Are we headed towards Web War I?[1]

Abstract

All nations across the world have succumbed to the possibilityof a "fifth" domain[2] of war-fighting.Whether all such 'cyber attacks' should be prohibited under Article 2(4) is debatable. It is argued that a reasonable threshold of cyber attacks amounting to 'use of force' must be internationally agreed, taking into account the holistic effect of the attack.Further, the author examines the possibility of the occurrence of a'cyber attack' reaching the threshold of an 'armed attack' warranting use of force in self defence. Finally, it is suggested that cyber defence be strengthened while facilitating international co-operation to avoid such unwarranted threats to world peace.

[1]ShrutiTulpule, BSL LLB, BCL (Oxon).

[2] US Department of Defense, '*The National Military Strategy for Cyberspace Operations*', 2006, p. 3.

Are we headed towards Web War I?

INTRODUCTION

Headlines such as '*The next Pearl Harbor could very well be a cyber attack*'[3] and '*Stuxnet is the Hiroshima of cyber war*'[4] and the cyber attacks on both private and public institutions in Estonia, Lithuania and Georgia have led to the possibilityof a "fifth" domain[5] of war-fighting.

In this article, I aim to examine the concept of a cyber attack and when it can attain the threshold of an 'armed attack' as defined under Article 51 of the UN Charter. Further, I seek to analyse the current scenario in India with respect to cyber attacks, and discuss the most effective solutions that nations could adopt to avoid such unwarranted threats to world peace.

DEFINITIONS

The author relies on the following definitions of the technical terms used in the course of this article.

"*Cyberspace*" can be described as a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein.[6]

Although no State may claim sovereignty over cyber space; States may exercise sovereign prerogatives over any cyber infrastructure[7] located on their territory, as well as activities

[3] Lisa Daniel, '*Panetta: Intelligence Community Needs to Predict Uprisings*', AmericanForces Press Service, 11 Feb. 2011.

[4] Michael Joseph Gross, '*A Declaration of Cyber-War*', Vanity Fair, April 2011.

[5] US Department of Defense, '*The National Military Strategy for Cyberspace Operations*', 2006, p. 3.

[6] The White House, *Cyberspace Policy Review*, 16 May 2011, p. 1.

[7] '*Cyber infrastructure*' refers to the communications, storage and computing resources upon which information systems operate.

associated with that cyber infrastructure. It is the sovereignty that a State enjoys over its territory that gives it this right to control cyber infrastructure and cyber activities within its territory.[8]

"*Cyber warfare*"encompasses military activity that primarily makes use of computer systems and networks in order to attack those of the adversary. The main goal hereby is typically to either deny the adversary the usage of such systems, or to access their functions in order to take control over structures under their management.[9]It includes[10],

- Online acts of espionage and security breaches – which are acts done to obtain national material and information of a sensitive or classified nature through the exploitation of the internet (eg. exploitation of network flaws through malicious software).
- Sabotage – the use of the internet by one nation state to disrupt online communications systems of another nation state (eg. military communication networks) with the intent to cause damage and disadvantage.
- Attacks on SCADA (Supervisory Control and Data Acquisition) networks.

While "*computer network attacks*" (CNA) comprise all cyber operations aiming "to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves",[11]"*computer network exploitation*" (CNE) refers to "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks".[12]"*Denial of Service*" (DOS) attacks are attempts to render a computer resource unavailable by sending as many communication requests as possible to the resource, thereby overloading the system so that it will effectively be rendered unavailable to regular communication requests.[13]

CYBER ATTACKSAMOUNTING TO 'USE OF FORCE'

[8]International Group of Experts, '*The Tallinn Manual on the International Law Applicable to Cyber Warfare*'at https://www.ccdcoe.org/249.html.

[9]Johann-ChristophWoltag, '*Cyber Warfare*', Max Planck Encyclopedia of Public International Law.

[10] http://www.unicri.it/emerging_crimes/cybercrime/explanations/cyberwarfare.php.

[11]US Department of Defense, *The National Military Strategy for Cyberspace Operations*, 2006.

[12]*Ibid.*

[13]Johann-ChristophWoltag, '*Cyber Warfare*', Max Planck Encyclopedia of Public International Law.

The 'use of force' standard is employed to determine whether a State has violated Article 2(4) of the UN Charter.

