ISSN- 2394-5125 VOL 7, ISSUE 01, 2020

REVIEW ON CYBER LAW

Mincy Vinod Satija [1] Dr jayendra singh Rathor[2]

[1]Research Scholar ,Law Department , Kalinga University, Raipur

[2] Prof. , Law Department , Kalinga University, Raipur

Abstract

Internet is the fastest technique on earth that one can find these days and for everything it is the best solution that people consider looking into. It has all the benefits and advantages like communication, advertisement, online movie and songs downloads, emailing, instant messaging and searching out the concerns and issues, there are plenty of things that internet has got wrong as well. There are different kinds of internet scams and frauds that are happening, proposing an utmost caution and care. This is something that has been bothering individuals and organizations ever since internet was introduced and many a time, simple things could make any one victim when the person is unaware of it.

Keyword information of law, Cyber crime , Human rights, Challenges in law

Introduction

Only cyber-attacks with effects equivalent to those of a conventional ―armed attack, occurring within the context of armed conflict, rise to the level of cyber-warfare. Apart from the four traditionally functional domains land, air, sea and space another domain cyberspace have been identified due to the augmented cyber warfare. So United States created the US cyber command that coordinates the functional operations of Army, Navy and Airforce. Further, the million dollar question is should the authors of the cyber warfare or the technical person physically involved in the act of the cyber-attack, need to be considered as the combatant in this particular warfare and also if the principles of Jus ad Bellum like the legitimate authority just cause/right intention, Possibility to success, proportionality and the last resort can be considered as the role played by the international law on armed conflicts or on uses of force becomes meagre in the cyberspace rather than in the physical world. The thesis reviews the issue of cyber-attacks and international law in terms of jus ad bellum, the law concerning the recourse to force by states. The thesis takes the view that the existing rules on the use of force, namely s Article 2(4) and Article 51 of the United Nations Charter and the corresponding rules of Customary International Humanitarian Law apply to attacks regardless of the way they are carried out and thus, they apply to cyber-attacks as well. Some of the examples of different kinds of cyberattacks are presented to illustrate the issue: the attacks against Estonia in 2007 and Stuxnet, the malware that targeted Iranian nuclear facilities and was discovered in 2010.

Literature Review

"M. Libicki, ***What is Information Warfare",*** The author in the book is of the opinion that information warfare has subsumed a great importance in the age of technology and the state which has mastered the techniques of information warfare will, therefore, find themselves at an advantage over those who have not. He further argues that information warfare will relegate other traditional and conventional forms of warfare to the side-lines. He is of the opinion that information warfare, as a separate technique of waging war, does not exist. There are, instead, several distinct forms of information warfare and cyber warfare is one of them. Information is not in and of itself a medium of warfare, except in certain narrow aspects (such as electronic jamming). Information superiority may make sense, but information supremacy (where one side can keep the other from entering the battlefield) makes little more sense than logistics supremacy.

"Jeffrey Carr, *Inside Cyber Warfare*", The author has defined cyber warfare as the art and science of fighting without fighting; of defeating an opponent without spilling their blood. The author has further provided fascinating and disturbing details on how nations, groups, and individuals throughout the world increasingly rely on Internet attacks to gain military, political, and economic advantages over their adversaries. The author has further focused on the complex domain of the cyberspace along with the players and the strategies that are adopted by these players. The author further states that sophisticated hackers work on behalf of states or organized crime patiently play a high-stakes game that targets their victim, regardless of affiliation or nationality.

"John Arquilla and David Ronfeldt, *Cyber war is Coming",* The authors argue that a situation of the netwarwasenvisaged with the advent of the technology. The current situation of netwar is owing to the transition that warfare was going on post-cold war era. The author defines Cyber war as conducting and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to ―know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the ―balance of information and knowledge‖ in one‗s favour, especially if the balance of forces is not. It means using knowledge so that less capital and labour may have to be expended.

"Dorothy Denning, *Information Warfare, and Security*",The author of this book provides a framework for understanding and dealing with information-based threats such as computer break-ins, fraud, sabotage, espionage, piracy, identity theft, invasions of privacy, and electronic warfare. The author has driven from her analysis of information warfare and operation carried out during the Gulf war. She defines information warfare consisting of offensive and defensive operations against information resources of a win-lose nature. The author has proposed sound advice for security practices and policies and laid stress on the countermeasures that are both possible and necessary against information warfare.

