARFARE: A Critical Analysis
   Veer Mayank & Nidhi Saxena 130

8. A STUDY OF THE LEGAL PROTECTION OF TRADITIONAL INDIGENOUS KNOWLEDGE OF NORTHEAST INDIA: A Legal Approach
Partha Sarothi Rakshit, Karobi Dihingia & Soumyadeep Chakraborti 152

9. THEORISING THE EFFECT OF STIGMATISATION ON THE CRIMINAL JUSTICE SYSTEM: Normalizing Prison Sentences
Mehreen Manzoor 170

10. COMBATING SEXUAL VIOLENCE AGAINST WOMEN WITH DISABILITIES IN INDIA: A Brief Conspectus of the Legal Framework
Monica Chaudhary 189

11. POLITICAL TERRORISM & POLITICAL CRIME VIS-À-VIS CRIMINALIZATION OF POLITICS: A Critical Analysis of the Efforts of Indian Judiciary in Preserving the Democratic Values
M.R. Sreenivasa Murthy & K. Syamala 217

Notes and Comments

12. TEXT, CONTEXT, AND HUMAN RIGHTS-BASED INTERPRETATIONS BY DOMESTIC COURTS
Deepa Kansra & Rabindra Kr Pathak 241

13. SURROGATE MOTHERHOOD IN INDIA: An Analysis of Surrogacy (Regulation) Act, 2021
Paramjit S. Jaswal & Jasdeep Kaur 257

14. THE CONTROVERSY SURROUNDING THE PLACES OF WORSHIP ACT, 1991: Challenges against Democracy, Secularism, and the Cherished Principles of Constitution
Shreshth Srivastava & Vaishali Gaurha 269

EMERGING NORMS OF INTERNATIONAL LAW AND CYBER-WARFARE: A Critical Analysis

Veer Mayank & Nidhi Saxena[*]

[***Abstract***: *Wars have been fought between contesting parties since the dawn of human society. In all ages technological advancements have been utilized by opposing parties to gain advantage over the opponents in the battlefield. Congruously, the laws of war also evolved to ensure that the harm caused due to wars did not become unlimited and did not extend to the general population of the country. Thus, in India, in the ancient period, the laws of war evolved to ensure that unarmed opponents would not be attacked, and wars shall not be fought at night. The laws of war were there to ensure that the objective of wars did not become a complete annihilation of a people or population. The laws of war have been shaped throughout history to regulate the use of kinetic weapons since in battle violent damage can be caused due to kinetic weapons. Cyber events and tools have however removed the distinction between the use of kinetic weapons and non-kinetic weapons for causing violent damage. In fact, cyber tools can cause greater damage to an opponent than whatever a kinetic weapon can, and such damage can be continuously extending in time and space. It is important in such a situation to study how the laws of warfare are poised to regulate the use of cyber tools in cyber warfare. To study the above topic, the chapter has been divided into four sections. Section one provides introduction to cyber warfare as the fifth domain of war; section two deals with the application of international law to acts of war; section three deals with present international law in the context of cyber-warfare; section IV studies the development of rules for providing cyber security while section V concludes.*]

Keywords: *War, technology, international law, cyber warfare, cyber security.*

I

Introduction

Cyber-Warfare: The Fifth Domain of War

Cyber-space as a domain of warfare is unique and different from other domains in that it is entirely man-made and there is a sense of immediacy in the transmission

[*] Dr. Veer Mayank & Dr. Nidhi Saxena are Assistant Professors of Law at the Department of Law, Sikkim University, Gangtok, Sikkim. India. *Email: veer.mayank@gmail.com; nidhisaxena.law.30@gmail.com*

of data or information from the point of origin and receipt of data at the point of reception. This aspect of immediacy renders the existence of boundaries – whether political or natural – immaterial in the context of cyber-warfare making the warfare unique in comparison to warfare in other domains.[1] International law and international relations are based upon the bedrock of sovereignty and the inviolability of political boundaries of the state, within which the state is supreme. Cyberspace challenges these very fundamental bedrocks of international law since the concept of political boundaries is alien to the concept of cyberspace.

There have been several instances of cyber intrusion into the cyber domain of institutions and facilities of a nation which have resulted in serious economic and political consequences. Such intrusions have been in the security apparatus of a nation such as the cyber-attack on the centrifuges in the nuclear power plant in Iran.[2] Scholars studying the literature on cyber-interference have been quick to call cyber intrusions as cyber-attacks providing to it a military terminology, though in the absence of kinetic damage to the targeted country's facilities the nomenclature of attack to cyber intrusions appears overstretched. This aspect therefore begs the question – whether such cyber – intrusion is in fact a cyber-attack looking at it from the cold war terminology or it is merely a cyber-intrusion having economic, political and infrastructural consequences, albeit extremely serious. The events cited below highlight this conundrum.

1. Estonia and NATO 2007 – Estonia suffered a distributed denial of service (DDOS) attack and a redirection of the website to the images of Russian soldiers, presumably in response to the relocation of the Soviet War Memorial. This particular cyber-interference was titled as cyber-attack with a call to invoke the collective security provision under Article 5 of the NATO alliance.[3]
2. Russian – Georgian Conflict 2008 – In the conventional conflict between Russia and Georgia, Georgia claimed that it was a victim of cyber-attack from Russia through the distributed DDOS attacks.[4]
3. Stuxnet 2009 – Stuxnet is said to be the first known worm to target real world infrastructure such as power stations, water plants and industrial

---

[1] *See generally,* Erez Kalir & Elliot E. Maxwell, RETHINKING BOUNDARIES IN CYBERSPACE: A REPORT OF THE ASPEN INSTITUTE INTERNET POLICY PROJECT (The Aspen Institute: Communication and Society Program) (2002).

[2] D. E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, (NEW YORK TIMES 01 Jun., 2012), *available at:* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (last visited, Oct. 15, 2021).

[3] M. Landler & J. Markoff, *Digital Fears Emerge After Data Siege in Estonia*, NEW YORK TIMES (May 29, 2007), *available at:* http://www.nytimes.com/2007/05/29/technology/29estonia.html (last visited, Oct. 15, 2021).