The *travauxpréparatoires*of the UN Charter clearly show that the prohibition of "force" wasnot intended to extend to economic coercion and political pressures.[14] Also, Article 41 of the UN Charter refers to "interruption of … communication" as a "measure not involving armed force", thus suggesting that certain DOS attacks would not fall under the prohibition of Article 2(4).However, cyber attacks span the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down an academic network temporarily), to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators).[15]

However, according to the International Court of Justice (ICJ), the prohibition in Article 2(4) applies "to any use of force, regardless of the weapons employed".[16] Thus, it is relatively uncontroversial that cyber operations fall under the prohibition of Article 2(4) of the UN Charter once their effects are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry.[17] Conspicuous examples of a use of "force" within the meaning of Article 2(4) of the UN Charter, would be cyber operations manipulating target computers systems so as to cause a meltdown in a nuclear power station, or opening the floodgates of a dam above a densely populated area, each with potentially horrific consequences in terms of death, injury and destruction.

However, the ICJ clarified in its *Nicaragua Case*, even minor acts of interstate force fall under the general prohibition of Article 2(4) of the UN Charter, regardless of whether they also qualify as acts of "aggression", or as "armed attacks" entitling the targeted State to resort to force in self-

[14] A Brazilian proposal to extend the prohibition to "the threat or use of economic measures in any manner inconsistent with the purposes of the United Nations"' was rejected at the San Francisco Conference; *Documents of the United Nations Conference on International Organization*, vol. VI, 1945, pp. 559, 720–721.

[15]Eric Talbot Jensen, '*Computer Attacks On Critical National Infrastructure: A Use Of Force Invoking The Right Of Self-Defense*', 38 Stan. J. Int'l L. 207.

[16]The International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, advisory opinion, 1996, § 39; and Ian Brownlie, *International Law and the Use of Force by States*, 1963, pp. 362, 431.

[17] Michael Schmitt, '*Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*', Columbia Journal of Transnational Law, vol. 37, 1999, p. 916.

defence.[18]But, cyber operations were not anticipated by the drafters of the UN Charter and, so far, neither state practice nor international jurisprudence provide clear criteria regarding the threshold at which cyber operations not causing death, injury or destruction must be regarded as prohibited under Article 2(4) of the UN Charter.[19]

However, I assert that when a nation is highly dependent on the internet and technology, the holistic effect of the cyber attack must be taken into consideration, albeit sans violent effects. Thus, given the heavy dependence of most sectors on the internet, it is inappropriate to conclude that absent violent effects, all cyber operations necessarily fall short of armed force.

CYBER ATTACKS AMOUNTING TO AN 'ARMED ATTACK'

The occurrence of cyber operations amounting to an "armed attack" (by a State or by non-state actors[20]) permits the attacked State to exercise its inherent right to self-defence through the resort to force. The ICJ, in the Nicaragua Case held that 'scale and effects' are to be considered when determining whether particular actions attributable to a State amount to an 'armed attack'.[21]

Interpreting the 'scale and effects' criterion exclusively in terms of physical destruction caused by the cyber attack, leads to two extreme approaches. It will either end up being too restrictive (that is, including only cyber operations directly resulting in physical destruction but not, for example, the "mere" incapacitation of the entire national power grid, telecommunication network or air defence system) or too expansive (that is, including any large scale denial of service attack even against nonessential, purely civilian service providers such as, for example, online shopping

---

[18] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, merits, 1986, §§ 191 and 195; International law Commission, *Report of the International Law Commission on the work of its Thirty-second session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth session, Supplement No. 10*, UN document A/35/10, 1980, p. 44; YoramDinstein, *War, Aggression and Self-Defence,* 4th ed., 2005, p. 174ff; Ian Brownlie, *International Law and theUse of Force by States*, 1963, pp. 363ff, 366.

[19]Nils Melzer, '*Cyberwarfare and International Law*',at unidir.org/pdf/activites/pdf2-act649.pdf.

[20]Albrecht Randelzhofer, 'Article 2(4)', in Bruno Simma (ed.), *The Charter of the United Nations: A Commentary, vol. I, 2002, p. 121; Lassa Oppenheim, International Law: A Treatise, vol. II, 1921, § 57; Alfred Verdross and Bruno Simma, UniversellesVölkerrecht: Theorie und Praxis, 1984, § 468*;UN Security Council Resolutions 1368 (12 September 2001) and 1373 (28 September 2001).It must be noted that the interpretation of the notion of armed attack to include acts carried out by non-state actors remains controversial and does not reflect universal consensus.

