2.

NEW MEDIA IN CYBER REGIME AND APPLICATION OF INTERNATIONAL HUMANITARIAN LAW: A CRITICAL APPRAISAL

Dinesh Kumar Singh[1]

Introduction:

> *"Media appear to be increasingly globalised, as national television, press, etc. are subsumed in gigantic worldwide flows of information and ideas, symbolized by the internet, which offers social and political actors new opportunities for direct communication."*(Jong et al., 2005:1)

The above observation shows the changing nature of media and introduces a new approach of negotiating and communicating round the world. The Internet is no respecter of national borders; similarly the new media with the help of Internet and World Wide Web have global coverage. The private and/or non-state actor especially transnational corporation (TNCs) is also constantly attempting to change the nature of media as mass media to corporate media. The information and communication system generally covers: global or international communication; mass media; new social media and media technologies information technology such as Internet and the World Wide Web are new 'socio-technical' phenomena in the New Media. The term 'socio-technical', as David Bell pointed out, is used to make explicit the complex commingling of society and technology; such that an object like a computer has to be seen as the product of, and occupying space within, particular socio-technical assemblages (Bell, 2009: 30). Considering function of media as information, entertainment and opinion – the new area of research in this discipline is to explore the nature and impact of web-based digital communication on media content and how they function in the world of cyberspace.

[1] Dinesh Kumar Singh is a Research Scholar in Centre for International Legal Studies, School of International Studies, Jawaharlal Nehru University, New Delhi. Email – dineshinjnu@gmail.com.

New media has developed through the emergence of cyberspace and advancement of information technology. Cyberspace and cyber culture are among the terms used in context with the Internet and the World Wide Web. Some important and relevant question about new/cyber media is: whether it is independent media (the part of a larger professional media system) or corporate media as a subset of marketing and promotion in global capitalist system. Other question is whether cyber/new media has the capacity to create public sphere like other media or it will also become a controlling mechanism in the hand of big corporations. New media is generally more liberal trans-boundary and uncontrolled media. Cyberspace, the producer and base for new media, is both a vast reservoir of useful information and a babbling brook of streaming consciousness (Berenger, 2006: 178). The new media provides users an alternative to become either passive or active consumers of information, but the information blitzkrieg might cause many casualties as destruction of understanding and cyberspace war. Cyber warfare, cyber conflict, cyber espionage, cybercrime, and cyber terrorism are the negative utilization of the new media or cyberspace. Jeffrey Carr has pointed out that international acts of cyber conflict (commonly referred as cyber warfare) are intricately enmeshed with cyber crime, cyber security, cyber terrorism and cyber espionage. One popular example of negative utilization of cyberspace is: the digitalized cartoons[2]of Prophet Muhammad which were widely distributed by Islamic activists over the internet, thus expending globally the reach of these drawing and eliciting violent protests in places that are densely populated by Muslims around the world. Arab and Muslim hackers mobilized to attack Danish and Dutch websites in 2006 during the prophet cartoon controversy. Another example, the website 'eljehad.netfirms.com' was established to defend Muslim websites, particularly Palestinian websites against Israeli hackers. The founder and supervisor of the website, in promoting cyber jihad, wrote: "I built this website for my Muslim brothers around the world. It is a gift to everyone willing to devote himself for jihad and E-Jihad. It is a present to every decent Muslim whose intention is only to use the internet to raise the religion and to fight the enemies of Allah…this website will guide you to the E-Jihad options (Maghaireh, 2013: 143)."

It can be seen that, for a different purpose and with different intention, a significant number of hackers and individuals have committed different cyber offences – including criminal access, cyber terrorism, cyber conflict and cyber war. In this way from website hacking to cyber warfare, any tiny activity can disturb global peace and security.

[2] In 2005 Danish political cartoon controversy that was believed to depict the Prophet Muhammad, a cultural taboo.