"R. Parks, D. Duggan, *Principles of Cyber warfare, Security Privacy",* The authors in this article argue that kinetic warfare is inherently distinct from cyber warfare and some principles of kinetic warfare have no application in the context of cyber warfare. He has further proposed some additional principles since the principles of warfare are not applicable to the cyber warfare owing to the unique nature of cyberspace. He has further definedcyber-warfare is the subset of information warfare that involves actions taken within the cyber world.

"P. Cornish, D. Livingstone, D. Clemente, C. Yorke, *On Cyber Warfare*",The authors in this report after identifying the essential characteristics of cyber warfare as a strategic phenomenon by describing the actions of cyber-attackers and the reactions of defending governments and by

analysing the _ends, ways and means' of cyber warfare put forth the definition of the cyber warfare as a conflict between states which could also involve non-state actors in various ways. The author further argues that in cyber warfare it is extremely difficult to direct precise and proportionate force because the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.
"Dorothy Denning, *Cyber security's Next Phase: Cyber Deterrence*", Dorothy Denning starts explaining the two main principles of deterrence in case of Cyberwarfare: denial and Punishment. Then author moves forward to explain the reasons why cyber deterrence is hard to implement. Moving further the author proposes three ideas which can be used to strengthen cyber deterrence. She states that if we improve our cyber security, employ active defences and establish international norms for cyberspace then we can strengthen cyber deterrence. She says that if the active cyber defence is employed then it can unmask the people behind the cyber-attack. .

"Amir Lupovici, *Cyber Warfare And Deterrence: Trends and Challenges in Research*",
In this, the author puts forth the necessary conditions that are required for asuccessful strategy of deterrence. The author begins with defining the different strategy of deterrence which a country can adapt to prevent their enemies from taking undesirable action by way of cyber-attack. The author describes punishment, capabilities, the credibility of the threat, and effective delivery of messages as some of the conditions for ba successful strategy of deterrence. The author argues that successful deterrence in cyber warfare can be created if the country adopts retaliation as one of the cybersecurity policies.

" Will Goodman, *Cyber Deterrence Tougher in Theory than in Practice?*",
The author argues that though there are many kinds of literature available consisting nothing but the theories on cyber Deterrence there is nothing to test those theories. Due to the lack of critical analysis of case studies, the efficacy of cyber deterrence cannot be determined. The author of this research paper has sought to augment the current literature by analyzing the generally agreed upon issues of cyber deterrence with the cases wherein cyber deterrence failed. The author in this evaluated only cases of suspected state –instigated cyber-attack because he considers that states are the preeminent actors in cyberspace, therefore deterring state-based attacks are going to yield the greatest benefit to overall security.

" Martin C. Libicki, *Cyber Deterrence and Cyber Warfare",*
The author in this book has tried to find out the answer whether it is possible to apply deterrence theory as a preventive measure in case of cyber-attack. The author examines two deterrence strategies available to non-states- punishment and denial in the light of cyber warfare. He concluded that both the deterrence strategy lacks credibility. Denial lacks credibility due to immature international legal frameworks, the absence of inspection regime and perception that are not dangerous enough to merit deterrence. Punishment strategy lacks credibility due to the daunting challenges of the cyber-attack attribution and asymmetry.

" Eric Talbot Jensen, *Cyber Deterrence.*",
The author argues that cyber deterrence offers much more flexibility and increased options from traditional deterrence methodologies developed in the Cold War's nuclear age. The author has further discussed the strategies of cyber deterrence such as traditional retaliation and has

discussed six prominent theories of cyber deterrence and briefly analysed legal issues associated with this vital area of national security. The author is of the opinion that cyber deterrence includes options such as taking legal action and making networks invisible, resilient, invulnerability and interdependent.

"Michael N Schmitt, *Classification of cyber conflict*",

The author of this is of the opinion that the emergence of the cyber warfare has complicated the classification of the armed conflict. They are also inherently transborder, thereby frustrating any approach to classification based on geographical factors.b Yet, the author argues that he will not consider the possible emergence of new categories ofb armed conflicts, such as "transnational armed conflict." Rather he has adopted a conventional approach, one acknowledging two basic genres of conflict international and non-international. He argues that classification of cyber operation falls with the accepted framework.