[21]*Nicaragua v. United States of America*, merits, 1986, §§ 195.

services or telephone directories).[22] To overcome this problem, a reference must be made to"critical infrastructures"[23] the protection of which has always been the key concern of States in their discussion of cybersecurity.[24]

Critical infrastructures include "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations".[25]

Thus, it is fairly evident that cyber attacks likely to result in death, injury or destruction will be classified as 'armed attacks'. However, I submit that cyber attacks without violent consequences could still amount to an "armed attack" if they aim to incapacitate "critical infrastructures" within the sphere of sovereignty of another State.

SELF DEFENCE AGAINST A CYBER 'ARMED ATTACK'

Self defence must be exercised against the entity to which the armed attack is attributable, while satisfying the requirements of necessity, proportionality[26] and immediacy. However, one of the major problems is identifying the perpetrators, and determining their intentto affix responsibility. Cyberspace isnot subject to geopolitical or natural boundaries[27]andit is readily accessible to governments, non-state organizations, private enterprises and individuals alike. IP spoofing[28] and

[22]Nils Melzer, '*Cyberwarfare and International Law*',at unidir.org/pdf/activites/pdf2-act649.pdf.

[23] Marco Roscini, '*World Wide Warfare—Jus ad bellum and the Use of Cyber Force'*, in Armin Bogdany and RüdigerWolfrum (eds), *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, p. 96.

[24] US Presidential Decision Directive 63, '*Critical Infrastructure Protection*', 22 May 1998; The White House, '*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*', 2003; and European Commission, '*Green Paper on a European Programme on Critical Infrastructure Protection*', document COM(2005) 576 final, 17 November 2005.

[25] UN General Assembly Resolution 58/199 of 30 January 2004.

[26]*Gabcikovo-Nagymaros Project (Hungary v. Slovakia)*, 1997 I.C.J. 7, 55-56 (Sep. 25) (Merits).

[27]Nils Melzer, '*Cyberwarfare and International Law*',at unidir.org/pdf/activites/pdf2-act649.pdf.

[28]'*IP spoofing*' refers to the creation of Internet Protocol (IP) packets with a forged source address with the purpose of concealing the identity of the sender or impersonating another computing system.

the use of botnets,[29]make it easy to disguise the origin of an operation, thus rendering the reliable identification and attribution of cyber activities particularly difficult.[30]Notably, the vast majority of known attacks are instead from recreational hackers, who are significantly harder to track than state organizations.[31]

It must be noted that self-defensive action in cyberspace is not permissible in *response* to harm which has already been caused by hostile cyber operations, but only with a view to preventing or repelling an imminent or ongoing attack, and only to the extent actually necessary for that purpose.The speed, unpredictability and clandestine nature of most cyber operations severely hamper the defending state's ability to detect, repel and react in time to an imminent or ongoing attack.[32]In fact, in most cases, the attack will already be over and the damage done by the time it is identified.[33]

These problematic characteristics of cyber operations, in conjunction with the fact that cyber attacks are increasingly conducted by non-state actors relying on series of small-scale operations, have presented a new angle to the debate on the permissibility of anticipatory self-defence.[34]

THE REALM OF PRACTICALITY

Apparently, the most violent 'cyber' attack to date was carried out in 1982, when an American covert operation allegedly used rigged software to cause a massive pipeline explosion in Russia's Urengoy–Surgut–Chelyabinsk pipeline.[35]No cyber offense has ever injured a person or ever

[29] A '*botnet*' is an interconnected series of compromised computers used for malicious purposes. A computer becomes a '*bot*' when it runs a file that has bot software embedded in it.

[30] On the characteristics and key features of cyberspace, see also US Department of Defense, *The NationalMilitary Strategy for Cyberspace Operations*, 2006, pp. 3–4.

[31]Eric Talbot Jensen, '*Computer Attacks On Critical National Infrastructure: A Use Of Force Invoking The Right Of Self-Defense*', 38 Stan. J. Int'l L. 207.

[32]*Ibid*.

[33] Jeffrey K. Souder, '*Information Operations in Homeland Computer-Network Defense*', at http://www.jedonline.com/jedonline/default.asp?journalid=4&func=articles&page=0110j12&year=2001&month=10&doct=features.