Some Definitions

The new media is usually defined as anything digital that communicates to known and unknown or actual and virtual audience. Nearly all new media used or have the capabilities of using a variety of different media that produce or synthesize into a new type of communication media. Manu argued that "there is no such thing as 'new media'. When telegraph messages sped the process of communicating from far-away places in the 19th century, it could have been regarded as a new media. The same could be said of commercial radio when it emerged early in the 20th century, and television as it became the dominant medium in the last half of that century (Berenger, 2006: 179). The adaptation of the internet for information, combining words, pictures sound and video is only the latest to fall under the rubric of a new media, while predecessors join the category of traditional or legacy media.

What then is new about New Media? In the era of information and technology, the new media is a new way of communication between people, between cultures and races, between human and machines, and between machines and machines. Berenger (2006: 26) has also characterized the new media as: ''the characteristics of new media fall into several broad categories i.e. convergent, ubiquitous (omnipresent), agenda-setting, credibility, interactivity and transferability."Using Marshall McLuhan's definition of media as an "extension of man", new media includes all the various forms in which a human being can expand his senses and brains into the world. It extensively covers websites, audio and video content streaming on the internet and mobile devices, audio and video content on demand (VoD), chat rooms, blogs, email, social media such as facebook, MySpace, and Twitter; digital marketing by e-mail and text messages; virtual reality environments, video games; internet telephony, digital cameras; and mobile technologies such as smart phones using 3G and 4G technologies to access the internet. In a nutshell, new media is the convergence of telecommunications, computing and traditional media and it includes any media production that is digitally distributed and interactive.

New Media has developed in the regime of cyberspace. Some definition related with cyber is also necessary. United Nations (UN) defines 'cyber' as "the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net. This mostly means the Internet; but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization (Winterfeld and Andress, 2013: 17). US Department of Defense

defines 'cyberspace' as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Castelli, 2008)."

There are some popular cyber offences which is necessary to explain here to understand the seriousness of cyber regime and to implement humanitarian law on it. These offences are: The United Nation Security Council Resolution No. 1113 of 2011 has defined cyber warfare as:

> *"Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: (a) Intentional access, interception of data or damage to digital and digitally controlled infrastructure. (b) Production and distribution of devices which can be used to subvert domestic activity".*

In other words cyber warfare includes a wide range of activities that use information systems as weapons against an opposing force. Cyber warfare is therefore composed of activities with the purpose to disavow, damage or destroy the opponent's sources of information, and it includes both attack and defense activities. Along with cyber war, cyber security can be challenged by three other major threats: espionage, crime, and cyber terrorism. With regard to global cyber security concern two crucial issues is necessary to emphasize: a politico-military stream focusing on cyber-warfare and an economic stream focusing on cyber-crime.

Mis(Use) of New Media in Cyber Regime

Generally the internet and new media are associated with positive development, as they represent technological progress. Technological progress indicates improvements of almost all aspects of life with the help of technology and reconstruct just and equitable distribution of wealth and power. New media regimes emerge from debates over which citizens should (or can) be part of democratic deliberation (Williams and Carpini, 2011: 19).The new media also have potential to play a crucial role in democracy and promote human development across the world. But it does not mean new media will cure all social or political evils and it has no shortcomings. New media or cyber technology can be used to threat or destroy the information and communication. The threats include different forms of attacks and techniques as well as malware and physical threat (Martti Lehto, 2015: 9). Some of the major threat agents or actors in cyberspace are

transnational corporations (TNCs), cybercriminals, employees, hacktivists, nation states and terrorists.

The common threats in internet or cyber regime are cyber activism, cybercrime, cyber espionage, cyber conflict, cyber terrorism and cyber warfare. Cyber activism encompasses cyber vandalism, hacking and hacktivism. Hacking is the crucial problem before new media especially digital or internet media. Hacking, also referred as information warfare, uses information technology tools to attack enemy websites (Siapera, 2012: 112). They use different techniques for different ends. These include Distributed Denial of Service (DDoS) attacks, and Domain Name Service (DNS) attacks. In the case of DDoS, websites are prevented from working because they are flooded by a very high number of page requests, usually by 'zombie' machines. In DNS attacks the domain name is severed from its numerical address, preventing users from accessing the site.