[4] J. Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES (Aug. 12, 2008), *available at:* http://nytimes.com/2008/08/13/technology/13cyber.html (last visited, Oct. 15, 2021)

units.[5] It destroyed the centrifuges used for Iran's nuclear enrichment program and was alleged to be the handiwork of US and Israel.[6] The complexity of the attack pointed towards its being sponsored by a nation state.[7]

4. Shamoon attack of 2012[8] - In the case of the Shamoon attack, data was wiped out from 35000 computers belonging to Saudi Aramco. It also compromised the computers of Qatari gas company RasGas. The US intelligence agencies attributed the attack on Saudi Aramco to Iran and could be regarded as an incidence of cyber-attack where a critical structure of the State was compromised.
5. Cyber-attack on the Turkey Electrical Grid, 2015 – the purported cyber-attack from Iran on Turkey's electrical grid shut down the grid for almost 12 hours and which stopped everything that was working on electricity – hospitals, fire services, airports etc., resulting in catastrophic consequences.[9]
6. Attack on Information Technology Firm 'Solar Winds' – In this case, malicious code was inserted in the software 'Orion' provided by the firm 'Solar Winds'. This software system 'Orion' was used by a large number of Fortune 500 companies and several US agencies to manage their IT resources and since the system was compromised, so did the security of the companies that relied on Orion. The impact of the breach is expected to be extremely massive and may take years before coming to light.[10]
7. Cyber-attack on US gas pipeline – US suffered a ransomware attack on the US fuel pipeline operator 'Colonial Pipeline'.[11] Attacks on energy and

---

[5] J. Fildes, *Stuxnet worm 'targeted high-value Iranian assets'*, (BBC News, 2010), *available at:* http://www.bbc.co.uk/news/technology-11388018 (last visited, Oct. 15, 2021).

[6] *Supra* note 2.

[7] US Department of Defense, *U.S. Cyber Command Fact Sheet*, 2010 *available at:* http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (last visited, Oct. 15, 2021).

[8] Council on Foreign Relations, *Compromise of Saudi Aramco and RasGas* (2012) *available at:* https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas (last visited, Oct. 15, 2021).

[9] Micah Halpern, *Iran Flexes Its Power by Transporting Turkey to the Stone Age*, OBSERVER (2015), *available at:* https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/ (last visited, Oct. 15, 2021).

[10] I. Jibilian, *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*, BUSINESS INSIDER INDIA (Apr. 15, 2021, 23:26 IST), *available at:* https://www.businessinsider.in/tech/news/heres-a-simple-explanation-of-how-the-massive-solarwinds-hack-happened-and-why-its-such-a-big-deal/articleshow/79945993.cms (last visited, Oct. 15, 2021).

[11] Christopher Bing & Stephanie Kelly, *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed*, REUTERS (2021), *available at:* https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (last visited, Oct. 15, 2021).

critical infrastructure of a country can cause greater damage than a regular kinetic attack that has a much lower probability of being successful in view of the defences present against it.

8. Cyber-attack on Microsoft Exchange Servers – Microsoft Exchange Servers were targeted and that affected a large number of organizations globally.[12] This attack has the potential of engaging in large scale espionage and theft of intellectual property and personal information. These attacks have been blamed on China by western intelligence agencies.
9. Cyber-attack by Chinese Defence Facilities – Chinese authorities have accused without providing any evidence that India backed groups have attacked Chinese Defence Facilities.[13]
10. Attack on Iranian Gas Stations - Cyber-attack was launched against Iranian gas stations that sell subsidized fuel.[14]

There have been other events such as Taiwan accusing that it faces 5 million cyber-attacks daily whereas India and China, both accusing each other of launching cyber-attacks. Nations are investing heavily in protection of cyberspace and development of offensive capabilities in cyber space from a military point of view and which has been stretched to the extent that the protection from cyber-attacks requires launching cyber-attacks to degrade the offensive capability of the hostile state before it launches an attack.

The events cited above can either be characterised as merely an intrusion exploiting a security loophole in the service, or the cyber-element targeted, or it may be characterised as an act of warfare depending upon the gravity of the cyber incident, making it difficult to draw an objective distinction between cyber-attack (warfare) and a mere cybercrime or cyber-intrusion. An act which may have been initially determined to be of cyber intrusion can easily metamorphose itself into an act of cyber-attack if the consequences of such an intrusion result in grave consequences such as shutting down of the nuclear reactor, scrambling the financial records or incapacitating the stock markets, opening of a dam, or blackening out of air traffic control system.

---

[12] Gordon Corera, *China accused of cyber-attack on Microsoft Exchange servers*, BBC NEWS (2021), *available at:* https://www.bbc.com/news/world-asia-china-57889981 (last visited, Oct. 15, 2021).

[13] Sakshi Tiwari, *'Evil Flower': Chinese Media Goes Ballistic Over Alleged Cyber Warfare By 'Indian Govt-Backed Group' On Defense Facilities*, THE EURASIAN TIMES (2021), *available at:* https://eurasiantimes.com/evil-flower-chinese-media-goes-ballistic-over-alleged-cyber-warfare-by-indian-govt-backed-group-on-defense-facilities/ (last visited, Oct. 15, 2021).

[14] Alicia Hope, *Iran Suffered A Cyber Attack Shutting Down Smart Gas Stations With Hacked Electronic Signs Allegedly Mocking The Supreme Leader*, CPO MAGAZINE (2021), *available at:* https://www.cpomagazine.com/cyber-security/iran-suffered-a-cyber-attack-shutting-down-smart-gas-stations-with-hacked-electronic-signs-allegedly-mocking-the-supreme-leader/ (last visited, Oct. 15, 2021).

