Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Analysis of China's Technological warfare: A Challenge to the existing International Law

Kanumuri Sai Pavani[a]

[a]OP Jindal Global University, Sonipat, India

Received 20 July 2022; *Accepted* 19 August 2022; *Published* 20 August 2022

The technological warfare by China is derived from a gap in existing international law. The rule of non-interference and state sovereignty fills such a gap. However, the solution is not permanent to solve the issue. The temporary arrangement is the US-led-international liberal order. Analyzing the position of the US to combat the technological warfare by the Chinese companies in their territory. The analysis of the Chinese companies having dual roles projects that the solution will be the US alone and not protect other countries from China's technological warfare. Further to understand the different ends of warfare: there are two case studies.

Keywords: *international law, china's technological warfare, liberal order.*

INTRODUCTION

We are in the era of technological developments, where every second there is innovation. Technological development is a constant variable that comes with uncertainties and challenges. One such tangent of this massive domain is technological warfare. Under international law, we assume armed conflict to be an extreme force of threat to the country. However, technological warfare is more dangerous than armed conflict as it tries to sabotage

the country with its information. The war is not on the borders but with the host country and victim country. China is the prime suspect in carrying out such activities. The technological operations of the country are spread out in the world. Understanding its nature, China presupposes the peculiarities of practising such activities. Even though the international community is alarmed by such activities, China takes a back seat and continues the activities. The community takes few steps but the proper mechanism to tackle such a problem is absent. This paper will analyze the existing gap between the existing international law in ensuring that China's technological warfare with the other countries is passive. However, understanding the rule of state sovereignty and non-interference in the context. Further, the aid of the US international liberal order in tackling the problem of technological warfare with China. The counter-act of China being a threat to the US. This part will analyze the operations of Chinese companies about state authoritarianism. The last part would analyze the impact of traps through two case studies of India and the African Union. The underlying analysis of this paper would be to unravel China's aim to become the global leader partaking in the US.

ABSENCE OF THE WORD "TECHNOLOGICAL WARFARE" IN INTERNATIONAL LAW

The governments and security agencies of the state rely on technological information which is easily targeted to cyber-attacks, hacking, and stealing information. China is one such country. The country transgressing their invisible borders to access such information and the vulnerability of the other country being targeted with their information is outrageous. The framework of international law does not address such vulnerability. The failure of international law to cope with the development of technology is the point of debate. International law mentions the definitions of armed conflict. International customary law has developed in the armed conflict but has been left out of technological warfare. Following the era of the cold war, where the armed conflict was not the only choice of deterring the opposite party[1] but other interventions to successfully sabotage the other party had a domino effect on the countries. One of the interventions was the technological capacity to attack the morale of

[1] Warren Chin, 'Technology, war and the state: past, present and future' (2019) 95 (4) International Affairs, 765, 771

the country without the need for physical power.[2] China's presupposition of a non-armed conflict mode like technological warfare has left the peculiarities in international law. Here, the armed conflict labelled to be the hard power has a declining effect and a surge of soft power is visible. Noticing the peculiarity in the international law of not referring to technological warfare as a threat is advantageous to China. Turning the technology into one of the major tents of exercising soft power has become a climbing step towards their goal of being a super-leader. However, such steps by China to transcend other countries' information have led to the countries responding through sanctions – diplomatic or economic. The point of contention is that international law has not fully developed in this regard and therefore the solution to these interventions has a different effect as per the rules. Article 2 (4) of the UN Charter has exclusively stated that the use of force or threat against territorial integrity should have refrained.[3]This article imposes the tenet of state sovereignty and non-interference of another state. Assuming that this tenet imposes on defined borders and the use of force or threat within the borders is against the state sovereignty. Along similar lines, the nature of technological warfare happens within undefined borders and territory but the implication is the same, that is a threat to territorial integrity. Since there is no definition of technological warfare and China has taken advantage of the same. The victim country has used the same gap in the framework of international to award sanctions on the Chinese government. The hacking of computers of various personnel in countries like Vietnam, the Philippines, Australia, and Myanmar[4] has threatened the integrity of their citizens. The concept of non-interference has a supplementing effect from state sovereignty. As China tries to interfere rather than steal the information from the victim countries, it is opposed to the non-interference rule. On the face of it, enforcing these two rules provides us with a remedy to counter-act China's action. However, this new force of vulnerability has a new set of questions that needs different answers. Applying the armed conflict rules of international law fails to underline the nuances of the problem. To understand the nuances of the problem, we shall

[2] *Ibid* at 782
[3] Charter of United Nations, 1945, art.2(4)
[4] Yogesh Gupta, 'Future War with China Will Be Tech-Intensive' *(The Tribune*, 26 October 2020) <https://www.tribuneindia.com/news/comment/future-war-with-china-will-be-tech-intensive-161196> accessed 13 July 2022

look after the case study of the USA. The country provides us with a legal standard to ensure that the problem is tackled from its root, that is the Chinese state authoritarianism.