Two other profoundly problematic techno-political phenomena are encountered in online and other new media environments. These include *cyber-conflict* and *cyber-terrorism*. In both cases some malicious methods are used: the spread of worms and unauthorized intrusions (Siapera, 2012). Worms may enable hackers to gain control of computer accounts, turning them into 'zombies' which operate without the owner's knowledge and approval. Unauthorized intrusions into computer system are the perhaps the most widespread form of hacking. Through their illicit action hackers can get access to top secret information or otherwise sabotage the system. These methods can work together as well as separately, and are quite effective weapons in cyber-war. The *cyber conflicts* may be defined as 'a confrontation between two or more parties, where at least one party used cyber attacks against the other(s).' while *cyber-terrorism* is understood as 'premeditated, politically motivated attack against information, computer systems, computer programs, and data systems that results in violence against non-combatant targets, and which are undertaken by sub-national groups or clandestine agent' (Pollitt, 1989). Both cyber-conflict and cyber terrorism may be considered problematic, because they involve violence and coercion on others.

With armed war, a hacking and cyber war is continuously going on between Israelis and Palestinians since long time. According to Gary Bunt (2003: 43), one of the most well-known hacking incidents was related to Ariel Sharon, one of the Israel's most senior political leaders. Sharon's election campaign website was hacked by the World's Fantabulous Defacers (WFD), who kept the original format of the site but changed the

image and text. Sharon was described as a ‘war criminal’; the photos are extremely graphic, including posting horrific photos of an injured Palestinian child, and the statement ‘Long Live Hizballah! Long Live Palestine! Long live Chechnya, Kashmir, Kosovo and Bosnia. In the ensuring cyber-war, visitors to the Hamas website were diverted to porn sites, alleged by Israeli hackers. Unity, a website which forms part of the British registered ummah.net domain sought to attack Israeli ISPs as part of a strategy which would disable Israeli government sites first, followed by financial sites, at the same time crippling Israeli ISP servers and disrupting e-commerce sites.

The use of new media in propaganda or rumors has sometimes more dangerous and disturbing consequences. In 2007 a video of a girl stoned to death was circulated on the internet (Siapera, 2012: 113). The girl, named ‘Du’a Khalid Aswad’ of Kurdish ethnic origin and Yazidi religion, was stoned because she had eloped with a Kurdish Muslim boy. This video was replaced in various Islamic and jihadist fora, which reframed it as a crime against Islam and because she had converted to Islam, she was killed. Subsequently calling for some sort of retaliation and revenge, several people with gun stopped a bus with factory workers returning to Bashika, abducting all men of Yazidi faith, and then executing them. The internet, in war or conflict situation, can be used in very effective way. It can be used to initiate events and control their outcome, as in the case of DDoS and DNS attacks; it can be used to regulate the flow of information. It can also be used to mobilize support, both in the form of new recruits as well as in the form of donation. The use of the internet in cyber-conflict and cyber-terrorism provides a good example of the mutual shaping of technology and world politics.

The aim of Hacking, cyber conflict or cyber terrorism is not only political but it also involves economic and cultural dimension. This shows its vulnerability to attacks motivated by financial gains. It is ranging from email scam to Trojans and other high-tech tools to defraud. When Google decided to enter China in 2006, it faces Chinese censorship of certain politically sensitive keywords and sites – at the same time Google local search engine in China was discontinued due to cyber attacks that supposedly originated from within China (Lindtner and Szablewicz, 2011: 89).The announcement led to heated debates about the divergent values and ethics of Chinese and American politics. From this point of view, political cyber-conflict and economic cyber-fraud provide for direct surveillance and control over cyberspace. All threat and crime, except cyber warfare, are regulated by domestic law and same procedures apply as other crime.

In India, cyber law is contained in the Information Technology (hereafter referred to as "IT") Act, 2000. The IT Act, 2000 specifically defines and punishes only a few cyber crimes, it recognizes that there are other crimes of cyberspace which are provided in the Indian Penal Code, 1860.Some of punishable offence in India under IT Act, 2000 are: Hacking (Section 66), virus on the computer or internet (Section 43, Section 66), obscenity (Section 67), destroys or alters any computer source code (Section 65), failure to comply with the order of the Controller of Certifying Authority (Section 68) and Breach of confidentiality and privacy (Section 72). Besides the cyber crimes other offences and violations have also been provided in the IT Act, 2000.

