NEW DIMENSION IN RIGHT TO PRIVATE DEFENCE; A STUDY WITH SPECIAL REFERANCE TO CYBER CRIME.

Ashish Kumar Gupta[1]

Scholar of B.A.LL.B(HONS.), 10th semester at law college Dehradun, Uttaranchal university Dehradun.

ABSTRACT:

The term private defence includes various concept from Anglo American Law. Private defence is an necessity for the act of criminality. In other word the condition of duress & necessity, private defence constitute the exception of criminal responsibility. "private defence applies to the use of the essential force and reasonable defensive force against those aggressor who perpetrates the illegitimate harmful attack in order to divert or repel this attack and also to save a legitimate interest from those risk of injury arising from the attack. critical analysis of those theories which have been proposed up to the present situation relating to the damage occurred due to cyber attack (the capability of that aggressor; equalising the interest and choice of the less evil etc.)

Right to private defence is not only centralised to the assault or any crime which is given in criminal law, it also holds the root of cyber law. In this era of technology crime is not only done by hardcore criminal with use of weapons but the way of criminal act is rapidly changing in different way likewise if we go through the IT (information technology) report we could see the different crime has been caused.

NATO has also an advance research workshop entitled a framework for a military cyber defence strategy, this shows the complexity of cyber security and the other numerous challenges associated with the field.

KEY WORDS:

Private defence, Cyber law, Cyber counter striking, Stuxnet, Spoofing, Counterfeiting, Mimicking, Mitigative counter striking, AIR (all India report).

[1]Author: Scholar of B.A.LL.B(HONS.), 10th semester at law college Dehradun, Uttaranchal university Dehradun.

INTRODUCTION

The right of private defence[2] is common to all system of law based on the maxims *Vim vi repellere omnes leges omniaque jura permittunt*[3]. It means As the significant technology development arising in this era the legal framework is lacking, currently there are several effecting way of addressing cyber crime under criminal law.

In the public discussion of private defence[4] in relation to cyber law the few major essentials Arises including the cyber security, cyber defence, cyber terrorism all the aspects clearly show that the effect and the necessity steps to be taken from it as private defence.

People discussion of cybercrime[5] has a few major words, including Stuxnet, zero-day vulnerabilities, HB Gary, RSA, and spoofing, counterfeiting, mimicking. The Stuxnet worm has exploited four zero-day vulnerabilities in the time of summer in 2010 and damaged Iranian nuclear infrastructure[6]. In Feb 2011, the security firm and government contractor HB Gary Federal has announced that they intended to go after every individuals involved in the loose knit hub of hackers that they call themselves Anonymous, and Anonymous represented their self by hacking into HB Gary Federal's systems and published confidential companies emails on the web and that they exposed some of HB Gary Federal's questionable activities[7].

Under Article 51of UN Charter on self-defence is granted 'if any armed attack occurs'. peoples agree that a cyber attack amounts to an huge 'armed attack'

---

[2] Traditionally accepted term is self defence, and this term is commonly used in the penal code of India as Indian Penal Code 1860. https://www.lawctopus.com/academike/right-private-defence/ last visit 6/2/2020

[3] http://latinmaximsandphrases.blogspot.com/2011/04/latin-maxims-and-phrasestxt-vim-vi.html last visit 6/2/2020.

[4] Self-defence in criminal law, page 2 by Boaz sangero

[5] https://currentaffairs.gktoday.in/current-state-cybercrime-report-2019-04201968376.html Last visited on 6/02/2020.

[6] William J. Broad, John Markoff, and David E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, NY Times (Jan. 15, 2011), available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html last visit 6/2/2020.

[7] Carlo Focarelli, 2015. "Self-defence in cyberspace," Chapters, in: Research Handbook on International Law and Cyberspace, chapter 12, pages 255-283, Edward Elgar Publishing.

and when the armed attack causes harm or damage which approximately possible to a 'kinetic' or conventional attack and in particular when it damage 'critical infrastructures'. Also, in case of cyberspace, it is permitted to every individual or collective self-defence has to meet the requirements of necessity, necessity to take private defence in proportionality and immediacy. Two major problems linked with self-defence against cyber-attacks[8] are related to the permissibility of anticipatory self-defence and self-defence against those people who does the grievous act of crime. Those crime which are never been tolerated and which causes major destruction in every ground of law, actors or against the breach by a state of its duty of prevention of cross-border harmful private acts.