[34] Michael Schmitt, '*Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*', Columbia Journal of Transnational Law, vol. 37, 1999, pp. 932–33; Eric Jensen, '*Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self- Defence*', Stanford Journal of International Law, vol. 38, 2002, pp. 221–24.

[35]Thomas Rid, '*Cyber War Will Not Take Place*', Journal of Strategic Studies, 35:1, 5-32.

damaged a building.[36]To date, no international armed conflict has been publicly characterized as having been solely precipitated in cyberspace.[37]Thus, it can be surmised that very rarely do cyber attacks attain the threshold of 'use of force', let alone that of 'armed attack'. Consequently, victim nation it is left with limited options to retaliate to a cyber attack falling below the threshold of 'use of force'.

Moreover, it has been opined that all politically motivated cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion.[38]

In this scenario, I propose that the best solution is to make the computer network defence up to date in order to proportionately combat a cyber attack, regardless of threshold. *Computer network defence* (CND) refers to "actions taken to protect, monitor, analyse, detect, and respond to unauthorized activity within information systems and computer networks".[39] Thus, it involves the primary safeguard of strengthening of cyber security through intelligence and law enforcement in order to avoid any cyber attacks. In the event of an attack, CND will aid to overcome the obstacles of identification and attribution while ensuring that proportionate retaliatory measures are undertaken.

THE INDIAN PERSPECTIVE

India has been a victim of several cyber attacks; notably, the hacking of government websites[40]. Recently, threatening images uploaded and messages sent in bulk, led to thousands of people fromNorth-EastIndia to flee to their hometowns. All these attacks obviously fell short of the 'use of force' requirement, and it was difficult to trace the identity of the perpetrators; but, little has been done to implement aclear, comprehensive, and effective the national cyber security policy.

---

[36] An accidental gasoline explosion that occured in Bellingham, WA on 10 June 1999, is sometimes named as a violent cyber incident; three youths were killed. Although the relevant SCADA system was found directly accessible by dial-in modem, no evidence of hacking was uncovered in the official government report; National Transportation Safety Board, '*Pipline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999*', Pipeline Accident Report NTSB/PAR-02/02 (Washington DC, 2002), 64.

[37]International Group of Experts, '*The Tallinn Manual on the International Law Applicable to Cyber Warfare*'at https://www.ccdcoe.org/249.html.

[38]Thomas Rid, '*Cyber War Will Not Take Place*', Journal of Strategic Studies, 35:1, 5-32.

[39]Nils Melzer, '*Cyberwarfare and International Law*',at unidir.org/pdf/activites/pdf2-act649.pdf.

[40]It has been reported that the websites of the Central Bureau of Investigation, the Supreme Court, the Planning Commission and the Bhaba Atomic Research Centre have been hacked into.

However, the Indian government is in the process of establishing its cyber security infrastructure in the form of a scanning agency called 'National Cyber Coordination Centre'. It will monitor all web traffic passing through Internet service providers in the country. The scanning agency will issue 'actionable alerts' to government departments in cases of perceived security threats.[41] All tweets, messages, emails, status updates and even email drafts will now pass through the new scanning centre.

It can be argued that this violates the right to privacy[42] but the thin line between individual privacy must be balanced with the collective right to security.However, I believe that individuals must sacrifice their individual right to privacy for the greater good, i.e. the collective right against such threats to world peace.

CONCLUSION

It must be acknowledged that the Internet is critical for the effective functioning of both,the government and the economy; but at the same time, this fifth domain has become a vulnerable target.As aforementioned, it can be surmised through practical and realistic considerations, that the threshold of cyber attacks will rarely reach the intensity of an 'armed attack'.

Whether the conclusion of an international instrument in this regard would be of help is questionable; since rapid technological progress in this field would make a detailed framework somewhat short-lived.[43]Thus, I submit that the most viable alternative is to strengthen cyber defence by each State, while ensuring international co-operation against harbouring criminals, entering into extradition treaties of cyber criminals, and safeguarding cyberspace from the launch of computer network attacks through a State's territory.

---

[41]http://www.ccaoi.in/UI/links/fwnewsletter/CCAOI%20Newsletter%20Feb%202012.pdf

[42]Article 21, *The Constitution of India*.

[43]Johann-ChristophWoltag, '*Cyber Warfare*', Max Planck Encyclopedia of Public International Law.