CHINA'S TECHNOLOGICAL RIVALRY WITH THE USA: LIBERAL ORDER

The USA has established its power in the technology industry since the end of the cold war. However, the technology industry changes every minute, and coping with such rapid change is impossible. After the end of the cold war, the USA secured the momentum but China wants to seal the entire industry with its cheap prices and unconcealed technological spies in the country. This vision of China marks the start of technological warfare with parts of the world. The liberal international order established by the USA is seen to be crumbled by this approach of China.[5]Even though China does not follow the liberal order, invading other countries' information is against the liberal order followed by the victim countries. This distinction between the competitors is abiding by this order to leverage without any hindrance in the freedom of affairs of the other country. The USA following the order is respected and China is disregarded with its tactics.[6] The assumption of the international world to follow the footsteps of the USA is incomplete because China's expansionist policy reached far beyond the limits of invading information from another country. It has expanded the threats to national security, one of the foundations of the international law community. Disregarding such an important tangent of international law has weakened the USA-led liberal regime of international law.

A. *Controlling the country through soft power: hacking, cyber-attacks, and 5G*

China leveraging such weakness of the USA has led to different cyber-attacks, hacking, and stealing of important information. A report by a Canada-based think tank has reported that the cyber-attacks/dangers of China in the USA would derail the existing rule of the government.[7]Attacks on different American state governments by Chinese network is another

[5] Naná de Graaff & Bastiaan van Apeldoorn, 'US-China relations and the liberal world order: Contending elites, colliding visions?' (2018) 94 (1) International Affairs, 113, 114

[6] *Ibid*

[7] 'China Mounting Cyber-Attacks to Fulfill Political Objectives: Think Tank' (*Business Standard,* 27 March 2022) <https://www.business-standard.com/article/international/china-mounting-cyber-attacks-to-fulfill-political-objectives-think-tank-122032700060_1.html> accessed 16 July 2022

such example.[8]Understanding the strategy behind such warfare of China is its aspiration of controlling the USA with soft power rather than hard power. The latter is the strength of the USA but China equally focuses on both variants. The aggressive attitude to pursue the label of being the most powerful country in the world. However, the USA has tried to stop such illiberal interventions through strict sanctions. One such example is the development of 5G technologies. As the world is trying to make 5G technologies available, this has become a contention between the countries. USA has tried to stop Chinese companies to develop such technologies in the US. Huawei, a Chinese technology company that is the proposed guarantor of 5G technologies has faced decades of transactions from the US government.[9]Understanding the nature of Chinese companies in hacking, cyber-attacks, and stealing pieces of information USA has tried to sanction restrictions on this company. The revenue of the company has declined but outside the USA Huawei has spread its wings deeply.[10]Huawei has targeted countries where American technology is limited. This step provides them with exclusive rights to develop without any sanctions because the governments welcome such development.

B. ***Chinese companies and their geopolitical motives***

Chinese companies are differently placed than other companies in the world market. The companies in addition to competitiveness carry the aspiration of China to be placed at the top. The dual role satisfies the state's interests in achieving the goal with commercial priorities.[11]Here, the state interests are multifaceted as it tries to break down the national security of countries. China incorporates a few sector companies including technology companies like Huawei to achieve the goal.[12]These companies freely advertise such goals but with a false addition of bringing world security together.[13] The irony is that a country trying to control world security is advertising about strengthening world security. China's reach and

[8] *Ibid*

[9] Dingding Chen & Wang Lei, 'Where Is China-US Technology Competition Going?' (*The Diplomat*, 2 May 2022) <https://thediplomat.com/2022/05/where-is-china-us-technology-competition-going/> accessed 16 July 2022

[10] *Ibid*

[11] Naná de Graaff & Bastiaan van Apeldoorn (n 5) at 121

[12] Lindsey W Ford, 'Extending the Long Arm of the Law: China's International Law Enforcement Drive' (*Brookings*, 15 January 2021) <https://www.brookings.edu/blog/order-from-chaos/2021/01/15/extending-the-long-arm-of-the-law-chinas-international-law-enforcement-drive/> accessed 17 July 2022

[13] *Ibid*

power have dominated the ethos of the companies to focus on their enhancement as a global leader. Here, the companies are seen as a means to achieve their geopolitical motives of becoming a great power. Understanding such a plot, the USA has tried to sanction such technology companies. However, the situation is differently placed for other countries which cause different impacts on them. This has caused a crack in the US liberal order. Other countries advocating for different orders have realized that the means to counter-act China's technological warfare is under US protection. However, in the transit of such protection, they are fallen into the clutches of their trap.