1. RELATION BETWEEN PRIVATE DEFENCE AND CYBER LAW:

As we know that the private-defence means the right to defend himself from the person or property or of any different person against an act of another, the act of private defence is not amount to crime at any condition when the act is to defend himself and the use of force is for the necessity, it is been provided under sec 96 to 106 in the Indian Penal Code 1860[9]. the Private defence does not only exists in the criminal law but its roots also found in the cyber law. The definition of Cyber law states that it is the part of the overall legal system which deals with the Internet, cyberspace, and their other respective legal issues. Cyber law spread in a fairly broad area, pointing several subtopics including freedom of expression, and also access to and usage of the Internet browser, and online privacy. Generally, cyber law is referred to the Law related to the use of the Internet. Cyber Laws obtained legal recognition for the electronic documents and a structure in

[8] Ben Pershing, On Cybersecurity, Congress Can't Agree on Turf, Wash. Post (Jul. 18, 2011), available at http://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-onturf/2011/07/18/gIQACGCWMI_story.html. last visit 6/2/2020.

[9] Bhattacharya, Prof. T , Indian Penal Code, 5th Edition, Central Law Agency, Allahabad, 2007.
Tandon, Mahesh Prasad, Indian Penal Code, Allahabad Law Agency, Faridabad, 2006.
Gaur, Shri Narain, Indian Penal Code 1860, Dwivedi & company, Allahabad, 2005.

order to support e-filing and e-commerce transactions and also provides a basic legal structure to reduce or check cyber crime[10.]

An wrongful act must be clearly described in law and also it should be prohibited by law either that wrongful act is been prescribed in criminal law or any other law were the offence is calculated. Subsequent if we see to the moral principle of *nullume crimen sine lege*[11], as per the criminal law no any individual can be punished for an act which was not defined or prescribed by law at the time that person committed the act[12].

Subsequent law defined the rights and responsibility of legal subject Which includes, person , states and organisation. The right to private defence is been provided to every citizen in every country as in India it was provide in Indian penal code1860. To take an immediate action against any cause for necessity shall be calculated in private defence. Any act is done in exercise of the right of private defence is neither an offence nor it does give rise to any private defence in return. Substensive cyber-crime law included law that restrict specific types of cyber crime include law that restrict specific types of cyber-crime[13], and punishes non-compliance with their law.

Cyber-crime law gives identity of standards acceptable nature for information and communication technology (ICT). It established socio legal sanction for cybercrime and to protect the ICT user and mitigates. It provides the rule of conduct and also the standards of behaviour for the use of internets, computers, and other digital technology, and other criminal justice matter in cyber space.

[10] https://www.britannica.com/topic/cybercrime last visit 6/2/2020.

[11]https://www.law.cornell.edu/wex/nullum_crimen_sine_lege last visit 6/2/2020.

[12] https://www.equalityhumanrights.com/en/human-rights-act/article-7-no-punishment-without-law, last visit 6/2/2020.

[13] https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html last visit 6/2/2020.

2. COMPARISON BETWEEN CYBER SECURITY AND CYBER DEFENCE

In the case of right to private defence government of India on the national cyber security on march 2011 which differentiates cyber security and cyber defence government of India had made to draft such law related to it. cyber security set up the programme for the protection and securing the information and also to the system like computers, internets, database, data counters and other applications with technological security measures. Cyber defence is also a private defence against the cyber-crime and to the users raised in the ambit of cyber law. cyber defence refer the actions taken by a individual to protect the interest of the party in anticipation of an cyber attack[14].

Cyber defence related to specialization activity in particular aspect, it distinguishes the factors between cyber security and cyber defence in a network. It relates to the defensive actions against those activity originating from hostile actors that are political, quasi-political or economic motivation which has a negative impact on national security, public safety. According to Dr. moroco grecke, a criminal law professor who has been consultant to both the council of Europe cyber efforts and to UN; about cyber-crime and cyber security. In the case when the I LOVE YOU virus caused damaged worldwide[15] due to the absence of law in US law and the absence of law in the Philippines.

2.1 LAW RELEVANT TO THE USE OF SELF-DEFENSE:

This part of the article will examine the possible content application of current law to the notion of cyber self-defence. This article will argues in favour of the validity of a mitigative counter striking domination of period to ensure that self-defence becomes recognized in the cyber space realm as well as the physical realm, the current legal regime that can support or hinder implementation of mitigative counter striking capabilities in this part.

[14] Anticipation in Cyber-Security: Ahrend, J, Jirotka, MDA.

[15] Philippine Prosecutors Drop Charges in 'Love Bug' Case.
By Robert Frank Staff Reporter of The Wall Street Journal.

Mean while there are some essentials of existing law that could appear to oppose any form of counter striking on the Internet, but we argue that the importance of self-defence in virtually all other areas of law would lead to a reading of the current laws as permitting actions in self-defence, provided that such actions comply to the principles of mitigation.

