Cyber Warfare as a Use of Force against Third-Party Countries: The Perspective of International Law

Dr Tareq Hamid AL-Fahdawi*
DOI: 10.21827/GroJIL.10.2.91-102

Keywords:
RUSSIA, UKRAINE WAR, CYBER WARFARE, THIRD-PARTY STATES, CYBER WEAPONS, USE OF FORCE, INTERNATIONAL LEGAL RESPONSIBILITY

Abstract

The use of force in international relations takes different forms and changes year by year due to the development of cyber technology. The problem mentioned in this study is that the Charter of the United Nations (UN Charter) and international law have not considered weapons development and future weapons that may be used in international relations, as Russia has used such weapons during the war against Ukraine. Unfortunately, cyber technologies were used to deter and weaken Ukraine's chance to gain an advanced result on the ground. Although such cyber operations can cause the same physical damage as other weapons, the international community is still struggling to determine whether using a cyber weapon is considered a use of force. This study argues that cyber attacks against third-party countries that support Ukraine during the war may count as the use of force and a breach of Article 2(4) of the UN Charter.

I. Introduction

Since the onset of the war between Russia and Ukraine in February 2022, there has been a significant shift in the landscape of warfare. As a direct consequence of this conflict, Russia has launched cyber attacks against third-party States that have not been involved in any direct military action in this war, particularly States that have supported Ukraine in various capacities. Russia has targeted States that have offered direct or indirect military assistance to Ukraine, imposed sanctions, or opposed the invasion of Ukraine during the United Nations (UN) Security Council meeting in 2022.[1] Russia used cyber malware against these third-party States instead of fighting them directly. The use of this new generation of technology represents a new dimension in warfare. It serves as a means of exacting revenge while avoiding the potential international legal repercussions of direct attacks. By utilising cyber attacks, Russia was able to retaliate against other countries without engaging in traditional warfare. However, these actions violated the principles enshrined in the UN Charter and international law.

* Dr Tareq Hamid AL-FAHDAWI is a researcher and lecturer at the University of Anbar, Centre for Strategic Studies in Iraq. Email: tareq.al-fahdawi@uoanbar.edu.iq.

1 Sean Lyngaas, 'Russian-Speaking Hackers Knock US State Government Websites Offline' (*CNN Politics*, 5 October 2022) <https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2022/10/05/politics/russian-hackers-state-government-websites/index.html> accessed 5 January 2024.

Notably, on 24 February 2022, Ukraine's critical institutions, including the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, the Security Service of Ukraine, and the Cabinet of Ministers, encountered network disruptions in what NetBlocks identified as a cyber attack.[2] While the war was between Russia and Ukraine, Russia extended its cyber attacks to other States. Between January and March 2023, the top three States that were impacted by Russia's attacks were Poland, which received 173 cyber attacks, Latvia, which received 92 cyber attacks, and the United States (US), which received 83 cyber attacks, most of which were by anonymous Russian actors.[3] In addition, there were a large number of cyber attacks against French, German, and European politicians. These cyber attacks were meant as a retaliation to the support that Ukraine gained from other States during the war. In March 2023, the website of the French National Assembly was temporarily disabled by Russian hackers through a Distributed Denial-of-Service (DDoS) Attack. In a message shared on Telegram, the hackers viewed the attack on the French government as a response to its support of Ukraine during the conflict.[4] In the same month, an unsuccessful DDoS attack was launched against a German defence firm for the same reason. According to a Kon briefing on 11 October 2023, nearly 33 States have fallen victim to cyber attacks, with some, such as the US, experiencing as many as 1,979 attacks.[5] This happened in addition to the cyber attacks against the US and European politicians who publicly denounced Vladimir Putin's invasion of Ukraine. In this case, Russia utilised its cyber capabilities in an offensive strategy that aligned with its foreign policy mission. It is clear that cyber attacks and their implications are considered as a use of force that breaches Article 2 of the UN Charter, which is significant for preserving international peace and security.

