**Rethinking the Dimensions of 21st Century Warfare: Reconciling 'Cyber War' with the Principles of International Law**

***Shubham Kataruka***

**11th December 2018**

Dear Editor,

In 21st Century International Politics, a new dimension of war has kindled in addition to war in sea, air, space and on land. It is popularly termed as 'Cyber Warfare'. Cyber space transcends beyond state boundaries and makes almost all the internet users the 'stakeholders' in the prevailing scourge of cyber war across the globe. It is becoming the greatest threat to national security of sovereign states across the globe.[1] Post 9/11, the thrust of development of cyber war techniques among the developed and developing nations has consistently gained momentum. In the United States, Bush Administration initiated actions in this regard which gained much pace during Obama as the President. The US policy definition of cyberspace could be traced in the National Security Presidential Directive of 2012.[2] Then there was Operation Olympic Games- a covert mission to sabotage Iranian Nuclear Facilities through cyber disruptions, which acted as an alarm at the international fora making all the nation states realise that a new archetype of war is at the door foot.[3] More recently in 2014, North Korea threatened to attack the computer systems of Sony Pictures so as to compel the latter to withdraw its then upcoming movie The Interview. The movie depicted a secret mission planned by CIA to assassinate North Korean Dictator Kim Jong-Un. The threat succeeded by a blow on the North Korea's computer system just after two days when US President Barack Obama stated that US would not accept such threats by North Korea against Sony pictures.[4] These events manifest the uniqueness, spontaneity and potential associated with the new dimension of warfare.

---

[1] Kate O'Flaherty, 'Cyber Warfare: The Threat From Nation States' (*Forbes*, 3 May 2018) <https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#4e158d951c78> accessed 11 November 2018; See also Jim Garamone, 'Cyber Tops List of Threats to US, Director of National Intelligence Says' (*US Department of Defence*, 13 February 2018) <https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/> accessed 11 November 2018.

[2] National Security Presidential Directive 54, *Cyber Security Policy* (22 January 2008).

[3] David E Sanger**,** 'Obama Order Sped Up Wave of Cyberattacks Against Iran' *The New York Times* (New York, 1 June 2012) <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> accessed 15 November 2018.

[4] 'The Interview: Obama Hails Move to Screen North Korea Film' *BBC News* (London, 24 December 2014) <http://www.bbc.com/news/world-us-canada-30594820> accessed 31 October 2018.

Studies suggest that a majority of nation states across the globe have developed means to use the internet for targeting financial markets, government computer systems and other valuable utilities[5]. States as well as Non-State actors are pervading into the cyberspace in order to annihilate the enemy's military as well as the economic capabilities.[6] Certainly, non-state actors do involve in cyber military operations although with a varying degree of dependence upon their own organisational structure, ideological backing and relation with the state. A criminal organisation known as 'Russian Business Network' administers various illegal cyber activities such as malware distribution and child pornography and is believed to have contributed in cyber attacks of 2008 during Russia- Georgia conflict.[7] Some of the so called 'patriotic' hackers are freely operating under the patronage of state. A Chinese hacker group known as the 'Red Hacker Alliance' is active since the year 2000 which the Chinese state media claim to be an anti-hacking group.[8] During a panel discussion on cyber warfare, a high profile member of the Russian ruling party, Sergei Markov stated that one of his assistants was responsible in orchestrating the cyber attacks on Estonia in the year 2007.[9] In these situations, non-state actors acting on behalf or on instructions of state parties engaging in cyber warfare must be brought under the umbrella of international law as incorporated in Article 8 of the Responsibility of States for Internationally Wrongful Acts 2001 adopted by the International Law Commission to ensure accountability and attribution of cyber attacks. Further, in consonance with the Article 29 of the Budapest Convention on Cybercrime, right to obtain expeditious preservation of data stored in computer systems located within the territory of the party in respect of which the request has been made shall be incorporated as a provision applicable to all member states of the United Nations. Attribution of cyber attack could be done once the offensive computer system or server is located, followed by tracing the individual(s) giving effect to the attack. Henceforth, substantial nexus between the offender(s) and the state must be proved in order to attribute such acts to the state.

---

[5]China Institute of International Studies, *Cyber War Preparedness, Cyberspace Arms Control and the United States* (Report No 3, 2014); Mohan B Gazula, 'Cyber Warfare Conflict Analysis and Case' (2017) Massachusetts Institute of Technology 2017-10 <http://web.mit.edu/smadnick/www/wp/2017-10.pdf> accessed 20 July 2018.

[6] BBC News (n 4); See also Nicolò Bussolati, 'The Rise of Non-State Actors in Cyberwarfare' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015), 102-103.

[7] Markoff John, 'Before the Gunfire, Cyber attacks' *The New York Times* (New York, 12 August 2008) <https://www.nytimes.com/2008/08/13/technology/13cyber.html> accessed 31 October 2018.