Such being the nature of cyber-attack, it is necessary to strictly determine the contours of a cyber event which may require it to be classified as cyber-attack. Richard A. Clarke defines cyber war as 'actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption'.[15] Michael Hayden understands cyber-war as the 'deliberate attempt to disable or destroy another country's computer networks'.[16] The first official military definition of cyber-attack defines cyber-attack as 'A hostile act using computer or related networks or systems and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions'.[17] This definition while acceptable is cryptic and more of an understatement. A cyber-attack does not necessarily limit its effect on the targeted system, or the data contained in the system – it can and does targets systems beyond the targeted computer or device. In addition, it utilizes not just the information channels for reaching its targets. A cyber-attack can be launched through a malicious code embedded in the most ordinary of devices such as thumb drive and the careless of human operator. Further, the effects of an attack need not to be immediate or even in the immediate vicinity. The attack and the consequences can be separated by time and space. Thus, it appears from the foregoing that cyber-attack is an aggravated form of cyber-intrusion and is chiefly distinguishable from the latter only from the amount of destruction or damage it causes or is intended to cause, and this obviously leads us to the question as to what is the legal framework that governs cyber warfare.

II

Applicability of International Law to Acts of War

Laws regulating warfare have been in existence since historic times. The purpose of such rules and regulations has been the preservation of the civilized world and recognize that in certain circumstances where war may be necessary, rules have to be followed to prevent infliction of unlimited suffering on the belligerents.[18] Article

---

[15] Richard Clarke & Robert Knake, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2012).

[16] T. Gjelten, *Extending the Law of War to Cyberspace* (2010), *available at:* https://www.globalpolicy.org/home/163-general/49941-extending-the-law-of-war-to-cyberspace.html. (last visited, Oct. 28, 2022).

[17] J. E. Cartwright, *Memorandum for the Chiefs of Military Services Commanders of Combatant Commands Directors of Joint Staff Directorates: Joint Terminology for Cyberspace Operations.* (The Vice-Chairmen of the Joint Chiefs of Staff 2010).

[18] CreateSpace Independent Publishing Platform, DEPARTMENT OF THE ARMY, THE LAW OF LAND WARFARE (FM 27-10) (2017).

22[19] of the Hague Convention provides 'the right of belligerents to adopt means of injuring the enemy is not unlimited, and this rule does not lose its binding force in a case of necessity'. In the context of the rules and laws regulating the conduct of war it is necessary to evaluate to what extent the rules and laws of warfare are applicable to cyber warfare.

Customary Laws for Regulation of Warfare

The laws and rules that regulate war are codified in the Geneva Conventions of 1949, the Additional Protocol of 1977 and Hague Conventions.[20] These rules deal with the means and weapons that could be employed for waging war and the rules of conduct of war with respect to the security of persons both civilians and military. They also deal with the protection of property.

The application of the laws for regulation of warfare can be studied under two heads – *jus ad bellum* and *jus in bello*. Application of law of war to actions or events that can be categorised as acts of war are categorised under *Jus ad bellum*. *Jus in bello* means the applicable law when the war is actually in progress and proscribes acts that are unjustified and impermissible during the progress of war. Geneva Conventions[21] are the treaties that regulate the conduct of war and while arguably they have been successful in their objective as they have achieved nearly universal adoption, they have not yet been invoked with respect to cases which involve cyber conflict. These two conventions suffer from the drawback that they were framed when the concept of cyber-conflict was something that could not even have been imagined, much less thought to be regulated. These conventions hence lack any provisions or understanding as to how such cyber-conflicts have to be regulated. Similar is the position with the Hague Conventions[22] that have enumerated the laws of warfare. However, though both Geneva and Hague conventions are silent on the aspect of cyber-warfare, it does not lead to the conclusion that the laws of war cannot be used to regulate new and novel weapons. Laws of war have been successfully applied to regulating several new weapon systems like biological weapons, laser weapons,

---

[19] International Peace Conference, The Hague conventions of 1899 (II) and 1907 (IV) respecting the laws and customs of war on land (1915).

[20] Christopher Greenwood, *Historical Development and Legal Basis in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW (Dieter Fleck ed., 2008).

[21] Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (Second Geneva Convention) 75 UNTS 85 (Aug. 12 1949); Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Third Geneva Convention) 75 UNTS 31 (Aug. 12 1949); Geneva Convention Relative to Treatment of Prisoners of War (Third Geneva Convention) 75 UNTS 135 (Aug. 12, 1949); Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) 75 UNTS 28 (Aug. 12, 1949); International Peace Conference, 1915.

[22] International Peace Conference, 1915.

etc.[23] Where the laws of war are silent on an aspect, as in the case of the use of 'nuclear weapons', the device of rule interpretation is resorted to as in the case of advisory opinion of the International Court of Justice on 'Legality of the Threat or Use of Nuclear Weapons'[24] in which the court ruled that the threat or use of nuclear weapons is illegal. There is the presence of other authorities that support the view that the 'laws of war' provided through various conventions and treaties are designed to be applicable to future weapons and weapon systems that may emerge in the course of time. The St. Petersburg declaration of 1868 provided for the following:[25]

> 'The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which, they have established, and to conciliate the necessities of war with the laws of humanity'.

Similar provision was incorporated in 1899 Hague Convention (II),[26] Geneva Convention of 1949 and the Additional Protocols of 1977 which later came to be known as Marten's clause which reads as:[27]

> 'Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience'.

Further Article 36 of the Additional Protocol-I provides:[28]

> 'Development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party'.

---

[23] J. Doge, *Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime*, 48 ARCHIV DES VOLKERRECHT, MOHR SIEBECK GMBH & CO. KG 486 (2010).

[24] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, 105 (2) (E). (Jul 8).

[25] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight 138 Consol. T. S 297 (Dec. 11, 1868).

[26] International Peace Conference, 1915.

[27] The Clause was named after a declaration read by Professor von Martens, the Russian delegate at the Hague Peace Conferences 1899; Doge, ARCHIV DES VOLKERRECHT, MOHR SIEBECK GMBH & CO. KG 26 (2010).

[28] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1125 UNTS 3 (Jun. 8, 1977).