Cyber warfare is the most grievous threat in cyber space and for some, cyber warfare is war which is conducted in the virtual domain. For others, it is the counterpart of conventional 'kinetic' warfare. According to the OECD's 2001 report, cyber war military doctrines resemble those of so-called conventional war: retaliation and deterrence. These are generally three types: strategic cyber warfare, tactical/operational cyber warfare and cyber warfare in low-intensity conflicts (Lehto and Neittaanmaki, 2015: 9).It is quite liberally being used to describe the operations of state-actors in cyberspace. Cyber warfare therefore requires a state of war between states, with cyber operations being but a part of other military operations.

Emerging Regulatory Mechanism

In 1999 former UN Secretary-General Kofi Annan, on issues of misuse of Internet and cyberspace, stated that:

> *"The same Internet that has facilitated the spread of human rights and good governance norms has also been a conduit for propagating intolerance and has diffused information necessary for building weapons of terror (Jaeger, 2004: 355)."*

The 56th regular session of the UN General Assembly declared that cyberspace threats are a weapon against UN goals and unanimously passed a resolution condemning terrorism and cyber terrorism. In December 2000 and January 2002, the UNGA adopted Resolution 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies. UNGA Resolution 55/63 (2001) recommends various measures addressed in comparable international anti-cybercrime initiatives, such as criminalization of illicit online activities, international cooperation in investigation and enforcement efforts, preservation and timely sharing of electronic data and evidence, and data confidentiality and integrity. It also provides that states should ensure that both

law and practice serve to eliminate "safe havens" for those who carry out cyber crime and criminally misuse information technologies."

Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure the criminal abuse is penalized. UNGAResolution 56/121 (2002) encourages the development of a global legal framework by noting the work of international and regional organization in combating cybercrime, including convention on cybercrime. UNGA Resolutions 57/239 (2002) and 58/199 (2004) were later adopted to create "a global culture of cyber security and the protection of critical information infrastructures."

There is no comprehensive international treaty in place that establishes a legal definition for an act of cyber aggression (Carr, 2010: 31) and to regulate cyber attacks. Consequently, states must practice law by *analogy*: either equating cyber attacks to traditional armed attacks and responding to them under the law of war or equating them to criminal activity and dealing with them under domestic criminal laws. *First* the legal aspects of cyber warfare could be analyzed in the light of international humanitarian law (IHL) and how it is used to respond to cyber warfare. The IHL deals with laws to prevent unnecessary destruction and suffering of human being. IHL covers two key areas: protection and assistance to those affected by the hostilities, and regulation of the means and methods of warfare. The main sources of the IHL are Hague Convention (1907), which sets out restrictions on the means and methods of warfare, and the four Geneva Conventions (1949), which provide protection to civilians, prisoners of war, the wounded, sick, and shipwrecked. IHL applies to international armed conflicts and in the conduct of military operations and related activities in armed conflict. The analysis of whether states can respond to cyber attacks with active defenses predominantly falls under IHL, if the cyber attack is considered acts of war.

Second, the relevant articles of the UN Charter are Articles 2(4), 39, and 51, which can provide the guidelines or direction in framing for the regulatory mechanism or international treaty for cyber warfare. Article 2(4) prohibits states from employing "the threat or use of force against the territorial integrity or political independence of another state, or in any other manner in consistent with the Purposes of the United Nations." In effect, it prohibits both the aggressive use of force and the threat of the aggressive use of force by states as crimes against international peace and security. Michael N. Schmitt (1999: 913) has advanced six criteria for evaluating cyber attacks as armed attacks.

