Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 2): pp. 3614-3622
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.02.377

Overview On International Level Cyber Warfare Study

Mincy Vinod Satija Research Scholar ,Law Department , Kalinga University, Raipur.

Dr jayendra singh Rathor Prof. , Law Department , Kalinga University, Raipur.

Abstract Cyber warfare as already established in the previous chapter is the act of hostilities in the cyberspace through cyber means and method which is analogous to the military hostilities that are conducted in the situations of the armed conflict. The unique nature that is associated with the cyber operations such as the dual use and the nature of the cyber arsenal and the effects generated by their use makes it a daunting task to govern such hostilities under the current framework of the international humanitarian law. Yet, any armed attack or an attack whose effects tantamount the effects of the traditional military weapons having uncontrollable effects, directed indiscriminately, in the international as well as non-international armed conflict are prohibited under the international law of war. With the terms incidental and related to the cyber operations defined and the differences between the different kinds of cyber operations enunciated the chapter further moves on with discussing the major cyber events that occurred in the past few decades and an attempt will be made to classify the cyber events as the cyber operations or an act of warfare that crosses the threshold of the use of force.

Keyword-Cyber Warfare , Global Senario, Law in force.

Introduction

The information within the computer network doesn't solely pertain to the matters of the national security however conjointly pertains to the social, economic, psychological, aspects of the individuals UN agency ar the benign actors within the computer network. because of the diversification of the facilities, and ease offered by the computer network it's become additional and additional jammed ever since. the quantity of actors has raised within the computer network. This has created them vulnerable to the assorted cyber-crimes, like phishing, spoofing and varied cyberattacks. Being a victim of the instances of cyber warfare and involuntary participation of
the benign actors within the cyber warfare has crystal rectifier to the gross violations of the principles of the international humanitarian law.

Literature review

Cyber-attack by the United States America

The CIA embedded software that is used to run valves, pipelines, turbines, in the critical cyber infrastructure of the Soviet Union in 1982. The software was a logic bomb designed to cause the pump speed and the valve settings to malfunction. This operation was authorised by the then president of the United States Reagen. "The result was the most monumental non-nuclear explosion and fire ever seen from space." This attack caused huge economic and psychological impact on the Soviet Union and is credited with being the cause of the end of the cold war.

The invasion of Iraq in 1991 is yet another example of the cyber warfare. The United States applied cyber warfare means and method for the invasion. The United States used its communication and the satellite systems extensively in this operation. The invasion involved the strategic air campaign and strikes against airfields and air crafts, telecommunication facilities, air defence and command and control systems.

Russia and Chechnya

This was another incident of cyber warfare where the pro-Russians and the pro-Chechen waged a virtual warfare in the cyberspace. The warfare was aimed at controlling and shaping the public perception with the object of uniting the Chechen diaspora. The Chechen hackers and separatist are a pioneer in the use of the cyberspace as a tool to deliver influencing PR messages. This skilful placing of propaganda and other information helped the Chechens in the furtherance of their object. Yet again, the Russians and the Chechens engaged in the cyber warfare during the second Chechen war in 1997-2001. The Russians invaded the breakaway region of the

Chechnya with the intent establish Moscow friendly regime. The propaganda that was spread was not pro Chechen but anti-Russian as several images depicting the military excesses of the Russians were circulated online. In an instance when the Russians officials denied the involvement in attacking and killing passengers on the bus, a video surfaced online refuting their claim. The Russians officials have been accused of hacking the Chechens websites and escalating the cyber conflict.

Kosovo and the U.S.A.

When the NATO started air strikes against Serbia in 1999, the anti-western groups such as Black Group and other pro-Serbian hackers started targeting the cyber infrastructure of the NATO. However, it could not be established if these hackers have any affiliation with the Yugoslav military. But, the object was to interrupt NATO from carrying out the strikes against Serbia. The US retaliated by hacking into the cyber infrastructure of the Air defence control system of Serbia to facilitate the air strike. This was the first broad-scale cyber warfare in the last century.79

Israel and Palestine

Israelis hacked into the websites of the Hezbollah, Hamas and Palestinian National Authority and launched a DDoS attack which jammed their websites in fall of 2000. This minor attack culminated in thefull-scale cyber war when Palestine and other Islamic supporting organisation called for a Cyber Holy War.The Palestine hackers hacked into the websites of the Israeli Parliament, defence force systems, stock exchange and the Prime Minister‟s office. Within 6 months of time, more than 150 websites of the Israel and 30 websites of Palestine has been targeted. The websites belonging to Israel were defaced and the hackers claimed that they can shut down the Israeli ISP Neti Vision that is responsible for hosting more than 60% of the internet traffic in Israel.