The United Nations Charter and Conduct of War

The foremost and arguably the most important treaty governing the regulation of the wars is the Charter of the United Nations and notably Articles 2(4) and Article 51 under the Charter. Article 2(4) of the U.N. Charter provides that the member states 'shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purpose of the United Nations'. Article 51 provides 'nothing in this present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs'. Another article of the Charter that deals with exceptions to article 2(4) is article 39 which provides for '[determination] of any threat to the peace, breach of peace, of acts of aggression and [to] make recommendations and to decide what measures shall be taken... to maintain and restore international peace and security'. Subsequent to the invocation of article 39, maintenance of peace can be ensured through 'measures not involving the use of armed force'[29] or through action by 'air, land and sea forces'.[30] The collective reading of the three articles provides the view that while article 2(4) provides for the norm of non-intervention in the internal affairs of a state, articles 51 and 39 provides for the recourse where such the norms of international law are violated. Article 51 provides for the individual and collective self-defence, whereas article 39 provides for action by the Security Council of the United Nations where international peace is threatened due to violation of the norm of non-intervention. The International Court of Justice in *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua* v. *U.S.*)[31] held the norm of non-intervention to be coterminous with article 2(4) when such non-intervention is on account of threat or use of force. The violation of the norm of non-intervention through the use of force has been sought to be extended to the use of political and economic coercion, however the overwhelming majority of the opinion is in the favour of use of armed forces as amounting the violation of the norm imposed by Article 2(4).

Other International Rules Regulating Conduct of War

Besides the (above) laws enshrined in the United Nations Charter, the Geneva and Hague conventions, other applicable rules are rules of necessity[32] and

---

[29] U.N. Charter, article 41.

[30] *Ibid.* at article 42.

[31] Military and Paramilitary Activities in and against Nicaragua (Nicar v. U.S.), Judgment, 1986 I.C.J. Rep. 14, at 288 (June 27).; The Secretary of State Daniel Webster's wrote –

> *It must be shown that admonition or remonstrance to the persons on board the Caroline was impracticable, or would have been unavailing ... but that there was a necessity, present and inevitable, for attacking her.*

[32] R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW 82 (1938).

proportionality[33] in the conduct of war. The principles of necessity and proportionality require that force must be used only as the last resort and should be used only to the extent necessary to counter the force being opposed and not more than that.[34]

The other two areas of international law norms that need to be followed are that of distinction and neutrality. Distinction requires that targeting in a war should be limited to combatants and care must be taken to avoid unnecessary injury to non-combatants[35] while the principle of neutrality dictates that the territory of the neutral state is inviolable and neutrality requires that the neutral state should not involve itself in the conflict and maintain impartiality.[36]

These bodies of law apply to the actual initiation and progress of the war, however in cases where belligerence may not be categorised as armed attack, different sets of laws are required to regulate such activities. One such body of law is the customary law principle of countermeasures. Countermeasures are defined as:

> 'Measures that would otherwise be contrary to the international obligations of an injured State vis-a-vis the responsible State, if they were not taken by the former in

---

[33] R.D. Sloane, *The Cost of Conflation: Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE JOURNAL OF INTERNATIONAL LAW 108 (2009).

[34] Protocol Additional to the Geneva Conventions (Aug. 12 1949) and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 UNTS 3 (Jun. 8 1977) article 51(5)(b); article 85(3)(b). Article 51(5)(b) states:

> '[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.

Art. 85(3)(b) of the same protocol provides:

> 'An indiscriminate attack, defined by excessive effect, is not to be confused with an attack that does not discriminate amongst civilian and military objectives, which is defined by objective, and is prohibited by article 85(3Xa)'.

[35] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1125 UNTS 3 (Jun. 8, 1977) articles 48, 51(2) and 52(2).

[36] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Third Geneva Convention); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (Second Geneva Convention); Geneva Convention Relative to Treatment of Prisoners of War (Third Geneva Convention); Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention); Protocol Additional to the Geneva Conventions (Aug. 12 1949) and relating to the Protection of Victims of International Armed Conflicts (Protocol I); Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Person in Case of War on Land, U.S.T.S. 540, 2 A.J.I.L. Supp. 117 (Jan. 26, 1910); Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War 3 Martens Nouveau Recueil (ser. 3) 713, 205 Consol. T.S. 395 (Jan. 26, 1910).

> response to an internationally wrongful act by the latter in order to procure cessation and reparation'.[37]

The countermeasures should be in nature of an act which forces the recalcitrant State to cease from its wrongful act. It therefore implies that once the offending act has ceased, the countermeasures should also cease.[38] The countermeasures cannot be such as to be in violation of the peremptory international law principles or the most important parts of international law such as the human rights etc.[39]

III

Regulation of Cyber-Warfare

The laws of war as detailed in the foregoing sections do not provide a *proper* remedy for the regulation of cyber–warfare since the laws have historically been used for the purpose of regulating kinetic attacks and cyber-warfare is an asymmetric warfare characterised chiefly by an absence of the kinetic element. The laws of war had the objective of making the war more humane and preventing wanton destruction of life and property that was not necessary for achieving a military objective. The laws of war to an extent were for the protection of the weak against the powerful. The equation in war was the stronger party carried out the most potent attacks and the population of the weaker country required protection. In the case of cyber-warfare, the costs of carrying out such cyber-attacks are extremely low compared to a traditional conflict and the stronger and developed states are more at risk of harm in a cyber-warfare since the systems in such developed nations have a greater dependency on computers and associated information networks. Secondly, the other attribute of cyber-attacks is the capability to hide the source of origin of the attack. In the case of traditional conflict, the attack is launched from the territory of a State and hence easily traceable. In the case of cyber-attacks, it is easy for a state to claim that rogue elements within the state launched the attack without the involvement of the state or its agencies thereby abdicating any international responsibility that may fall upon it due to such an act. However, in most of the cases of cyber-attacks such a clear line of attributability is hard to come by. The origin of a cyber-attack can be hidden by a variety of technical means and it is a long and arduous task to reach to the origin of the cyber-attack.

---

[37] G.A. Res. 56/83, Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/RES/56/83 (Jan. 28 2002).

[38] *Id.* at article 49.

[39] *Id.* at article 49.