These criteria are:

- *Severity* which looks at the scope and intensity of an attack i.e. the number of people killed, size of the area attacked, and amount of damaged property.
- *Immediacy* which looks at the duration of a cyber attack, as well as other timing factors.
- *Directness* which looks at the harm caused. If the attack was the proximate cause of the harm, it strengthens the argument that the cyber attack was an armed attack.
- *Invasiveness* which looks at the locus of the attack. An invasive attack is one that physically crosses state borders, or electronically crosses borders and causes harm within the victim-state.
- *Measurability* which tries to quantify the damage done by the cyber attack. Quantifiable harm is generally treated more seriously in the international community and
- *Presumptive legitimacy* which focuses on state practice and the accepted norms of behavior in the international community. Actions may gain legitimacy under the law when the international community accepts certain behavior as legitimate.

Taken together, they allow states to measure cyber attacks along several different axes. Some scholars anticipate that Schmitt's criteria if get wider acceptance, will help to bring some uniformity to state efforts to classify cyber attacks.

Another attempt that have made by NATO Cooperative Cyber Defence Centre of Excellence in 2013 and the document is known as '*The Tallinn Manual on the International Law Applicable to Cyber Warfare'* (hereafter Tallinn Manual). It contributed greatly to national and international understanding and directly related with cyber warfare."This document was developed to examine as to what extent international law norms apply to this "new" form of warfare. The Tallinn Manual consists of "rules" adopted unanimously by the International Group of Experts that are meant to reflect customary international law and highlights any differences of opinion among the experts as to their interpretation in the cyber context.

Following are the key conclusions from the Tallinn Manual:

- States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States (Rule 5 of Tallinn Manual).

This rule establishes a standard of behavior for State in relation to two categories of infrastructure: (i) Any cyber infrastructure (government or not in nature) located on their territories; and (ii) cyber infrastructure located elsewhere but over which the State in question has either *de jure* or *de facto* exclusive control. The principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States. In the *Nicaragua case (1986),* International Court of Justice (ICJ) held, 'between independent states, respect for territorial sovereignty is an essential foundation of international relations. In *Corfu Channel case (1949)* the ICJ observed that a state may not 'allow knowingly its territory to be used for acts contrary to the rights of other states.' So a cyber-operation, which comes under the category of use of force or armed attacks, cannot allow operating from the territory by a sovereign State.

- A State bears international legal responsibility for a cyber-operation attributable to it and which constitutes a breach of an international obligation (Rule 6 of Tallinn Manual).

States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the State itself will be responsible under international law for any actions of individuals or groups who act under its direction .*Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001)*[3] also indicated that State agency must be held responsible for the act of individual or non-state actors. This body of law has most recently and most comprehensively documented on the international law of state responsibility. The use of force (including through cyber operations) by individual hackers and other non-state actors may be relevant under IHL and, in some cases, international criminal law, but is not prohibited by article 2(4) of the UN Charter.

[3] The Draft was adopted by the International Law Commission at fifty-third session, in 2001 and submitted to the General Assembly. The text reproduced as it appears in the annex to General Assembly Resolution56/83 of December (2001).

- A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is any other manner inconsistent with the purposes of the United Nations, is unlawful (Rule 10 of Tallinn Manual).

  The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that any cyber operation that caused harm to individuals or damage to objects qualified as a use of force. The International Group of Experts also agreed that cyber operations that merely cause inconvenience or irritation do not qualify as uses of force (Watkin and Norris, 2012: 132). It includes taking control of its national cyber systems or causing severe disruption to economy, transportation system or other critical infrastructure. International law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure per se. Obviously, not every cyber operation by one State against another should amount to an armed conflict. But where should the line be drawn?

- A State injured by an internationally wrongly act may resort to proportionate countermeasures, including cyber countermeasures against the responsible State (Rule 9 of Tallinn Manual).

  States may respond to unlawful cyber operations, if do not rise to the level of a use of force, with countermeasures. Where a computer network attack not amount to an armed attack (or a use of force) any countermeasures can be taken by the victim state. In the *Case Concerning the Gabcikovo-Nagymaros Project (1997)*, ICJ set out a three-part test justifying proportionate countermeasures. First, the action must be taken in response to an internationally wrongful act of another state and be directed against that state. Second, the victim state must have called upon the offending state to discontinue its wrongful conduct or to make reparation for it. And finally, the effects of the countermeasure must be commensurate with the injury suffered, taking account of the right in question. The court also stated that the purpose of countermeasures must be to induce the

wrongdoing state to comply with its obligations under international law, and that measures must therefore be reversible.