[8]'China's Anti -Hacking Alliance Regrouped' *China Daily* (London, 26 April 2005), <http://www.chinadaily.com.cn/english/doc/2005-04/26/content_437502.htm> accessed 17 November 2018.

[9] John Leyden, 'Russian Politician: My Assistant Started Estonian Cyberwar' (*The Register*, 10 March 2009) <https://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/> accessed 17 November 2018.

Academic debate over cyberspace reflects a paradigm shift with the passage of time. Earlier scholars propagated the idea of cyber 'exceptionalism',[10] however, in the last few years there has been a sea change in this view and possibilities of incorporating cyberspace within the legal hemisphere are being explored. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence appointed an International Group of Experts (IGE) which came with the first full draft of a document laying down certain legal principles to govern cyber warfare. The document was titled as 'Tallin Manual', which appeared in August 2012.[11] The Manual proposes solutions to certain questions which require primary attention. Rules in the manual make a distinction between force and other forms of coercion on the basis of the 'scale and effects' of a particular action.[12] Other factors which have been discussed elaborately are the severity of the attack, the immediacy of the response, the directness of the link between the attack and the harm done, the invasiveness of the attack, the measurability of the effects, the military character of the attack, state involvement in the attack and the presumptive legality of actions under international law generally.[13] On the other hand, the second world countries have also submitted their own version of 'International Code of Conduct' on cyber warfare. On 9th January 2015, six members of the Shanghai Cooperation Organisation (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) proposed an updated version of the International Code of Conduct for Information Security to the United Nations.[14] The problem persists with regard to universal acceptance of the abovementioned Rules as the bipolar political world organisations still need to engage in a meaningful dialogue so as to arrive at a consensus on the issue of regulating and securing cyberspace.

The Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is a touchstone to develop mutual understanding to fight against the prevailing scourge of cyber war at the global level.[15] As suggested in the report, common understandings on norms, rules and principles applicable

---

[10]Pierre Pahlavi, 'Cyber-Diplomacy: A New Strategy of Influence' (Canadian Political Science Association General Meeting, Nova Scotia, 30 May 2003) <https://www.cpsa-acsp.ca/paper-2003/pahlavi.pdf> accessed 4 September 2018.

[11] Michael N Schmitt, *The Tallin Manual on International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

[12] ibid Rule 11.

[13] Michael Schmitt, 'Computer Networks and the Use of Force in International Law: Thought on a Normative Framework' (1999) 37 Colum J Transnat'l L 885, 914.

[14] UNGA 'Developments in the Field of Information and Telecommunications in the Context of International Security' (13 January 2015) UN Doc A/69/723 <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf> accessed 16 November 2018.

[15]Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Contex t of Int'l Security, UN Doc A/68/98 (2013).

to the use of information and communication technologies by States and voluntary confidence-building measures can play an important role in advancing peace and security. In addition to regulatory framework, an International Cyberspace Station (ICS) may be set up under the International Telecommunication Union, a special UN agency specially dedicated for information and communication technologies.[16] This body shall have power to investigate any incident of cyber attack across the globe on an application made by the victim state or a private organisation. The findings of ICS can be brought to notice of the appropriate court or Security Council to justify the act of 'self defence' by the victim or to seek appropriate action against the belligerent state or non state actor as the case may be.

On the issue of applicability of international law on Cyber Warfare, the Group of Governmental Experts has reiterated that the Charter of UN is essentially applicable to maintain peace and stability and promote an open, secure, peaceful and accessible cyberspace.[17] Now, it is upon the world community either to maintain the status quo of cyber security which has rendered the international security vulnerable to disastrous consequences or the countries may strive towards pure internationalisation of cyber warfare. The world community must unite to neutralise the prevailing scourge of cyber warfare by way of forging accountability and transparency in cyber operations. It is high time that states across the globe accept the fact that cyberspace is that one weapon which cannot be snatched away from the hands of terrorists. If this weapon is brought to use with its maximum capacity, it may end up yielding a more disturbing picture than what is often perceived for a nuclear catastrophe. It is so because a cyber attack of highest degree will result in a global blackout and consequently the world will end up witnessing the largest chaos one could ever think of. A transnational shutdown is the worst that this modern world could think of. In nuclear apocalypse, the tragic moment would be of a split second. However, a cyber attack can trigger the global civil war which will take lives in phases and the war will not come to an end till the last survivor on the planet earth dies.

Is mise le meas,

Shubham Kataruka

---

[16]See International Telecommunication Union, <https://www.itu.int/en/about/Pages/default.aspx> accessed 31 October 2018.

[17]David P Fidler, 'The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers' (*Council on Foreign Relations*, 15 March 2018) <https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers> accessed 31 October 2018.