ISSN: 2308-5096(P) ISSN 2311-620X (O)
[International Journal of Ethics in Social Sciences
Vol. 5, No. 1, June 2017]

Cyber Warfare and International Humanitarian Law : A Study

Mohammad Saidul Islam*****

Abstract

The technological advancement has made States, societies and individual fully dependent on computers, computer systems and internets and simultaneously made them vulnerable by broadening the scope of cyber-attacks. The cost effectiveness, easiness and safetyness of cyber attackers have significantly contributed to increase cyber attacks worldwide. The wider use of computers in many places including many dangerous and important installations like nuclear power plant, water dams, electric power grids, hospitals, oil and gas installations have fallen the people in a havoc danger in all time of cyber attacks. In this regard some important issues are unsettled yet namely, identification of the attackers, whether international humanitarian law applies in cyber attack. This study will not explore the technique of identification of cyber attackers which is the works of the scientists; it will only focus the most important controversial unsettled issue of contemporary world whether IHL applies in the cyber attacks.

Key words: *Cyber attack, cyber warfare, international humanitarian law, armed conflict, technological advancement.*

1. Introduction

With the development of new technologies the importance of the cyber space,[1] the virtual domain, is increasing rapidly day by day. States, societies and even individuals have become increasingly dependent on computers and internets. Our daily life, fundamental life, social

* Assistant Professor, Department of Law, International Islamic University Chittagong
Islamm.saidul@yahoo.com

1 Cyber space is defined as 'a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. Cyber space, then, goes beyond the internet and includes all networked digital activities. The United States contains a different definition of cyber space "a globally domain within the information environment consisting of the interdependent network of information technology infrastructures, including internets, telecommunications networks, computer systems and embedded processor and controllers'.

interactions and economics depend on information and communication technology working seamlessly. It has broken down the boundaries between States, communities and citizens, allowing interaction and sharing of information and ideas across the globe ('Cyber Security' 2013, p.2). Now a modern State cannot run even for a single day without using the cyber space as all the functions of a State are dependent on computer, computer technology, information, information technology, internet and so on.

In this twenty first century, information is the key coin of the realm and from nation state to individuals is increasingly dependent on information and information technology including computer and computer technology. Information technology is needed in every stage and step of modern life to conduct businesses, i.e., pay roll and accounting, recording inventory and sales and research and development, transportation, health care and financial services, manufacturing products in the factories more rapidly and efficiently, managing military forces, for distribution networks for food, water and energy. Even the terrorists also use cyber space to conduct their operations and it is also rapidly used in the battle fields and in many respects the states attack the enemy states and cause havoc damages to the infrastructures and civilians and military property (Lin 2012:516).

However, the more development of technology and dependence on it has promoted more possibilities of cyber attacks and more damages to the states and civilians. Cyber security[2] incidents are increasing at an alarming pace and disrupt the supply of essential services. The threats in the cyber space can have different origins including criminal hackers, individual groups, states, state motivated non-state actors, politically motivated groups, terrorists, non-state actors etc. On the basis of the origin of actions in the cyber space and gravity of the impact of the attacks, the cyber operations are classified as cyber crime, cyber attacks and cyber warfare. Different types of cyber actions are committed by means of computer systems by individuals, non-state actors or state is not a new concept in the cyber realm but recently various cyber actions (cyber crimes and cyber attacks) turn to the cyber warfare which is the matter of concern for the world communities. The cyber crimes are enormously committed by individuals but no acceptable definition has been given by any international convention. The inactiveness of the world communities to halt cyber crimes and difficulties to identify the makers of the crimes encouraged the cyber criminals to broaden the area of cyber crimes through developing their technologies, which lead them to commit cyber attacks and in course of time to carry out cyber warfare. On the other hand the Geneva Conventions and its Additional Protocols are also not clear whether international humanitarian law applies in the cyber warfare. This study is not going to focus on all the cyber attacks related unsettled

2 Cyber-security refers to the safeguards and actions which are taken to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.

issues, it highlights only one most important question whether international humanitarian law applies in the cyber warfare although most of international humanitarian law documents are silent regarding this question.