- A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an attack dependent on its scale and effects (Rule 9 of Tallinn Manual).

  A State that is the victim of a cyber armed attack may respond by using force. In international law, an "armed attack" is a "grave" use of force. Any cyber operation that results in death or significant damage to property qualifies as an armed attack. The 'use of force' standard is employed to determine whether a state has violated Article 2(4) of the UN Charter and the related customary international law prohibition.

Cyber Warfare: Some Critical Issue

The cyberspace creates new opportunity and new challenge before global system. In international law it presents a very fundamental question whether old laws of international law especially international humanitarian law applies to new cyber regime/warfare. Legal Adviser for the U.S. Department of State, Harold Hongju Koh answered some fundamental questions about cyber space and cyber warfare in a conference.[4] Some of his crucial observations are:

> *"The principles of international law apply in cyberspace. But Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint. Under international law, Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law."*

In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances. In other words *'jus in bello'* rules

[4] Harold Hongju Koh (2012), Speech delivered on 18 September 2012 at USCYBERCOM Inter-Agency Legal Conference on the topic, "The Roles of Cyber in National Defense ", [Online: Web] Accessed on 23 June 2015 URL:http://www.state.gov/s/l/releases/remarks/197924.htm

apply to computer network attacks. On the other hand, a state's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof. States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control. States should undertake a legal review of weapons, including those that employ a cyber capability.

Conclusion

The new media has challenged the role of professional journalists as the source of politically relevant information. The new media environment has challenged the role of professional journalists as the source of politically relevant information. New media regime had emerged, consisting of the increasing dominance of electronic over print media, concentrated ownership of a shrinking number of media outlets, a limited public service obligation imposed on radio and television networks in obligation imposed on radio and television networks in exchange for the use if the public airwaves fir private profit.

Cyber attacks through new media as well as on the new media are greatest threats to international peace and security in the21st century. Securing cyberspace is an absolute imperative. In an ideal world, states would work together to eliminate the cyber threat. Unfortunately, our world is no utopia, nor is it likely to become one. The United Nations, a crucial international organization, has taken extremely few steps towards the setting of an international standard regarding the regulation of computer attacks. Because Security Council is concerned with peace and security, it has been proposed that the Security Council should be the organ that decides when a perpetrated cyber attack constitutes a threat or breach of the international peace. There should be a binding international hard law which regulates the activity of State's as well as non-State actors in cyber warfare. The creation of a UN subsidiary body is necessary to investigate claimed acts of cyber warfare. Similar to INTERPOL there should be vigilance and policing body which can observe and investigate the activity of private actors such as cyber media agency, transnational corporation, cyber hackers and terrorist organization. The gap between developed and developing country is also seen in cyberspace. Maximum ownership and controlling agency are from the developed world so there should be a global forum which can raise cyber and new media issue which are concerned with developing country.

References

1. Bell, David (2009), "On the Net: Navigating the World Wide Web", in Glen Creeber and Royston Martin (eds.) *Digital Culture: Understanding New Media*, Berkshire: Open University Press.

2. Berenger, Ralph D. (2006), "*Cyber media go to war*", Milwaukee: Marquette Books.

3. Berenger, Ralph D. (2006), "Introduction: War in Cyberspace", *Journal of Computer-Mediated Communication*, 12: 176-188.

4. Bunt, Gary R. (2003), "Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments", London: Pluto Press.

5. Carr, Jeffrey (2010), "*Inside Cyber Warfare*", Cambridge: O'Reilly Pub.

6. Christopher, J. Castelli (2008), "*Defense Department Adopts New Definition for Cyberspace*," Inside the Pentagon, 22 May 2008: http://www.insidedefense.com.