The legal framework over the use of force should be based on prohibition and exclusion from that prohibition is been framed by UN Charter. As per the UN charter Article 2(4) of the Charter prohibits "threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations"[16]. In this order to accomplish its purpose and to maintain peace and security. This Charter makes "exclusive exceptions" from the general prohibition of use of force. Under the Article 39 in accordance with Articles 41 and 42 of the UN Charter the Security Council shall decide some of the measures shall be taken to maintain or restore international peace and security. If we see the Second exceptions from general prohibition of this charter of use of force is located in Article 51 of the UN Charter which shall regulate the rights of states(nation) to use force for individual or collective self-defence[17] from any kind of threats or attack. Although self-defence is regulated under the Article 51 of the UN Charter, later on the existence of customary right of self-defence have emphasized by many Western scholars in order to survive in International arena. This is however, it has also been recognized by the International Court of Justice (ICJ) in "Nicaragua case[18].

3. SELF-DEFENSE AGAINST CYBER-ATTACK

Here private defence is not only available for the individuals but it also used by the different states globally, in order to protect their self from cyber terrorism, cybercrime or cyber-attack.

[16] As per the UN Charter article 2(4).

[17] Charter of The United Nations, art.39, 41, 42 and 51, available at: http://www.un.org/en/documents/charter/.

[18] ICJ: Military and Paramilitary Activities in and against Nicaragua, ICJ Cases (1986).

Using a private defence against the wrongful act is a necessity, if a major act caused which brings the greater damage in order to use of private defence that should be calculated as necessity not a crime. In Munney Khan S/O Gulam Mohammad v. State of Madhya Pradesh[19], at time to recourse to the protection of public authorities There is no right of private defence in case. The right of private defence is basically a defensive right circumscribed by the statute available only when the circumstances clearly justify it. The international court of justice in case of *Oil Platforms (Islamic Republic of Iran v. United States of America) Judgment, 6 November 2003*[20] has given the judgment related to private defence.The use of force by a victim state of a cyber-attacks is lawfully in self-defence would be possible only if the essentials shall follows: (1) standards of an armed attack meets the cyber-attacks, (2) where the self-defence is being carried out cyber-attack is attributable towards the state (3) the use of any kind of force which carried in self-defence is the "necessary" and "proportional". An Legal analogy-based on debates between the scholars in the context of applicability of international legal principles relating to cyber-attacks which is stimulated numerous debates in the light of these conditions too, but it was Precisely disagreement steam from the absence of the definition of what constitutes an armed attack under international law and challenges to attribute cyber-attack(s) to a state; the applicability of customary rules of private-defence along with the given provisions under the UN Charter and interpretation.

3.1 CYBER ATTACK AS AN ARMED ATTACK?

Even in many conferences relating to cyber defence may arguments is been kept that guidance shall and also relating to the origin of the armed attack. This is not so defined that the armed attack only call the disaster only because of the weapons but also the cyber tech which is a medium of conversation and

[19] *1970 SCC (Cri) 491: ((1970) 2 SCC 480: AIR 1971 SC 1491), it has been held as follows at page 1494 of AIR.*

[20] https://ruwanthikagunaratne.wordpress.com/2017/08/17/list-of-icj-cases-relating-to-self-defense-and-other-matters-related-to-the-use-of-force/.

the bas of armed attack, the use of technology is vast and day by day the work on it was increasing and causes serious damage, similarly it is called that the cyber-attack is an armed attack. There are Some Relevant international organizations guidance provided on certain international instruments and also the legal scholar expressed their opinion, they had just tried to fill the absence of authoritative definition of armed conflict and cyber-attack. It is well know in Geneva Conventions[21] that Jean Pictet's guidance to determine the existence of an international armed conflict under Common Article 2 of the 1949, which spread a useful guide for assessing whether a particular use of force in order to defend himself could be considered as an act equal to armed attack. According to Pictet's guidance[22] a use of force is considered an armed attack when the force is of "sufficient scope, duration, and intensity. Another useful tool that helps to fill the absence of legal definition of what constitutes armed attack is the U.N. General Assembly's Resolution for "Definition of Aggression". Although the Resolution does not contain definition of armed attack this instrument provides examples of state actions that could be considered as an armed attack. acceptance[23.] Some scholars have tried to give the proper definition of armed conflict by explaining the difference between terms "war" and "armed conflict.