2. Definition of Cyber Warfare

The cyber warfare refers to those attacks which come within the definition of armed conflicts (Common article 2)[3] or resort to armed forces (*Prosecutor* v *Dusko Tadic*).[4] Though the analysts and experts anticipate that cyber attacks have grave and widespread economic and physical damages to the civilian population, yet, no document has been singed internationally giving a comprehensive defining of cyber warfare and prescribing provisions regulating the cyber warfare. Individual and groups have taken various initiatives to define cyber warfare and the most cited definition given by Richard and Robert (2010), cyber war is "actions by nation-state to penetrate in another nation's computer or networks for the purpose of causing damage or disruption." Hyden says that we don't call an attack a cyber war. Cyber war involves a deliberate attack to disable or destroy another country's computer networks. But how much damage would be done before a cyber operation could be considered as cyber war, yet to be settled (Tom 2010).

Rose (2010) says that cyber warfare is an internet based conflict where the state or individual groups being politically motivated attacks on information or information system of the enemy state. Cyber operations are operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance, to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system. By these means, a variety of 'targets' in the real world can be destroyed, altered or disrupted, such as industries, infrastructures, telecommunications, or financial systems.[5] Adam Liff mentions that cyber warfare is "... computer network attacks with direct political and/or military objectives ... distinct from cyber espionage, hacking, and crime." (Liff 2013)

Cyber warfare is always a cyber attack but all cyber attacks are not cyber warfare. A cyber attack becomes cyber warfare if the attack occurs with effects equivalent to the conventional armed conflict or occurring within the context of armed conflict, rise to the level of cyber warfare.

---

3 Common article 2, Geneva Conventions 1949 states that armed conflict is a conflict which may arise between two or more High Contracting parties, even if the state of war is not recognized by one of them.

4 ICTY, The Prosecutor vs Dusko Tadic, (1995) Para 70.

5 US Department of Defense, Dictionary of Military and Associated Terms, 8 November 2010 (as amended on 31 January 2011),Washington, DC, 2010: 'Computer network attacks are actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

3. Application of International Humanitarian Law in the cyber Warfare

It is an important question and matter of consideration for world communities whether international humanitarian law (IHL) applies in the cyber warfare. A cyber attack is cyber warfare if that attack amounts to an armed conflict, because international humanitarian law is applied only in international armed conflict (IAC) and in certain circumstances in non-international or internal armed conflict.[6]

Under common article 2 of the Geneva Conventions of 1949 an international armed conflict is a declared war or any other armed conflict which may arise between two or more states, even if the state of war is not recognized by one of them. On the other hand article 1 of Additional Protocol II of 1977 states that this protocol applies to all armed conflicts which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups.[7] These two articles make it clear that IHL applies in an armed conflict either international or non-international.

4. Armed Conflict

An armed conflict exists only if, there is any recourse of armed force by a State against another State, regardless of any reasons or severity or the intensity of this confrontation. Actually the existence of an armed conflict depends on what happens on the ground (ICRC, 2008, P.1). The view of ICRC commentary of Geneva Conventions is "any difference arising between two States and leading to intervention of armed force is an armed conflict."It makes no difference how long the conflict lasts or how much the slaughter takes place.[8] The most adopted definition pronounced by the International Criminal Tribunal for the former Yugoslavia in the *Prosecutor v Dusko Tadic* case, the Tribunal stated that "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a state."[9]

This study found that there are two types of armed conflict (i) international armed conflict which may be declared war or any other armed conflict between two or more states[10] or

6 Common art. 3 and art. 1, of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non- International Armed Conflicts (Protocol II)

7 Article 1, of Additional protocol II of 1977

8 See ICRC. Commentary of the Geneva Convention 1, art. 32. ICRC. Commentary of the Geneva Convention 11, art 28; ICRC. Commentary of the Geneva Convention 111, art 23; ICRC. Commentary of the Geneva Convention 1V, art 20.

9 ICTY, The Prosecutor *v.* Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para. 70.

10 Article 2, Common to all Geneva Conventions of 12 August 1949,

situations of partial or total occupation of the territory of a state party or fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination[11] and; (ii) non-international armed conflict. IHL, however, is applicable in the cyber attack if it amounts to an armed conflict or if it is done as a part of an armed conflict. It is quite uncontroversial that when cyber operations are conducted in the context of an ongoing armed conflict then they are governed by the same IHL rules as that of kinetic conflict, for instance, if in parallel or in addition to a bomb or missile attack, a party to the conflict also launches a cyber attack on the computer systems of its adversary, the IHL is applied both for bomb and missile attacks and cyber attacks. The problem arises regarding application of IHL in a distinct cyber attack.