The primary question here is, to what extent does the current international legal framework that encompasses the UN Charter and associated instruments, sufficiently regulate and manage cyber attacks and offensive cyber activities used against third-party countries? Therefore, this study argues that the impact of weapons, whether malware or physical, share common ground. Before delving into why cyber attacks should be considered a breach of the UN Charter, it is imperative to explore the development of cyber weapons and understand their usage in the realm of human life and international relations. By exploring these aspects, this research aims to contribute to the ongoing discourse surrounding the use of cyber weapons, their legal ramifications, and the imperative to shape a robust framework that effectively governs cyberspace.

II. Development of weapons

---

2 @Netblocks, 'Confirmed: #Ukraine's Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, the Security Service of Ukraine and Cabinet of Ministers websites have just been impacted by network disruptions; the incident appears consistent with recent DDOS attacks' (*X*, 24 February 2022) <https://twitter.com/netblocks/status/1496498930925940738?s=20&t=tUz_SlNzCPGv9r0sQT-q_g> accessed 5 January 2024.

3 Cyber Peace Institute, 'Quarterly Analysis Report Q1 January to March 2023: Cyber Dimensions of the Armed Conflict in Ukraine' (*CyberPeace Institute,* 2023) <https://reliefweb.int/report/ukraine/cyber-dimensions-armed-conflict-ukraine-q1-2023> accessed 5 January 2024.

4 Laura Kayali, 'Russian Hackers Strike French National Assembly Website' (*Politico*, 27 March 2023) <https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron/> accessed 5 January 2024.

5 Bert Kondruss, 'MOVEit Hack Victim List' (*Kon Briefing*, 20 December 2023) <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html> accessed 5 January 2024.

Due to the unnecessary suffering inflicted on civilians using weapons in conflicts, the UN regulations divide weapons into conventional and non-conventional weapons.[6] This distinction is based on how much unnecessary suffering the weapons could cause to civilians and combatants. Conventional weapons are any weapons that can be used without excessively injurious and indiscriminate effects, or those that have not been prohibited by convention.[7] Non-conventional weapons are those that have been prohibited by UN conventions, such as Weapons of Mass Destruction (WMD), which include biological, chemical, and nuclear weapons.[8] Non-conventional weapons are prohibited from being used due to the unnecessary suffering and harm they may cause to current and future generations.

All member States that have signed the conventions preventing non-conventional weapons share that responsibility, because the consequences of using these weapons may transcend national borders.[9] This means that the consequences will not be limited to the States in conflict and will likely affect others. For example, when any State uses a nuclear weapon, radioactive fallout can travel through the air to neighbouring States, and have both immediate and long-term impacts. The World Health Organization (WHO) adopted a major report in 1987 regarding the use of nuclear weapons, which concluded that they have serious impacts on human health:

> The report noted *inter alia* that the blast wave, thermal wave, radiation and radioactive fallout generated by nuclear explosions have devastating short- and long-term effects on the human body, and that existing health services are not equipped to alleviate these effects in any significant way.[10]

International law divides weapons that can be used in conflict based on the fundamental principles of the law of armed conflict, such as distinction, military necessity, proportionality, and unnecessary suffering.[11] Therefore, non-conventional weapons are used less often and are considered to be less dangerous to civilians because their use is regulated nationally or internationally, and any party who violates those regulations are likely to be subject to prosecution before international or domestic courts. However, more recently, a new generation of weapons has emerged that is capable of launching attacks through cyberspace to target computer systems and achieve results comparable to traditional weapons.

---

6 'Weapons of Mass Destruction' (*United Nations*) <https://www.un.org/disarmament/wmd/> accessed 5 January 2024; See also, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects as amended on 21 December 2001 (adopted 10 October 1980, entered into force 2 December 1983) 2260 UNTS 82.

7 International Committee of the Red Cross, '1980 Convention on Certain Conventional Weapons: Legal Factsheet' (*ICRC*) <https://www.icrc.org/en/document/1980-convention-certain-conventional-weapons> accessed 5 January 2024.

8 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (opened for signature 13 January 1993, entered into force 29 April 1997) 1974 UNTS 45.