Estonia and Russia

Estonia is considered to be the most advanced nations in terms of ICT such that even the votes in the elections are cast through the PC. The majority of the banking and financial transactions in Estonia are carried out online. This reliance of Estonia on the internet brought it in the radar of the Russian hackers. The Russian hackers launched DDoS attacks against Estonia and increased the traffic by flooding the websites with the data such that the websites that normally received 1000 visits a day now reported receiving more than 2000 visits per second.81 The government websites and servers were flooded with the excess of traffic which the servers were incapable of handling thereby leading to the shutdown. The government of Russia denied any involvement in these attacks but the Estonian officials assert that Kremlin was behind these attacks. However, the situation was stabilised by the teams of the computer expert sent by USA and NATO. Later, this attack led to the establishment of Cooperative Cyber Defence Centre of Excellence in Estonia in May 2008. The aim of this agency is to coordinate cyber defence and aid the allies in the cross-jurisdictional attacks. This attack violated the principles of international humanitarian law as it was not launched without a just cause nor did it follow the principles such as discrimination, proportionality.

Israel and Syria

The Israelis launched an air strike against a nuclear reactor in Syria during operation Orchard in 2007. The Israelis hacked into the Syrian air defence system and disabled it temporarily to enter the Syrian airspace undetected. This air strike and the cyber-attack was in furtherance of the failed diplomatic efforts to stop the collaboration of North Korea and Syria in developing nuclear weapons.82 The strikes were legitimate as it was undertaken as last resort when the diplomatic efforts failed. This pre-emptive strike was targeted against the military object to render the defensive forces helpless withoutthe destruction of civilian life and property.

Lithuania

Consequent to the declaration that curtailed the freedom of speech and expression and assembly in 2008 such that the displaying Soviet and Nazi German insignia, such as the hammer and sickle, the red star, and the swastika, as well as playing of the Soviet and Nazi anthems at public gatherings were prohibited. This attracted widespread criticism from Russia and soon after this declaration many government and corporate websites in Lithuania were hacked and the Soviet era graffiti were displayed on the websites. This suggested that Russian hackers were behind this cyber operations.83

Russia and Georgia

This is the classic example of warfare where the battle was engaged in land, airsea and cyberspace. When Russia invaded Georgia in response to Georgia‟s attack against the separatist in South Ossetia in 2008, a highly coordinated but the decentralized cyber campaign was launched against the Georgian government websites and other critical cyber infrastructure including the embassies of the US and Britain. The object of these attacks was to support the invasion of Georgia by Russia and the cyber-attacks added to the military style invasion. The cyber-attacks were legitimate since they were primarily aimed at disabling the disabling the control and command of military capacities of the government.

Russia and Kyrgystan

This is another classic example of the cyber-attack launched against a country by Russia. The hackers attacked the service providers by the DDoS and soon brought the internet to a halt in 2009. The IP addresses were traced back to the hackers in Russia however, the intent and the motive behind the attacks remain unclear. It is speculated that it could have been due to the tensions between the administration and the differing views of the opposite party pertaining to the national policies. The attack could also have launched by the Russian supporters over a dispute pertaining to the US access to the Manas air base in Kyrgyzstan.

South Korea and the U.S.A.

Several DDoS attacks were launched against critical national infrastructure and websites of the USA and South Korea. The targets included government and commercial websites along with the Korean Assembly, the US and South Korean presidents‟ websites, the US State Department, the public websites for the US stock exchanges NYSE, and NASDAQ, the popular sites in South Korea such as „naver.com.‟ these attack occurred from July 4 to July 10, 2009. The timings of the attack suggested that North Korea was behind these attacks since North Korea tested a missile on the 4th of July and celebrated the 15th anniversary of Kim Sung‟s death on the 8th of July. However, the real motive behind the attacks is not clear.