5. Cyber Attack Amounts to Armed Conflict

Is a distinct cyber attack amounts to an armed conflict? In response to this question International Group of Expert opined, as used in the Tallinn Manual, armed conflict refers to a situation involving hostilities, and including those conducted using cyber means (Schmitt 2013: 75). Hostilities used in dual senses both as attacks and military operations. Attacks, according to article 49 of Additional Protocol I, mean acts of violence against the adversary, whether in offence or in defense.[12] Under article 49, an act to be an attack shall encompass violence, so by strict textual interpretation of this provision, non-kinetic operations, i.e., cyber operations which do not themselves comprise physical force, shall be excluded from the list of attack.

This concept was prevailing among the drafters, which is apparent from the comments of them. As noted in Bothe, Partsch and Solf's respected commentary on the provision: "the term 'acts of violence' denotes physical force" (Schamitt 2011). In views of the International Group of Experts an armed attack encompasses at least use of force (Schamitt 2011). Every use of force does not constitute an armed attack. Only that force constitutes armed attack in response to which the victim state can lawfully uses force for the self-defence. In *Nicaragua* case, the court noted that the scale and effects is the only criteria to distinguish force constituting armed attack and not constituting armed attack. It noted that it needs to distinguish the most grave forms of use of force (those constituting armed attack) from less grave forms of use of force (those not constituting armed attack).[13] The court did not prescribe

11 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978), Art. 1 (4)

12 Article 49(1), the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I).

13 Nicaragua Judgment, *para* 191.

any definition of grave forms of forces. Therefore depending on the judgment of *Nicaragua case* it can be said that a use of force reaches either at the level of an armed attack or not, depends on the scale and effects of the attack. The International Court of Justice in its *Nuclear Weapons Advisory Opinion* stated that a use of force to be an armed attack just to consider the effects of act is enough and it is regardless to consider the weapons employed.[14]

It is a widely accepted rule that the acts of violence do not refer only to the violence of means but it indicates the violence of consequences also (Schamitt 2002: 377). For example, it is a settled principle that the use of biological, chemical, or radiological agents would constitute an attack and prohibited under Geneva Protocol of 1925, even though the attack does not involve physical force (*Prosecutor* v *Tadic*).[15]

Therefore, cyber attack amounts to armed conflict as the consequences of a distinct cyber attack held in the real world not in virtual world and in many time the consequences of cyber attack are not less than those of traditional kinetic attack. As cyber warfare is conducted by software or software and hardware through internet in the virtual realm, it seems that it may cause damages to software which has no impact on the real world but cyber attack to the control systems of some important installations has a long term widespread impact on the civilians and civilians` objects which may result in injury and death of many civilians, even in some cases the consequences of cyber attack may be more ubiquitous and dangerous than those of the traditional kinetic attack, i.e., cyber attack in water barrage, manipulation of an air traffic control system etc. The followings are some examples when the effects of cyber attacks may be more dangerous and devastating in compare to traditional attacks by swords, boobs missile and so on.

6. Cyber Attack on Air traffic control system[16]

Among many highly critical installations, air traffic control system is the most dangerous installation as the attack on air traffic control (ATC) systems may cause violent damages to

14 Nuclear Weapons Advisory opinion, *para*, 37-50

15 See also, New York Times, 15 September 1988, at A 13; Washington Post, 20 September 1988, at A 21.) State Department Daily Briefing, 20 September 1988, Transcript ID: 390807, p. 8. New York Times, 16 September 1988, at A 11. *Hearing on Refugee Consultation with Witness Secretary of State George Shultz*, 100th Cong., 2d Sess., (13 September 1988) (Statement of Secretary of State Shultz, United States, Department of State, Press Guidance (9 September 1988).) . U.N. GAOR, 1st Comm., 43rd Sess., 31st Mtng., at 16, U.N. Doc. A/C.1/43/PV.31 (1988) 59 *British Yearbook of International Law* (1988) at 579; U.N. GAOR, 1st Comm., 43rd Sess., 4th Mtg., at 47, U.N. Doc. A/C.1/43/PV.4 (1988)(statement of 18 October 1988 in the First Committee of the General Assembly); U.N. GAOR, 1st Comm., 43rd Sess., 31st Mtg., at 23, U.N. Doc. A/C.1/43/PV.31 (statement of 9 November 1988