Application of the Test of Necessity, Proportionality, Distinction and Neutrality to Cyber – Attacks

The concept of cyber-warfare also challenged the applicability of the principles of proportionality and necessity. It is difficult to apply the concepts of proportionality to cyber–warfare as it requires determination of the harm in the conventional sense of the term. Cyber-attacks on computer networks cast its effect beyond the immediately affected computer networks and in general may have a latent attribute which may be visible at a time far different from when such attack was launched. It could also have its effect on systems that are completely separate from the computer network under attack. In such cases the primary question that arises is what should be the qualifying magnitude of damage due to such a cyber-attack separated in time so as to require 'armed response' in the conventional sense. Subsequent to such a determination the principles of proportionality and necessity can be applied. The test of proportionality requires an evaluation, as explained by Gillard:

> 'An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, would be excessive in relation to the concrete and direct military advantage anticipated'.[40]

In the context of cyber-attacks, it becomes difficult to apply the above test as while the direct effects of the cyber–attack may be to merely temporarily disable a particular system which may have the same effect as destruction of the system through a kinetic attack with the attendant consequences. A cyber-attack may disable the telecommunications system of a region as would a kinetic attack but while in the case of the former, a kinetic response would likely be disproportionate, in the latter case, a kinetic attack may pass the test of proportionality. Additionally, the threat with a cyber-attack is not mere disablement. A cyberattack might lead to the attacked systems being turned against the targeted States' population with the result that both the *ex ante* proportionality analysis and 'in bello' proportionality analysis carries a large element of uncertainty. Cyber-attacks as compared to kinetic attacks change the whole arena of attacks and countermeasures. Since uncertainties are inherent by nature in cyber-attacks, as compared to kinetic attacks, it forces States to take decisions in the face of these uncertainties and mount an adequate response which may be disproportional.[41]

---

[40] E.C. Gillard, *Proportionality in the Conduct of Hostilities The Incidental Harm Side of the Assessment*, CHATHAM HOUSE (2018), *available at*: https://www.chathamhouse.org/sites/default/files/publications/research/2018-12-10-proportionality-conduct-hostilities-incidental-harm-gillard-final.pdf; Protocol Additional to the Geneva Conventions (Aug. 12 1949) and relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 51(5)(b).

[41] Doge, ARCHIV DES VOLKERRECHT, MOHR SIEBECK GMBH & CO. KG (2010).

In the case of cyber-attacks, it is difficult to distinguish between combatants, non-combatants and civilians associated the combat functions. Similarly, the enormous overlap between the infrastructure used for civilian telecommunications channels and those used for military channels has rendered the identification of military targets extremely difficult.[42] The principle of distinction requires that states should distinguish between civilian and military targets[43] and in a war only the targeting of military targets is legitimate, unless military necessity dictates targeting of civilian infrastructure. The dual use nature of cyberspace – implying that the same infrastructure is being used for military and civilian purposes while on one hand advances the military necessity, on the other hand it fails to meet the criteria of the distinction doctrine.

Further, the difficulty in identifying the source of cyber-attacks has made it difficult to apply the laws of neutrality as it is applied to conventional conflicts. The principal duty of a neutral nation in a conflict is that of abstention and impartiality while such a nation has the right of inviolability of its sovereignty. The belligerent thus also has the corresponding rights of such abstention and impartiality by the neutral State and the duty of not violating the sovereignty of the neutral state.[44] In the context of cyber-conflict scholars have taken two contrasting positions regarding the characteristics of neutrality with one side insisting that neutrality implies that the state has been unable or unwilling to prevent other parties from using the infrastructure of the state to launch the cyber-attack. The shield of neutrality is lifted the moment the state is itself complicit in the launching of cyber-attack, i.e., it has the knowledge that the state is being used in the launching of cyber-attack and takes no steps to prevent such a use.[45] The counter opinion which is more favourable to the neutral State is that States are not obliged to prevent others from using the communication facilities in the state; they are only obligated to prevent the building up of such facilities in the state by the belligerents.[46] The requirement of knowledge by the concerned State that the cyber-attack is being carried out from its territory is the condition precedent prior to disrobing the state of its protection of neutrality. This existence of this knowledge is however a complicated question, since the technological world of cyber-operations does not make itself readily available to the identification of the source and therefore the origin of such cyber-attack remains

---

[42] *See*, V. M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Place*, 51 NAVAL LAW REVIEW (2005).

[43] *See generally,* L. Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (M. N. Schmitt & B. T. O'Donnell eds., 2002).

[44] *See generally,* Doge, ARCHIV DES VOLKERRECHT, MOHR SIEBECK GMBH & CO. KG (2010).

[45] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, para 89 (Jul. 8).

[46] Doswald-Beck 2002.

hidden unless copious amounts of time and resources are invested into the investigation.[47]

Countermeasures

Countermeasures have been defined as:

> '…Measures that would otherwise be contrary to the international obligations of an injured State vis'-a-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'.[48]

In the light of the discussion in the above foregoing paragraphs, it is evident that it is not easy to categorize a cyber-incident as *jus ad bellum* invoking the right to self-defence and therefore in most of the cases, countermeasures would work as a viable option.

In the case of cyber-attacks, the option to deploy countermeasures consists of protective measures such as firewalls and counter-attacks that have the purpose of disabling the source of the attack. According to Doge, active defences can be considered a form of reciprocal countermeasure if the affected state ceases or responds in the same manner as the responsible state, that is, it disregards or disobeys the same or a similar obligation as the belligerent State was under a responsibility to obey.[49]

The purpose of countermeasures is to force the responsible actor to abide by other restrictions and undertake the responsibility that is imposed by international law. In the case where non-state actors launch cyber-attacks or where the cyber-attacks are launched with the active connivance of the State, the use of countermeasures may not be fully effective as it would have been in the case if a State is involved. Countermeasures can be effective only in cases where the attacked state finds the countermeasures costly. In cases where the state or origin of a cyber-attack is identifiable, the problem arises in identifying the target which if not a state actor could easily be mobile changing its position continuously making the targeting through the countermeasure of cyber-attack difficult. Lastly, countermeasures impose a responsibility upon the state to target the originator of the attack. This could prove to be difficult as such countermeasures may target individuals and computer systems that had nothing to do with the launch of the cyber-attack and have been unknowingly involved in the carriage of cyber-attacks.