"Noah Simmons, *A Brave New World: Applying International Law of War to Cyber-Attacks*",

The author in this argue that cyber-attacks do not fit under the conventional analyses of "use of force" and "armed attacks" under the UN Charter, and no satisfactory approaches have been put forth to treat cyber-attacks. He has proposed a definition of an armed attack as a state's kinetic or virtual use of force made with the intent of altering a target country's sovereign or strategic power by significantly disrupting its military, critical, or strategic infrastructure. The author has put forth a test to determine whether cyber-attacks constitute a "use of force" and "armed attack" that reflects the traditional goals of the UN Charter while taking into account the present realities of the use of cyber-attacks. The author argues that cyber-attack will constitute an armed attack if a state has launched a kinetic or virtual with the intent of altering a target country's sovereign or strategic power by significantly disrupting its military, critical, or strategic infrastructure.

" Michael N. Schmitt, *Cyber Operations and the JusAd Bellum Revisited*",

The author argues that states resort to the countermeasures to respond to cyberattacks that do not reach the level of an armed attack. He opines that many cyber activities which do reach the threshold of an armed attack still amount to an "internationally wrongful act" justifying countermeasures. This includes placing malware on a system, hacking into a network, and destroying data all violate a state's sovereignty, and abuse the principle of non-intervention. He concludes that countermeasures are an adequate way to respond to attacks that do not qualify as an armed attack

Conclusion - The first and foremost suggestion is that the developing of an early warning system will be helpful in repealing and avoiding a lot of the cyber-attack that are directed towards the critical national infrastructure. Effective legal framework in the cyber domain, at international level need to be adopted that can complement in the application of principle of deterrence in cyber space and to take stringent actions against the violators of the peace and tranquility of the cyber space. Secondly it is suggested to the states to come up with the devices and techniques that support in attributing the cyber-attack to the perpetrator**.**

References

1. Abbate, J. (2000). Inventing the Internet. MIT Press.

2. Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning .
3. Animesh Sarmah, Roshmi Sarmah & Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Law's of India, Int. Res. J. Eng. Technol. (2017).
4. Brenner, W. Susan (2010). Cybercrime: Criminal threats from cyber space. Green Wood Publishing Group, Westport.
5. Carr, J. (2012). Inside Cyber Warfare: Mapping the Cyber Underworld. 2 nd ed., O'Reilly Media.
6. Clarke, R. A. and Knake, R. (2010). Cyber War: The Next Threat to National Security and What to do about it. Reprint ed., Ecco.
7. Cyber Crime Lawyers in Delhi, India, https://cybercrimelawyer.wordpress.com?category/66-c-punishment-for-identity-theft/ .
8. Cyber Laws in India, http://cyberlawsinindia.net/black-html .
9. Cybercrime Definition, http://cybercrime.org.za/definition .
10. Denning, D. E. (1999). Information Warfare and Security. 1 st ed., Addison Wesley ProfessionaL.
11. Dinstein, Y. (2011). War Aggression and Self Defence. 5 th ed.,Cambridge University Press.
12. Distefano, G. (2014). Use of Force, The Oxford Handbook of International Law in Armed Conflict.Oxford University Press.
13. Draper, G.I.A.D. (1998). Reflections on Law and Armed Conflicts: The Selected Works on the Laws of War. Martinus Nijhoff Publishers.
14. Email Spoofing: https://www.techopedia.com/definition/1664/email-spoofing .
15. Encyclopedia Britannica, https://www.britannica.com/EBchecked/topic/130595/Cyber crime.
16. Freedman, L. (2004). Deterrence. 1 st ed., Polity Press.
17. Gardam, J. G. and Jarvis, M.J. (2001). Women, Armed Conflict and International Law. Cambridge University Press.
18. George, A. and Smoke, R. (1974). Deterrence in American Foreign Policy: Theory and Practice. New York: Columbia University Press.