16 (ATC) is the "service provided for promoting safe, orderly and expeditious flow of air traffic, including airport, approach and en route ATC service. It depends on hardware and humans. The current ATC system depends primarily on ground based radars which direct and monitor aircraft flying along pre-determined, designated airways or essentially "aircraft highways in the sky.

the property and death to both civilians and military. The ATC system, especially Next Gen,[17] Autopilots[18] and transponders[19] are "dumb" hardware systems driven by computer code instructions written by human being, so it is possible for an attacker to override something the system is doing, usually in response to an emergency. These characteristics point to obvious vulnerabilities. For these vulnerabilities, an attacker can intervene in these systems in a harmful way. The most extreme case is the attackers after taking the control of airliner may direct a commercial airliner into some large office buildings as was done manually by onboard hijackers on 9/11, which may cause the death of many people and damage of many property.[20]

The cyber attack may successfully disable the air space control system, allowing for example, carpet bombing of the territory by hostile aircraft without any early-warning alarms being set off (Mele 2010). The high-risk situation arises when the attacker takes control over the computer, modifies the systems and steals data (Kirk 2009) which in some cases, resulting to collision between aircrafts. On the other hand these systems becoming compromised by cyber attack can cause problems for aircraft during take-off and landing. For instance, the Spanish newspaper El Pais carried the news that the investigating authorities of the Madrid air disaster of 2008 had discovered that one of the computer systems, which monitored technical issues on the aircraft, was infected by cyber attack which led to technical malfunctioning resulting to the crush of the air craft and death of 154 people. According to El Pais, an internal compiled

17 The Next Generation Air Transportation System is new air traffic satellite-based control system instead of ground based control system. So instead of an air traffic controller seeing an aircraft on his radar screen, when that aircraft is within radar range, every controller working anywhere in the US will be able to see every aircraft in US airspace. Next Gen uses area navigation and GPS technology to shorten routes, save time and fuel, reduce traffic delays, increase capacity, and permit controllers to monitor and manage aircraft with greater safety margins. Planes will be able to fly closer together, take more direct routes and avoid delays caused by airport "stacking" as planes wait for an open runway.

18 Autopilot refers to an airborne electronic system which automatically stabilizes aircraft about its three axes… restores original flight path following any upset, and … [follows a path] preset by pilot or remote radio control to cause aircraft to follow any desired trajectory. In advanced combat aircraft it receives signals from sensing and weapon-aiming systems enabling it to fly aircraft along correct trajectories to fire guns or other ordnance at aerial target or lay down unguided [and guided] bombs on surface target

19 Transponder is a "transmitter/responder; radio device which when triggered by correct received signal sends out pre-coded reply on same (rarely different) wavelength; received signal usually called interrogation, and reply usually coded pulse train." ATC controllers can ask a pilot to "swak ident" (identify their aircraft). The pilot presses the IDENT button on the transponder which sends out a signal and briefly brightens the aircraft symbol or blip on the controller's radar screen representing that specific aircraft. Specific transponder codes can also be transmitted to tell the controller the aircraft is being hijacked, has a radio failure, or has an emergency.

20 Publious. University of Calgary, seminar on Cyber War, paper presented by Publious, on A "9/11" Cyber Attack Using the US`s New Air Traffic Control System (Next Gen), available at : http://uofccyberwar.blogspot .com/ accessed on July 2014.

by the airline company revealed that the computer, which is situated at the Palma di Majorca headquarters of the airline, should have recognized at least three technical problems with the aircraft which, had they been correctly diagnosed by the server, would not have been allowed to take off. The Trojan virus, therefore, despite not having directly caused the incident, could have contributed to allowing an aircraft which should never have left the ground to do so (Mele 2010).

7. Cyber Attack on Fully-Automated Subway Control Systems

In these systems the conductors or drivers are not required to be present in the trains to run the trains but it is driven automatically by "VAL" systems.[21] Like the VAL systems, some other driverless metro systems like Docklands Light Railway, Vancouver`s sky train etc, which are under the threat of cyber attack and by attacking on the security systems, it is possible to make collision between two trains or may cause individual trains to derail or travel beyond the end of the line, which may result the havoc losses of human lives (Prosecuting criminal crimes 2010). Professor David Stupples (BBC News 2015) says that cyber attack may cause major disruption in the functioning of train and alter the way the train will respond.