---

[47] J. Goldsmith, *What is the Government's Strategy for the Cyber-exploitation Threat?* LAWFARE (Aug. 10, 2011) *available at:* https://www.lawfareblog.com/what-governments-strategy-cyber-exploitation-threat; T. Shanker & E. Bumiller, *Hackers Gained Access to Sensitive Military Files* NEW YORK TIMES (Jul. 14, 2011), *available at:* https://www.nytimes.com/2011/07/15/world/15cyber.html. (last visited 25 Dec., 2021).

[48] G.A. Res. 56/83, Responsibility of States for Internationally Wrongful Acts (Dec. 12 2001).

[49] Doge, ARCHIV DES VOLKERRECHT, MOHR SIEBECK GMBH & CO. KG, (2010).

Owing to the unique characteristics of cyber – attacks, several initiatives have been taken by various organizations around the world for the purpose of addressing the threats of cyber-attacks. In 1999, the United Nations General Assembly passed a resolution to seek information from member-states on matters related to information security.[50] The primary aspect that is required to be highlighted the most is the need for confidence building measures between different countries and a group of governmental experts submitted a set of recommendation for confidence building and stability and risk reduction.[51] Since the use of ICT in conflicts has to be addressed jointly and in tandem, the recommendation calls for the exchange of national views on the matter.[52] Through an initial first step it sought to address the first concern regarding the use of Information & Communication Technology (ICT) potential for wars by requiring States to initiate confidence building measures which could be achieved through exchange of national views on use of ICT in conflict. There are efforts by other international organizations to address the issue of cyber-attacks and cyber-crime. The Cyber Crime Convention of 2001 by the Council of Europe promulgated 'a common criminal policy aimed at the protection of society against cybercrime'.[53] It required the states to frame legislation and initiate international cooperation. While the cyber-crime convention required the States to initiate legislative action for ensuring cyber–security meaning thereby providing legal protection against offences relating to 'confidentiality, integrity, and availability of computer data and systems',[54] it on the other hand has left governmental action free from any restrictions relating to the use of cyber or information technology for carrying out its lawful objectives. Similar has been the action by the Organization of American States (OAS) that adopted 'Comprehensive Inter-American Cyber-security Strategy',[55] which provides for

> 'Cybercrime policies and legislation that will protect Internet users and prevent and deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of Internet users'.[56]

---

[50] G.A. Res. 54/49, The Developments in the Field of Information and Telecommunications in the Context of International Security, UN. Doc. A/RES/54/49 (Dec. 01, 1999).

[51] U.N.G.A. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security transmitted to the General Assembly (Note by the Secretary-Genera) l U.N. Doc. A/68/98 (Jun. 24, 2013).

[52] *Id.* at para 16(c).

[53] Convention on Cybercrime (Budapest Convention) § [Online] opened for signature Nov. 23, 2001, ETS No. 185.

[54] *Id.* at Preamble.

[55] OAS General Assembly Res. (XXXIV), Adoption of A Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating A Culture of Cybersecurity, A.G./RES. 2004 (XXXIV-O/04) (Jun. 8, 2004).

[56] *Id.* at Annexure I.

The Shanghai Cooperation Organization (SCO) has also come out with its Yekaterinburg Declaration[57] which provides for defining cyber security in a new way that includes bringing with the ambit of cyber-attack or cyber-crime offences related to political dissent. While the organizations have started initiating legislative action for regulating and controlling cyber-offences and binding its members to certain norms of conduct of desisting from initiating cyberattacks, however, acknowledging the potency of cyberattack to cause harm, NATO has set up two dedicated divisions for countering the threat to cyber security. These divisions are The Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.[58]

The above are the treaties that try to address the problems of cyber-attacks. However, there are other instruments that address the problems related to cyber-attacks. The telecommunications law, while not preventing the use of telecommunications for military purposes, provides that military installations must observe as far as possible all measures to prevent harmful interference.[59] Similarly the aviation law in the form of Chicago Convention, Montreal Convention and Montreal Protocol requires states to take measures to ensure safety of civilian aircraft, persons at airports and associated infrastructure for safe operation at airports. The law of space prohibits the use of space for military purposes while the Law of sea *inter alia* provides for the duty to prevent any unauthorised broadcast which has the purpose of preventing or hampering the broadcast or communication channels of coastal states or of ships on high seas. The UNCLOS (Law of Seas) also incorporates provisions for preventing damage to submarine cables and asks the member States to enact rules and regulations for punishing wilful damage to submarine cables.[60]

IV

Progress Towards Norms of Cyber–Security

From the analysis in the foregoing sections, it is evident that the development of laws and treaties relating to cyber security and cyber war are still at a nascent stage of development. It is in this context that the issue of cyber–security has to be

---

[57] Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation (Jun. 17, 2009) *available at*: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/200906/t20090626_679272.html (last visited 12 Dec., , 2021).

[58] Hathaway, et al., CALIFORNIA LAW REVIEW, (2012).

[59] Constitution and Convention of the International Telecommunication Union 1825 U.N.T.S. 31251 (Oct.1, 1994) article 48.