9 Treaty on the Prohibition of Nuclear Weapons (opened for signature 20 September 2017, entered into force 22 January 2021) UN Doc A/CONF.229/2017/8.

10 International Committee of the Red Cross, 'Humanitarian Impacts and Risks of Use of Nuclear Weapons' (ICRC, 29 August 2020) <https://www.icrc.org/en/document/humanitarian-impacts-and-risks-use-nuclear-weapons#_ednref3> accessed 5 January 2024.

11 Sean Watts, 'Regulation-Tolerant Weapons, Regulation-Resistant Weapons and the Law of War' (2015) 91 International Law Studies 540, 543; See also Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts* (Bloomsbury Publishing 2008) 46.

Cyber weapons represent a new generation of weapons capable of launching attacks through cyberspace to disrupt computer systems and achieve desired outcomes. Unlike conventional and non-conventional weapons, cyber weapons possess unique characteristics that make them particularly complex. During the war against Ukraine, Russia has used weapons that can effectively target and inflict damage on desired objectives while operating covertly, leaving minimal traces of attribution. Consequently, cyber weapons have emerged as powerful tools in contemporary conflicts, significantly contributing to the destabilisation of the international community. Their impact extends to the compromise of State infrastructures, including transportation and healthcare systems, and their deployment as malware to target nuclear programs.[12]

III. Cyber weapons

A cyber weapon is malware or computer code designed to be used and damage the structure or operation system of any program run by a computer,[13] that has 'the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings'.[14] This malware is usually used to attack and destroy information systems or cause physical damage. Malware or cyber weapons have been used on numerous occasions to cause direct physical damage (such as in the 2010 cyber attack against Natanz in Iran),[15] or to change information or the results of an election (such as in the 2014 Ukraine parliamentary elections).[16] Therefore, cyber weapons can be deployed for both political and military purposes.

There are numerous instances where cyber weapons have been deployed. The first malware called Stuxnet was used as a cyber weapon against the nuclear program in Iran. Stuxnet was developed by NSA and Israel's Unit 8200.[17] It was a worm capable of attacking a target connected to the public internet, and it could also attack through a USB drive or a connection with a shared printer to access Windows systems running WinCC and PCS 7 programs. Simply put, it was a new generation of malware.[18] This worm was designed to sabotage the Iranian nuclear program and prevent Iran from enriching uranium to develop nuclear weapons. In the first month of his presidency, Barack Obama ordered that this malware be used against Iran.[19] The purpose of Stuxnet was to attack the

---

12 International Committee of the Red Cross, 'Cyber Warfare: Does International Humanitarian Law Apply?' (*ICRC*, 25 February 2021) <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law> accessed 5 January 2024.

13 Peeter Lorents and Rain Ottis, 'Knowledge Based Framework for Cyber Weapons and Conflict' (paper presented at the Conference on Cyber Conflict, Tallinn, Estonia, 2010) 139 <https://ccdcoe.org/uploads/2018/10/Lorents-et-al-Knowledge-Based-Framework-for-Cyber-Weapons-and-Conflict.pdf> accessed 5 January 2024.

14 Emilio Iasiello, 'Are Cyber Weapons Effective Military Tools?' (2015) 7(1) Military and Strategic Affairs 23, 24.

15 James P Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War' (2011) 53(1) Survival 23.

16 Tim Maurer, 'Cyber Proxies and the Crisis in Ukraine' in Kenneth Geers (ed), *Cyber War in Perspective: Russian Aggression against Ukraine* (NATO CCD COE Publications 2015) 81.

17 David E Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Broadway Books 2019) 9.

18 Josh Fruhlinger, 'Stuxnet Explained: the First Known Cyberweapon' (*CSO Online*, 31 August 2022) <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html> accessed 5 January 2024.

19 David E Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran' (*The New York Times*, 1 June 2012) <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all> accessed 5 January 2024.

Programmable Logic Controller (PLC) at the Natanz nuclear program in Iran.[20] In 2010, the attack achieved its purpose of destroying a large number of centrifuges.