The United States is had declared its view that the full range of self-defensive instruments is been opened on some of the cyber-attacks; it is also said by the United Nation that in order to us of private defence for an armed attack is a necessity to protect the individual from the damage not to cause harm. Offering some more detail as to its legal position on the private defence, in 2011 the United States done its interpretation of Article 51 to the UN Group of Global Experts in the following terms: It may be difficult to reach a definitive legal conclusion as to whether a disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defence. Any such act

[21] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.

[22] *EX-99.(P)(3) 64 dex99p3.htm code of ethics of pictet ltd. and pictet asset management s*

23 Walter G. Sharp: Cyberspace and the use of force, Aegis Research Corporation, (1999) 60-61
The U.N. Documents: Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess. (Dec. 14, 1974)
NRC REPORT, supra note 10, at 34; see Jensen, supra note 25, at 208 (questioning whether a cyberattack triggers the right to self-defence or whether a nation cannot use self defence in the absence of a more traditional military attack.

if it is done in cyberspace which resultant in to war or cause harm to the people collectively or individually the legal remedy shall be provided as right of private defence.

3.2 NECESSITY AND PROPORTIONALITY AGAINST CYBER-ATTACKS AS CYBER DEFENCE.

In order to protect our rights from the force the Necessity and proportionality are founding principles of appropriate self-defence[24]. The other elements which create the threshold of lawful private-defence against cyber-attacks those principles considered in the context of cyber-attacks are highly disputed among the legal scholars. A dispute through peaceful means self-defence against cyber-attack will meet the requirement of necessity if under the given evidences state cannot achieve a reasonable settlement. If victim state limits it actions to the amount use of force required to defeat or to protect from ongoing cyber-attack or to later a future cyber-attack[25] Private defence against cyber-attack is proportional, in Compliance with the principles of necessity and proportionality. cyber-attacks present new hard challenges in front of the nation and it is also challenging task for all the nations in order to protect themselves and use of necessary force as a self-defence. It is also stated in the UN Charter that use of the private defence is a necessity and this force can also use prior to the attack if it is sure that an act of war is going to happen.

3.3 ANTICIPATORY SELF-DEFENCE AND CYBER-ATTACKS

The issue of anticipatory self-defence has been long debated by the legal scholars even in conventional terms. Measures and precaution undertaken in anticipatory self-defence are lawful when the "necessity of that self-defence is instants, overwhelming, and leaving no choice of means, and no moment for deliberation[26], UN article 51 of the Charter it is well accepted that

[24] Thomas Wingfield: The Law of Information conflict: National Security Law in Cyberspace (2000) 42.
[25] . Yoram Dinstein: War, Aggression and Self-defence (4th ed. 2005) 237.
[26] Yoram Dinstein: War, Aggression and Self-defence (4th ed. 2005) 237.
This is the Caroline standard of anticipatory self-defences that arose concerning an attack on a ship in 1837. NRC REPORT, supra note 10, at 243; Hoisington, supra note 60, at 450; Jensen, supra note 25, at 218-19; Sklerov, supra note 40, at 34, 48.

anticipatory self-defence is considered as customary self-defence. . Article 51 preserves an inherent right of self-defence in response to armed attack Contrary to these views significant part of the legal community believes that self- defence should be practiced not outside the Charter[27] Under this circumstances lawful *ex-ante* use of force (as "strict liability" or to a certain degree "effect based" analytical models suggest) would require victim state to sufficiently demonstrate the transcendence of an anticipated attack. In the case of cyber-attacks, such a requirement would invariably be difficult to meet, if not impossible. The overall debate of states over the applicability of Ius ad bellum[28] principles, standards and norms to cyber-attacks unequivocally showed that legal community is not united with these regards. Although under specific conditions cyberattacks could amount to armed attack(s), it is very hard to attribute such attacks to a state or non-state actors. Additionally necessity and proportionality along with the ex-ante attitude (i.e. anticipatory self – defence) are highly disputed among the legal scholars. All of these challenges require for one to reconsider legal alternatives that could provide more appropriate solutions to cyber-attacks and cyber-security. Accepting that in some situations, a cyberattack can be an "armed attack," some argue that a state still cannot legitimately respond in self-defence unless the state establishes that another state is responsible for the cyberattack[29].
Others argue that Article 51 of UN Charter merely codifies an inherent right of self-defence, and that anticipatory self-defence under the Caroline standard is still available as a response[30]. Some have argued, however, that the requirements of the Caroline standard that the necessity for response be "instant, overwhelming, and leaving no choice of means, and no moment for deliberation" make it unlikely that anticipatory self-defence could apply in a cyberattack context.

---

[27] https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 last visit 6/2/2020.
[28] Ibid.
Condron, supra note 26, at 414-15Sklerov, supra note 40, at 30-31 (asserting that the right of self-defence is an inherent right "derived from the fundamental right of states to survive.").