IMPACT OF SUCH TRAP ON DIFFERENT COUNTRIES:

Through their expansionist policies, they have tried to control other countries. These countries cannot counter-act because these governments grant Chinese governments/companies access to their information. Without understanding the threat, they are going to face, they hand over such power to China. Few countries have tried to identify such ignorance and laid down various sanctions. Even though there are only two case studies, both of them explain how China's technological warfare works differently.

A. India:

India is one of the vulnerable neighbours sharing a border with China and has repeatedly laid down sanctions against China. Under section 69 A of the Information Act India has banned around 53 apps this year.[14] The section includes the threat to national sovereignty and actions against such an act. Even after the Galwan Attacks 2020, the Indian government tried to ban a couple of apps of Chinese origin. These instances project how the Indian government has tried to counter-act the Chinese actions. Recent reports of China's attack on the electricity grid close the line of control.[15]Other countries in Asia have faced the same fate.[16] The constant threat to

[14] 'Garena Free Fire, 53 Other "Chinese" Apps Banned: Full List of Banned Apps' (*The Indian Express*, 17 February 2022) <https://indianexpress.com/article/technology/tech-news-technology/garena-free-fire-and-53-other-chinese-apps-banned-full-list-7772673/> accessed 18 July 2022

[15] Kartik Bommakanti, 'Chinese cyberattacks against Ladakh electricity grid: A déjà vu' (*Observer Research Foundation*, 15 April 2022) <https://www.orfonline.org/expert-speak/chinese-cyberattacks-against-ladakh-electricity-grid/> accessed 18 July 2022

[16] Yogesh Gupta (n 4)

national security should be a wake-up call for India as well as other countries. This case study explains how India's action is slower yet provides an efficient counter-act to the threat imposed by China. As India tries to establish itself as a global leader, the steps taken are neck-to-neck. The reason behind such action is the border tensions[17] at various points between India and China. This is one of the major reasons for such efficient counter-acts taken by the Indian government.

B. African Union:

Another victim is parts of the African continent. China has diplomatic relations with all most every country on the continent. As a token of diplomatic relations, China built the African Union. One report has alleged that the Chinese government had redirected the surveillance from the African Union to China.[18] The report further stated that this might be in a larger scheme of developing AI systems.[19] This case explains the larger plot of developing the AI through trial and testing of the information by hacking the surveillance system. Still considered to be hacking, China denied all such reports. Here, this case study is completely different from India's. The reason being China's operations in Africa are unimaginably different from India. China's operations provide Africans with the hope of development.[20]Even though, they have hacked the surveillance system of the African Union the measures taken by the union were nothing. Owing to the economic and diplomatic relations between China in Africa, there is an unbalanced relationship between them. China is on the lighter side of the seesaw and Africa is placed on the heavier side of the seesaw. Africans see the Chinese government as their saviour but the latter is taking advantage to develop their own goals.

---

[17] Vikram Mittal, 'The Lesser-Known Border Dispute: China and India' (*Forbes*, 21 February 2022) <https://www.forbes.com/sites/vikrammittal/2022/02/21/the--lesser-known-border-disputechina-and-india/?sh=60698761192d> accessed 19 July 2022

[18] Salem Solomon, 'Experts: Report of China Hacking African Union HQ Fits Larger Pattern' (*VOA*, 5 January 2021) <https://www.voanews.com/a/east-asia-pacific_voa-news-china_experts-report-china-hacking-african-union-hq-fits-larger-pattern/6200356.html> accessed 19 July 2022.

[19] *Ibid*

[20] Larry Hanauer & Lyle J Morris, 'China in Africa: Implications of a Deepening Relationship' (*Rand,* 2014) <https://www.rand.org/pubs/research_briefs/RB9760.html> accessed 18 July 2022

CONCLUSION

The absence of technological warfare in the existing international law framework has turned out to be the starting point of China's technological warfare with the countries. Not placing armed conflict with technological warfare on the same footing would help China surge its soft power. Using the same loophole, the victim countries enforce the rule of non-interference and state sovereignty through economic and diplomatic sanctions. To tackle the failure to understand the nuances of this problem US-led international liberal order becomes the guide. The US has faced the brunt of China's hacking and cyber-attacks and has levied sanctions. Majorly Chinese companies are the initiators of such warfare, so the US has tried to undermine their operations. However, the act is effective only for the US and not the countries outside the territory. For understating technological warfare, we analyzed two cases. The former is the Indian case study, where the country has countered the attacks from the Chinese government. The relationship between the countries being hostile like the US has proven to be the deterrent factor to leverage such actions. The latter is the African union case. A completely different relationship has caused China to use the territory as a trial for their AI development. After analyzing the US, India, and African Union the ambition of China to become the global leader in technology development is slowly coming true. However, these developments are at the cost of rigid international law.