8. Cyber Attack on Nuclear Plants Control System

Another dangerous installation is the nuclear plants. The cyber attack on this installation may cause catastrophic damages to both human lives and property. Cyber attack on nuclear plants, which may in extreme cases, results to the release of radiation leading to consequent loss of lives, radiation sickness and psycho-trauma, extensive property destruction and economic upheaval (Maurizio et al. 2012). In addition to the external loss and damage, the cyber attack may cause havoc damages to the nuclear plant which is a great loss for the attacked State. For instance, the stuxnet virus, which attacked the uranium enrichment plant of the Islamic Republic of Iran at Natanz, between late 2009 and early 2010 with the purposes of the total destruction of all the centrifuges in the FEP, Stuxnet failed. It was reported that the stuxnet attack, as reported in the press was launched by USA and/Israel, succeeded to lead to the destruction of at least a thousand centrifuges (David et al. 2010). Earlier after the attack, many commentators opined that IHL would not be applied for such an isolated cyber attack without any kinetic attack but later on most of the commentators including Michel N. Schmitt concluded the debate stating that such type of cyber attack amounted to armed conflict as the stuxnet virus is reported to have caused physical destruction of about one thousand IR-1 centrifuges which had to be replaced at the uranium enrichment facility at Natanz (Droege

21 VAL is a type of automatic rubber-tired people mover technology, based on an invention by Professor Robert Gabillard. It was designed in the early 1980s by French Matra, for the then new metro system in Lille. The VAL design uses platforms that are separated from the rollways by a glass partition, to prevent waiting passengers from straying or falling onto the rollways.

2012: 547). The networks attacked on Georgia in August 2008 is another good example of cyber attack which is considered as the first instance of a coordinated traditional and cyber war for the application of IHL. The attack on Estonian networks which did not amount to armed conflict nor it seemed as cyber war where IHL can be applied as its consequences did not reach to the level of armed conflict (Zhang 2012: 801).

In addition to abovementioned cases, there are many more installations which are under the threat of cyber attacks and although the attacks do not constitute any damage to the physical infrastructures of those installations but disrupt the proper functioning which may lead to severe damages and losses to the people. It is true that the effects of such bloodless means and methods of warfare might not be the same as the kinetic weapons as used in the traditional warfare, yet, in some cases it may be more severe than bombing and shelling. For example, the manipulation of electrical grid management system, opening the floodgates of dams, causing trains to collide, shutting down the banking systems, interrupting in gas and oil pipelines, attacking on hospital electronic systems etc. The cyber attack on electricity grid management systems, at this age of technology, is a big threat for every peace loving state because each and every important installation depends on electricity for its running. The malfunctioning of electricity grids will throw the state in the darkness stopping the functions of governments, computers, trains, aircrafts, hospitals, telecommunication services, nuclear plants, banking services etc. Though the attack will not cause any physical damage to the electrical grids but it will cause a lot of immeasurable losses and sufferings to the people.

Lin (2012: 524) mentions that what will constitute an armed attack in cyberspace? is that if a cyber attack causes the same effects as a kinetic attack that rises to the threshold of an armed attack, the cyber attack will itself be considered an armed attack. Schmitt (2011: 6) opines that cyber operation, like any other operation, is an attack which may result in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.

The study found that the effects or consequences of a distinct cyber attacks in certain cases may be more dangerous and devastating in compare to the traditional warfare. It also found that where the scale and effect of devastation of a cyber attack is equal to or more than that of a kinetic warfare there cyber attack amounts to an armed conflict or when cyber operations cause severe damage to the property and cause death of individuals, it amounts to an armed conflict.

9. Conclusion

The study can be concluded by the statement that IHL applies in a distinct cyber attack where that attack amounts to an armed conflict. A cyber attack becomes an armed conflict when it causes severe damages to property and death of human beings. The cyber attacks on the

nuclear power plant, electric power grids, water dams, air traffic control systems, fully automated subway control system and so on may cause severe damage to property and deaths of many persons. Considering the effects of cyber attacks many countries including the US, (Koh 2012) the United Kingdom of Great Britten and Northern Ireland,[22] and Australia,[23] have stated that IHL applies to cyber warfare. China`s stance on the application of IHL in cyber warfare is that the nations of the world should cherish the value of cyber space–the first social space created by humankind and should firmly oppose the militarization of the internet. Its view is that the current UN Charter and the existing laws of armed conflict as well as the basic principles of international humanitarian law that relates to war and the use or threat of force all still apply to cyberspace (Zhang, 2012). The opinions of many experts, views of many countries and the aforesaid justifications indicate that international humanitarian law applies in cyber warfare or cyber attacks when it amounts to an armed conflict.