[60] Convention on the Law of the Sea 1833 U.N.T.S. 397 (Dec. 10, 1982).

discussed at an international level between the various stakeholders and the best forum for facilitating this discussion is the United Nations. The issues related to cyber–security are discussed at the first, second, and the third committees of the United Nations General Assembly.[61] The issue of 'Developments in the Field of Information and Telecommunications in the Context of International Security' was placed on the agenda of the first committee known as Committee on Disarmament and International Security, on the Russian Initiative in 1998.[62] The Second Committee (Economic and Financial Committee) and Third Committee (Social, Humanitarian and Cultural Committee) cover aspects of internet governance and freedom of expression on the internet.[63] The committee though has been the best forum for the discussion of cyber-security issues but collaboration between the different parties to the committee has not yet sufficiently materialised because of principally different approaches of the parties to information security regarding terminology, the scope of the problem, the mandate and role of the UN, and perspectives on the threat.[64] In 2001, Russia formulated a proposal to convene a Group of Governmental Experts (GGE) to discuss the threats, possible cooperation and other issues of international information security,[65] an initiative that led to concrete developments on considering the challenges of cyber security. The second report of the GGE in 2010 led to developments in understanding the position of the parties so as to pursue the matter in a collaborative manner which represented a development as previous efforts made over the last ten years to formulate standard recommendations in the cyber security realm have always ended with no agreement being reached.[66] The third meeting of the UN GGE group which submitted its report in 2013 upheld the view that International law applies to cyberspace.[67] The most recent report of the UN GGE that was presented in 2015 further adds on the work of the UN GGE report of 2013 and seeks to develop a set of norms for regulating cyberspace.[68]

The 2015 UN GGE report defines for its objective as:

---

[61] Incyder News, *United Nations: Recent Developments in the Field of Information and Telecommunications in the Context of International Security* (Nov. 14, 2012), *available at:* https://ccdcoe.org/united-nations-recent-developments-field-information-and-telecommunications-context-international.html (last visited 12 Dec., 2021).

[62] *Id.* at para 3.

[63] *Id.* at para 3.

[64] *Id.* at para 4.

[65] *Id.* at para 5.

[66] Ministry of Foreign Affairs Republic of Estonia, *National Experts Shared Cyber Security Recommendations with UN Secretary General*, MINISTRY OF FOREIGN AFFAIRS REPUBLIC OF ESTONIA (Jul., 21, 2010), *available at:* http://vm.ee/en/news/national-experts-shared-cyber-security-recommendations-un-secretary-general (last visited 12 Dec., 2021).

[67] Supra note 61.

[68] *Id.* at para 9.

> '…to study with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them ...as well as relevant international concepts aimed at strengthening the security of global information and telecommunications systems'.[69]

The report has made several recommendations and highlights the present condition of the ICT environment and thus leads to the building of norms for further development of legal regulation of the area. It points out that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among states to reduce risks to international peace and security and ICTs provide immense opportunities for social and economic development and these opportunities are continually growing.[70] The necessity of the development of norms for regulating the cyber – environment has been recognized by the report in the form that it recognizes the increase in the malicious targeting by State and non-State actors through the use of ICT tools which may have a deleterious effect on international peace and security.[71] ICT tools can be easily used for the purpose of disabling the critical infrastructure or freezing the information architecture of the adversary such that the logistical and essential infrastructure of the adversary collapses leading to threats to international peace and security.[72]

The report recommended the formulation of certain norms for the development of an ICT environment that can be relied upon to be safe, secure, accessible, and peaceful.[73] These norms have been recommended to attain the objective of increasing stability and security in the use of ICTs and prevent practises that pose a threat to international peace and security.[74] It calls upon the states to develop practises which take into account Human Rights Council resolutions 20/8 and 26/13 which have for their object the protection and enjoyment of human rights in the online environment as well as take into account the General Assembly resolutions 68/167 and 69/166 which deal with privacy in the online environment and ensure the norms and practises so developed do not run contrary to the observance of human rights.[75] The recommendations call upon the States to render cooperation to each other in preventing wrongful and criminal use of ICT and assist each other in managing and countering the threats by extending cooperation in terms of

---

[69] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security transmitted to the General Assembly: Note by the Secretary-General, UNITED NATIONS UNDOC A/70/174 (22 Jul., 2015).

[70] *Id.* at para 9.

[71] *Id.* at para 3.

[72] *Id.* at paras 5 & 6.

[73] *Id.* at para 2.

[74] *Id.* at para 6.

[75] *Id.* at para 13(e).

exchanging information and prosecuting wrongful use of ICTs.[76] The report also takes into account the various issues that arise in the case of cyber-attacks, such as the problem of attribution and the vulnerability of the critical infrastructure to ICT attacks and the total ambit of the consequences of such ICT attacks. This is because it may be difficult to attribute an ICT attack to a particular source, but such ICT attack may have the capability to cause harm beyond the immediately visible area and such harm can be to the critical infrastructure of the state. Thus the report provides that States in the case of an ICT incident should consider all aspects of the cyber incident including the difficulty in attributing the attack to a certain defined individual or state and the gravity of the attack in terms of its consequences.[77] It further calls upon the States that it should not conduct or support cyber operations that may disable or severely demote the use of critical infrastructure of a State as the consequences of such an incident for the nationals of the country could be extremely grave.[78] Besides calling upon the States to refrain from activities that seek to damage the critical infrastructure, it calls upon them to understand the that safeguarding the critical infrastructure of their states is their responsibility and adequate measures have to be taken by the states to protect their critical infrastructure in accordance with the General Assembly Resolution 58/199 which dealt with protection of information systems of the state through an emphasis on cyber security.[79] Looking at the importance of protection of critical infrastructure, the report seeks to develop the norms that the States should respond to requests for assistance by other States whose critical infrastructure is under threat because of malicious ICT attacks, whether emanating from their territory or elsewhere.[80] One of the ways the ICT security can be compromised is through the insertion of malware in ICT products. The report calls upon the nations to take steps to ensure that the supply chain security of their products is maintained, which would ensure the development of a robust ICT infrastructure. It further asks the States to take measures to prevent the spread of malicious codes independently or in compromised hardware thereby promoting security. The report further seeks to ensure the security of ICT systems through sharing of information on vulnerabilities and remedies to eliminate or reduce threats to the digital infrastructure. Similarly, it further seeks to develop the norms on responding to an ICT emergency. Norms related to the emergency response teams have to be developed to ensure the security of emergency response teams that are there to counter the threat or control damage emerging from ICT related incidents. The work of emergency response teams is crucial to curtail damage and prevent harm from spreading. Any hindrance to the activity of emergency response teams is likely to amplify the damage by orders of magnitude

---

[76] *Id.* at paras 13 (c) & (d).
[77] *Id.* at para 13(b).
[78] *Id.* at para 13 (f).
[79] *Id.* at para 13(g).
[80] *Id.* at para 13(h).