Iran

The centrifuges of the Iranian nuclear facility were sent spinning out of control in 2009 by a cyber-worm known as Stuxnet that was released in a number of countries. This attack

substantially damaged the Iranian nuclear program. Although this was in violation of the nuclear-proliferation treaty, this did not violate any international humanitarian law since the attacks were undertaken as last resort after failed diplomatic attempts to deter Iran from pursuing a nuclear program. The attacks were targeted against the nuclear weapon development program which Iran claimed to have put off tracks for several years.

Myanmar

The DDoS attacks were launched prior to the first election in Myanmar which were due to be held on 25 October2010 in 20 years.The large-scale DDoS attacks were launched targeting the Ministry of Post and Telecommunication. The motive and the perpetrators of the attacks were unclear but since it is speculated that this was a preemptive attack by the Burmese government to disrupt elections because the ruling government has been accused of the gross violation of the human rights and was not in favour of stepping down from power.

Operation Israel (OpIsrael)

On the eve of Holocaust Remembrance day i.e. 7th April 2013, a group of anti- Israeli hackers including Anonymous launched cyber-attacks in the nature of DDoS, defacement, database hacking, leaking and targeting schools, banks and critical cyber infrastructure of Israel with the intent to erase Israel from the cyberspace in protest against the alleged atrocities committed by the Israel on the Palestine.

Singapore

A series of cyber-attacks in the nature of hacks were launched against the critical cyber infrastructure. The attacks were launched by the group “Anonymous” represented by a member known by his online handle as “The Messiah” as aprotest against the censorship regulations in the country.Later a person named as James Raj was apprehended and charged as the alleged Messiah.

Operation Shady Rat

The attack started in mid-2006 and claimed to have hit more than 70 organisations that included defence contractors, business organisations, United Nations and the International Olympic Committee. The acronym RAT is derived from Remote Access tool that was a five year targeted operation by one specific actor. The investigations pointed out towards the involvement of the People‟s Republic of China as the operation targeted various athletic oversight organisations during the time of 2008 summer Olympics.

Red October malware

This was a cyber-espionage malware program that came into the public know when it was uncovered by the Russian firm Kaspersky Lab.92 it was stated that this malware program

has been operating for at least five years and was responsible for transmitting information pertaining to the diplomatic secrets. This was an advanced cyber espionage program that targeted the governmental, diplomatic, and scientific research organisations throughout the world. The attackers were unknown.

Wannacry Ransom ware attack

This was a worldwide DDoScyber-attack that spread during May 2017 and targeted the computers that run on Microsoft Windows operating system. This attack denied the access to the administrator and demanded ransom payment in form of cryptocurrency. The attack was soon contained due to the security patch issued by the Microsoft but not before it has affected more than 200,000 computers across 150 countries. It is widely believed that North Korea was behind this attack.93

Attack on Yahoo

The Internet service company Yahoo! reported two major data breaches of user account data to hackers during the second half of 2016. The first announced breach, reported in September 2016, occurred sometime in late 2014, and affected over 500

Conclusion: The above discussed were only the few of the cyber operations that take place on day to basis and is not plausible to analyse all the cyber operation as that being outside the scope of this work. However this chapter made an attempt to analyse all the existing literature to analyse the available definitions to delimit and interpret the key terms closely related with the research thesis such as cyber-attack, cyber-war, cyber-space, information warfare and cyber warfare. The interpretation of the definitions is warranted on account of erroneous interchangeable use of terms, due to lack of awareness among civilians who unknowingly become combatants in the cyber war, which might undermine the gravity of the offense/act and providing appropriate definition for the classification of the offense/act when the cyber-attack may cross the threshold of use of force and warrant self-defence. The chapter closely analysed the existing definitions and the gaps that hinder the future research in the field of cyber warfare. An attempt has been made to fill the research gaps by proposing alternative definitions of cyber-attack that conforms to contemporary paradigm shift in the means and method of warfare. The chapter also discussed various methods that are used by cyber criminals against individuals and organization to procure financial, informational, psychological or tactical gains above the opposite State. A detailed analysis of the differentiation between cyber-attack and cyber warfare was necessary to draw a fine line between cyber-attack and cyberwar to emphasize that a cyber-attack which crosses the threshold of the use of force will warrant the exercise of self-defence from the opposite state actor.

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?catego ry/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.