7. Corfu Channel (*United Kingdom of Great Britain and Northern Ireland v. Albania (1949)*), ICJ Reports.

8. Flew, Terry (2002), "*New Media: An Introduction"*, Oxford: Oxford University Press.

9. Jaeger, Charles W. (2004), "Cyberterrorism", in Hossein Bidgoli (ed.), *The Internet Encyclopaedia* (Vol. 1), New Jersey: John Wiley & Sons.

10. Jong, Wilma De et al. (2005), "Introduction," in Wilma De Jong et al. (ed.) *Global Activism, Global Media*, London: Pluto Press.

11. Lehto, Martti and Pekka Neittaanmaki (2015), "Cyber Security: Analytics, Technology and Automation", New York: Springer Pub.

12. Lindtner, Silvia and Marcella Szablewicz (2011), "China's many Internet: Participation and Digital Game play across a Changing Techonology Landscape", in David Kurt Herold and Peter Marolt (eds.), "*Online Society in China: Creating, Celebrating, and Instrumentalising the online carnival*, New York: Routledge Publication.

13. Maghaireh, Aladldin Mansour (2013), "Arbic Muslim Hackers: Who are they and what is their relationship with Islamic Jihadists and Terrorists," in K.

Jaishankar and Natti Ronel (eds.), *Global Criminology: Crime and Victimization in a Globalized Era*, New York: Taylor And Francis Group.

14. Manovich, Lev (2002), "*The Language of New Media*", London: The MIT Press.

15. Manu, Alexander (2010), "*Disruptive Business: Desire, Innovation and the Re-design of Business*", Surrey, UK: Gower Pub.

16. NATO Cooperative Cyber Defence Centre of Excellence (2013), "*The Tallinn Manual on the International Law Applicable to Cyber Warfare"*, Cambridge University Press (2013).

17. Quinn, Stephen (2009), "*Convergent Journalism: The Fundamentals of Multimedia Reporting*", New York: Peter Lang Pub.

18. Pollitt, M (1998), "Cyberterriorism – fact or fancy, Comput Frud Sector," 3 (2): 8

19. Schmitt, Michael N. (1999), "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law* 37: 885-997.

20. Secretary of Defense, Department of Defence Publications: National Military Strategy for Cyberspace Operation (NMSCo 2006) (http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-023.pdf pg. 3, accessed 26/08/2014).

21. Siapera, Eugenia (2012), "*Understanding New Media*", London: SAGE Publishing.

22. US Department of Defense: Dictionary of Military and Associated Term (Joint Publication 1 -02: 8 November 2010, as amended on 15 June 2014) pg. 64 (http://fas.org/irp/doddir/dod/jp1_02.pdf, 2014, accessed 26/06/2014)

23. Watkin, Kenneth and Norris, Andrew J. (2012), "*Non-international Armed Conflict in the Twenty-first Century*", Maryland: Military Bookshop.

24. Williams, Bruce A. and Michael X. Delli Carpini (2011), "After Broadcast News: Media Regimes Democracy, and the New Information Environment" New York: Cambridge University Press.

25. Winterfeld, Steve and Jason Andress (2012), "*The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in theory and practice*", Waltham: Syngress Press.

26. *The Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua V. United States of America (1986)), ICJ Reports,.

27. *Case Concerning the Gabcikovo-Nagymaros Project* (Hungary/Slovakia), (1997) ICJ Report 7

28. The Geneva Convention (on Law of War), 1949, [Online: Web] Accessed on 24 August 2014, URL: http://www.icrc.org/eng/assets/files/publications/icrc-002-0173.pdf

29. UNGA Resolution on combating the criminal misuse of Information Technologies (A/RES/55/63, 22 January 2001).

30. UNGA Resolution on combating the criminal misuse of Information Technologies (A/RES/56/121, 23 January 2002).

31. UNSC Resolution on the definition of cyber warfare, S/RES/1113 (2011), (http://www.upeace.org/upmunc/2011/pdf/SC%20Cyberwarfare.pdf)

32. Hague Convention (1907) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land.

33. http://unterm.un.org/dgaacs/unterm.nsf/WebView/99B98BDBCBAB096185256E620052EFD3?OpenDocument; 2014 (accessed 26/06/2014)

34. Indian Information Technology Act, 2000