[29] Jensen, (noting the difficulty of responding to cyberattacks from non-state actors); Sklerov, supra note 40, at 2. Sklerov notes, however, that most legal scholars believe that the Law of War can be applied to address attacks by non-state actors. Sklerov, supra note 40, at 3.
[30] NRC REPORT.

4. POLICY CONCERNS RELATING TO MITIGATIVE COUNTERSTRIKING

mitigative counter striking[31] can be justified under current law governing self-defence, and described various issues that might arise in the context of both domestic and international law. In this chapter, we examine various new policy issues that may be raised coinciding with the implementation of an active defence regime emphasizing mitigative counter striking. This chapter evaluate the specific circumstances in which mitigative counter striking would be an optimal response, the potential for government to take responsibility for mitigative counter striking, and the potential role of public-private partnerships. We also provide suggestions for possible procedures for mitigative counter striking and how to protect third parties who might be harmed as a result of a counterstrike. Mitigative counter striking is also legally justifiable under several areas of domestic and international law, and can be made consistent with other areas of law by amending the law or by reinterpreting it.

The use of spiders to mine data would be categorized as cyber exploitation, rather than cyberattack, because the goal is to obtain data, not to cause immediate harm[32], In terms of rapidity, it is important to develop a standard to determine whether an intrusion is sufficiently severe to justify a mitigative counterstrike. This could potentially be done by applying tests that have been used by other researchers in analyzing whether international law would apply to prohibit either cyberattacks or mitigative counterstrike. Non-State groups such as terrorist organizations against which military self-defences might make any sense will generally have already threatened other violence. Regardless of how such non-cyber moves and threats figure formally into a

[31] https://experts.illinois.edu/en/publications/mitigative-counterstriking-self-defense-and-deterrence-in-cybersp last visit 6/2/2020.

[32] Lahle Wolfe, what are Robots, Spiders, Web Ants, and Worms? http://womeninbusiness.about.com/od/internetmarketingandseo/a/what-r-robots.htm (last visited Apr. 1, 2011) (defining robots, spiders, and web crawlers as programs that are designed to collect large amounts of data last visit 6/2/2020.

defending State's legal analysis, as a political matter they will no doubt figure significantly in its public justification of force.

CONCLUSION

As we know that the right to private defence is been provided to all the individual, and also the use of private defence in case of cyber law is permitted by the UN article 51, In the case where self-defence is permitted in cyberspace, it is important to meet the criteria for proportionality, immediacy and necessity, i.e. making sure a cyber-attack in self-defense does not exceed the limitations imposed by law to the right of self-defense and become an unlawful 'use of force'. The act of self-defense in cyberspace may also mean counter-striking or hacking back the suspected hackers. Problems may however arise when it is not sure of where the attack is coming from or if the correct hackers have been hacked back.

That the damage experienced by the attacked organization's system potentially outweighs the potential damage to third parties. That it is highly probable that the original hackers are likely to be the ones hacked back rather than innocent third parties. Also, the use of civil force-based litigation or police enforcement won't be helpful when it comes to cyberspace. It is also important when thinking about self-defense to be sure if the cost of self-defense outweighs the information resources that is available to be defended. Confusion may arise where there is an equilibrium between the cost of self-defense and the cost of potential damage.

SUGGESTION'S

Use of internet mobile phones, computers, laptop and other electronic devices which are upgrading social life day by day towords the technical world doesn't mean it is safe or it can't damage. As the world stepping towords high tech zone the risk of threatening, cyber-crime is increasing. As we know that the use of technology is so convenient to all but it rise more risk, to avoid such risk the use of technology should be very care full likewise:- Malicious links can do damage in several different ways, so be sure to inspect links and

ensure they’re from trusted senders before clicking, Try to limit using another user’s device when possible. Never share your credentials with others, and never give anyone remote access to your computer, keep lock your device, Keep track of your digital footprint, Use strong passwords and biometric features, ensure you turn off your Bluetooth and don’t automatically connect to any public Wi-Fi, and download with caution, Beware Social Engineering, Back Up Your Data.

The most harmful thought you can have is “it won’t happen to me,” or “I don’t visit unsafe websites.” Cyber criminals don’t discriminate in targeting all sorts of users. Be proactive. Not all mistakes can be undone with “ctrl + Z”. these all tips must be followed to avoid cyber-attack or cyber-crime. In order to protect yourself from these attacks if necessity occurs an individual can use the force as a private defence. The most necessary thing is for the legislation to develop the strict cyber laws relating to the cyber-attack, or cyber-crime.