References

BBC News, (2015). Westcott Richard, 'Rain Signal Upgrade Could be Hacked to Cause Crushes' April 24, 2015.

'Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace' (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, p. 2.

David, Albright. Paul, Brannan and Christina Walrond. (2010). 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment'. *ISIS report* (Institute for Science and International Security), viewed 12 November, 2013, http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Droege, Cordula. (2012) . 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians'. In: Vol. 94, No. 886 *International Review of Red Cross,* Avenue de la Paix : Geneva, p.547.

International Committee of the Red Cross. (2008). 'How is the Term "Armed Conflict" defined in International Humanitarian Law?'. (ICRC) Opinion Paper, p. 1.

Kirk, Jeremy. (2009). Study: 'US Air Traffic Control Vulnerable to Cyber Attack'. http://www.pcworld.com/article/164501/article.html

22 Report of the Secretary-General, 23 June 2004, UN Doc. A/59/116, p. 11; Report of the Secretary-General, 20 July 2010, UN Doc. A/65/154, p. 15.

23 Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security, 15 July 2011, UN Doc. A/66/152, p. 6.

Koh, Harold. (2012). 'International law in cyberspace'. In: the US Cyber Command Inter-Agency Legal Conference, available at: http://opiniojuris.org/2012/09/19/harold-koh-on- international-law-in-cyberspace/; Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security, 15 July 2011, UN Doc. A/66/152, p. 19. US Department of Defense Strategy for Operating in Cyberspace: 'Long-standing international norms guiding state behaviour–in times of peace and conflict–also apply in cyberspace.

Liff P. Adam. (2013). 'The Proliferation of Cyber warfare Capabilities and Interstate War, Redux: Liff Responds to Junio'. In: Vol. 36, No. 1*Journal of Strategic Studies*

Lin, Dr. Herbert.(2012). 'Cyber Conflict and International Humanitarian Law'. In: Vol. 94, No. 886 *International Review of the Red Cross*, Avenue de la Paix: Geneva, p.516.

Maurizio, Martellini, Dr Thomas, Shea and Dr. Sandro, Gaycken. (2012). *'Cyber Security for Nuclear Power Plants'*. US Department of State, Washington D.C. Viewed 11November 2013 http://www.state.gov/t/isn/183589.htm

Mele, Stefano. (2010). '*Cyber warfare and its damaging effects on citizens*'. available at: http://www.stefanomele.it/public/documenti/185DOC-937.pdf

Prosecuting Criminal Crime. (2010). 'Computer Crime and Intellectual Property Section, Criminal Division, US Department of Justice, 2nd Edition.

Richard, A. Clarke & Robert, K. Knake. (2010) . 'Cyber War: the next Threat to National Security and What to Do About it'. http://www.amazon.com/Cyber-War-Threat-National-Security/dp/0061962244

Rose, Margaret. (2010). 'Cyber Warfare'. *Tech Target*, http://searchsecurity.techtarget.com/definition/cyberwarfare

Schmitt N. Michel. (edit.). (2013). '*Tallinn Manual On the International Law Applicable to Cyber warfare'*. Cambridge University press, (2013) p. 75, prepared by International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence.

__. (2011). 'Cyber operations and the Jus in bellow: Key Issues'. In: Vol. 87 *Naval War College International Law Studies* , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1801176

__. (2002) 'Wired warfare: computer network attack and jus in bello'. In: Vol. 84 No.846 *International Review of the Red Cross*, p. 377.

Tom, Gjelten. (2010). 'Extending the Law of War to Cyber space'. Viewed 15 September 2013. http://www.npr.org/templates/story/story.php? storyId=130023318

Zhang, Li .(2012). 'A Chinese perspective on cyber war'. In: Vol. 94, No. 886 *International Review of the Red Cross*, Avenue de la Paix: Geneva, p.801.