19. Gillies, J. and Cailliau, R. (2000). How the web was born: The story of the World Wide Web. Oxford University Press.
20. Gupta, M.P., Kumar, P. and Jaijit, B. (2004). Government Online: Opportunities and Challenges. Tata McGraw- Hill, New Delhi.
21. Hafele, D. M. (2004). Three different shades of Ethical Hacking: Black, White and Grey. February 23, 2004.
22. Halder, D. and Jaishankar, K. (2011). Cyber- Crime and the Victimization of Women: Laws, Rights and Regulations. 1 st ed., IGI Global.
23. Hammes, T. X. (2004). The Sling and The Stone: On War in The 21st Century. St.Paul, MN Zenith Press.
24. Higgins, A.P.(1912). War and The Private Citizens. Oxford University Press.
25. Higgins, George (2010). Cybercrime: An Introduction to an Emerging Phenomenon. Mc Graw Hill Publishing, New York.
26. Holt, Thomas J. (2011). Crime Online: Correlates Causes and Contexts. Caroline Academic press, USA
27. Howard A Davidson & Gregory A Loken, ChUd Pornography and Prostitutuon Back.ground and legal Ana!ysis (1987).
28. http://www.yourdictonary.com/cyberpornography .
29. Kuehl, D. R. (2009). Cyberpower and National Security. 1 st ed., Potomac Books and 1630 Defence University.
30. Law and Practice. Cambridge University Press.
31. Libicki, M. (1995). What is Information Warfare? National Defence University.
32. Libicki, M. C. (2009). Cyber Deterrence and Cyber Warfare. Rand Corporation.
33. LulzSec: what they did, who they were and how they were caught LulzSec | The Guardian,
https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail
34. Luvaas, J. (2001). Napoleon on The Art of War. New York, The Free Press.
35. Mccoubrey, H. (1998). International Humanitarian Law: Modern Development in The Limitation of Warfare. 2nd Revised ed., Dartmouth Publishing Co. Ltd.
36. Mearsheimer, J. J. (1983). Conventional Deterrence. Cornell University Press.

37. Meron, T. (1998). Bloody Constraint: War and Chivalry in Shakespeare. Oxford University Press.
38. Modh, S. (2010). Introduction to Disaster Management. Macmillan, New Delhi.
39. Moore, J. B. (1906). A Digest of International Law. Washington: Gov. Print. Off.
40. Morgan, P. M. (2003). Deterrence Now. Cambridge University Press.
41. Nadav Morag, Cybercrime, Cyberespionage, And Cybersabotage: Understanding Emerging Threats (2014), www.cnbc.com/id/101605470# (last visited Aug 20, 2021).
42. Nippold, O.(1923) The Development of International Law After the World War. At the Clarendon Press.
43. Oppenheim, L. (1921). International Law: A Treaties. 3rdedn. Longmans Green and Co.
44. Reed, T. C. (2004). At the Abyss: An Insider's History of the Cold War. New ed., Presidio Press.
45. Republic Act No. 9775 An Act Defining The Crime Of Child Pornography, Prescribing Penalties Therefor And For Other Purposes.
46. Roscini, M. (2010). World Wide Warfare- Jus Ad Bellum and The Use of Cyber Force. Max Planck, Yearbook of United Nations Law.
47. Ruys, T. (2010). Armed Attack and Article 51 of The UN Charter: Evolution in Customary.
48. SANS Information Security White Papers, https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-grey-1390 .
49. SANS, https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-grey-1390 .
50. Schmidl, M. (2009). The Changing Nature of Self-Defence in International Law. Nomos.
51. Scott, J.B. (1909). The Hague Peace Conference of 1899 and 1907. Baltimore, Johns Hopkins Press.
52. Sharp, W.G. (1999). Cyberspace and The Use of Force, United States, Aegis Research Corporation.

53. Shimshoni, J. (1988). Israel and Conventional Deterrence: Border Warfare from 1953 to 1970. 1 st ed., Cornell University Press.
54. Shin, B. (2008). International Law And The Use Of Force: Shaping The UN Charter And Its Evolution. Seoul, Republic of Korea, KIDA PRESS.
55. Shrivastava, M. (2013). Re- Energizing Indian Intelligence. 1 st ed., vij books (India) Pty Limited.
56. Simma, B. (1994). The Charter of United Nations: A Commentary. 3 rd ed., Oxford University Press.
57. Singer, P. W. and Friedman, A. (2014). Cyber Security and Cyber War- What Everyone Needs to Know. Oxford University Press India.
58. The Jargon Dictionary on website, http://www.netmeg.net/jargon/terms/c/cracker.html .
59. Varghese, Grace (2016). A Sociological Study of Different Types of Cyber Crime. International Journal of Social Science and Humanities,4(4), 599-607.