and therefore as a corollary if emergency response teams are to be protected from any interference from other states so that they may carry out their assigned tasks effectively, it also implies that the emergency response teams should not be used to carry out malicious ICT activities. The report recognizes that for developing countries implementation of cyber security measures immediately may not be possible and norms for developing countries may have to be developed over time.[81]

Confidence-Building Measures as Recommended in the Report

The report has also emphasized on the confidence building measures for the purpose of enhancing cyber-security and reducing cyber related incidents. It starts with the recommendation for the primary action that should be taken in the case of a cyber-security incident. It recommends that appropriate points of contact should be highlighted which can be approached in the case of a cyber-security incident. Subsequent to this could be efforts to reduce the risk of such incidents escalating into a full -fledged cyber - security conflict and which could take the form of inter-state consultations. A further effort could be to encourage transparency by voluntary sharing of threats to the ICT infrastructure both at national and transnational levels;[82]sharing of vulnerabilities that may be present in ICT products and functions of such products that could be manifest themselves as a threat to cyber security;[83] sharing of best practises that could be adopted to reduce the threat of cyber incidents;[84] promoting confidence-building measures that would promote international peace and security so far as the ICT infrastructure is concerned;[85] creating national organizations, and adopting strategies for promoting ICT security.[86] Another set of measures that could lead to confidence building is making a provision for exchanging views on categorising infrastructure as critical for the nation and the steps that they have taken to protect such infrastructure including information on the laws and policies that have been adopted for such purpose.[87] States could also seek to address the critical infrastructure vulnerabilities that have cross-border components by developing a mechanism consultations,[88] preparing a repository containing laws, guidelines and policies for the protection of critical infrastructure and effective action in case of an attack.[89] The report recommends certain other confidence building measures to strengthen cooperation between States and which may include exchange of personnel and cooperation between

---

[81] *Id.* at para 14.
[82] *Id.* at para 16(c).
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.* at para 16(d).
[88] *Id.* at para 16{(d)(ii)&(iii)}.
[89] *Id.* at para 16{(d)(i)}.

agencies involved in dealing with technical matters of ICT or with law enforcement and with research.[90] The report stresses on the creation of cyber security incident response team which may the function of emergency response once a cyber threat has materialized with the objective of limiting damage and bringing the systems back to normalcy.[91] The report calls for cooperation in areas related to the full spectrum of ICT infrastructure and its operation while also emphasizing cooperation in prevention of ICT related threats and coordinating mitigation activities in case of a cyber incident.[92] Similarly the ambit of cooperation can extend to joint investigation of ICT related criminal activities such as terrorist financing or creation of malicious tools and prevention of malicious activities. The report also recommended the creation of a forum where institutional dialogue could take place amongst the representatives of the States for promoting cyber security[93] as a confidence building measure.

Assistance in ICT Security and Capacity Building

The third aspect of the report was cooperation with other states in enhancing ICT Security and Capacity Building of such states in the ICT infrastructure. It says that the certain states may lack the requisite capacity of ensuring cyber security for their ICT infrastructure[94] which would make their ICT infrastructure susceptible to attacks and utilization which would such unprotected systems a threat for international security. The report emphasized upon providing assistance to such states for cooperation and capacity building for peaceful use of ICT. It also recommended capacity building and assistance for improving the environment of security for their ICT infrastructure, steps towards the development of an institutional framework for supporting the development of technical skills and laws for the purpose of utilizing the ICT infrastructure while ensuring its safety.[95] The report further laid emphasis on the fact that cyber security is not the responsibility of an individual State but it is a joint and collective responsibility of the States and therefore steps should be taken to ensure that States carry out their responsibilities collectively which would include developing capacity in States that lack such capacity.[96] The report further called upon the States to provide assistance for developing and strengthening mechanisms which ensure cooperation with emergency response teams; provide assistance in capacity building for ICT related infrastructure to developing countries; improve access to essential technologies for ICT infrastructure security; create and strengthen procedures for cooperation and

---

[90] *Id.* at para 17.
[91] *Id.* at paras para 17(c) & 17(d).
[92] *Id.* at para 17(d).
[93] *Id.* at para 18.
[94] *Id.* at para 19.
[95] *Id.* at para 20.
[96] *Id.* at para 20.

assistance to address ICT related incidents; promote cooperation for activities which have the objective of addressing vulnerabilities in critical infrastructure that have cross border ramifications; allocate sufficient funds for developing ICT security infrastructure, addressing cyber incidents and for developing capacity in cyber forensics so that effective and preventive measures could be taken for preventing cyber incidents. [97]

The recommendations of the group are in the nature of soft law recommendations for cyber-related events. It has taken into account that a cyber-related incident has the potential to escalate into an international crisis. It is also evident that the group has acknowledged that there is a problem of attribution in cyber-incidents and has configured its recommendations in the light of this specific characteristic of cyber-incidents. The group has contoured its recommendations along the lines of responsibility of States and has provided recommendations for States in terms of dos and don'ts along the lines of encouraging an understanding of the ambit of cyber-related incidents and its potential to escalate into a fully-fledged conflict.

V

Conclusion

The development of the humanitarian law in the form of *jus ad bello* and *jus ad bellum* has followed a trajectory which for its subject had the regulation of war through traditional means and through kinetic weapons. These laws were able to regulate activities that had more or less a direct impact on the target and affected population and were framed at a time when the parties in conflict were more or less identifiable and determinable and hence the application of the laws was not questioned. The emergence of cyber-conflict has changed all these assumptions. The damage that can be wrought by a cyber-attack can equal if not exceed the damage wrought by traditional weapons. In addition, in case of cyber-attack it is difficult to identify the aggressor and victim and differentiation between combatants and non-combatants. The recommendation of the UN GGE 2015 takes into account the unique characteristics of cyber-conflict and offers recommendations as to how to build up a corpus of laws and legal regulations for regulating cyber -conflicts. Developing rules for regulation of cyber-conflicts needs a set of new norms to be followed by the states and the UN GGE 2015 seeks to achieve the development of such norms.

---

[97] *Id.* at para 21.