Stuxnet's development was a revolution in modern warfare in several important ways, including the cost of the attack, the results, and the legal responsibility. Compared with a physical attack, the use of a cyber weapon is much easier. For example, in 1981, Israel attacked the Iraqi nuclear program using a surprise airstrike, which carried significant risk factors. For instance, the mission could have failed if Iraq had managed to shoot down Israel's aircraft. Additionally, if the aircraft were intercepted while crossing the airspace of Arab countries to Iraq, it could potentially have escalated tensions and cause conflicts with those countries. This attack killed eleven Iraqi soldiers and civilians,[21] and was a clear violation of Iraq's sovereignty and international law. Thus, Israel clashed with the international community as the attack was a breach of Article 2(4) of the UN Charter.[22] The attack was also a violation of the 1974 General Assembly resolution that defined the crime of aggression as 'bombardment by the armed forces of a State against the territory of another state or the use of any weapons by a State against the territory of another State'. When Iraq had launched a missile attack against Israel in 1991 during the second Gulf War, some experts argued that it was Iraq's response to what had happened in 1981.[23]

More recently, on 3 January 2020, the US launched an airstrike on Baghdad to assassinate the Iranian Quds Force commander Qassem Soleimani, and the Popular Mobilization Forces' (PMF) deputy chief Abu Mahdi al-Muhandis.[24] Although the attack took place in Iraq, outside Iranian territory, and both States were thousands of kilometres away from the US, Iran responded by launching ballistic missiles against the US base in Iraq.[25] This was Iran's response to an attack by the US, and the chosen target was within range of Iran's missiles. Iran launched another retaliation attack in cyberspace, this time against Israel. In March 2022, 'two Israeli media outlets were hacked […] with warnings from an Iranian propaganda video linked to the second anniversary of the assassination of top general Qassem Soleimani'.[26] Although this cyber attack caused no physical damage, it was a clear threat to Israel's national security, showing that Iran was capable of breaching Israel's information security at will. These two examples show that the US needs to consider that some States, like Iran, could use military force to respond to a direct attack, while also attacking via cyberspace if the target is outside the range of its missiles. In this

---

[20] Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment' (2013) 36(1) Journal of Strategic Studies 120.

[21] P W Singer, 'Stuxnet and its Hidden Lessons on the Ethics of Cyberweapons' (2015) 47(1) Case Western Reserve Journal of International Law 79, 85.

[22] Målfrid Braut-Hegghammer, 'Revisiting Osirak: Preventive Attacks and Nuclear Proliferation Risks' (2011) 36(1) *International Security* 101, 116.

[23] Avner Cohen and Benjamin Frankel, 'Gulf War Saved Iraq From Nuclear Attack: Mideast: Israelis have been Spared from Having to Use their Ultimate Weapons against a Difficult Foe' (*Los Angeles Times*, 22 February 1991) <https://www.latimes.com/archives/la-xpm-1991-02-22-me-1449-story.html> accessed 5 January 2024.

[24] 'Intelligence Briefing: A Thousand Hezbollahs: Iraq's Emerging Militia State' (*New Lines Institute*, 4 May 2021) <https://newlinesinstitute.org/iraq/a-thousand-hezbollahs-iraqs-emerging-militia-state/> accessed 5 January 2024.

[25] 60 Minutes, 'Never-Before-Seen Video of the Attack on Al Asad Airbase' (28 February 2021) <https://www.youtube.com/watch?v=lGP7hZQuTL0> accessed 5 January 2024.

[26] Toi Staff, 'Jerusalem Post Website Hacked with Iran Warning on Anniversary of Soleimani Killing' (*The Times of Israel*, 3 January 2022) <https://www.timesofisrael.com/israeli-news-sites-hacked-with-iran-warning-on-anniversary-of-soleimani-killing/> accessed 5 January 2024.

way, as in this study, the cyber attacks by Russia against third-party countries need to be categorised as a use of force if they are for military purposes.

IV. The differences between cyber weapons and other weapons

A cyber weapon is different from other weapons, in that it can be hidden and the perpetrator can be anonymous. The Stuxnet attack on the nuclear program in Iran illustrates this difference. The attack was hidden for a long time, and Iran did not suspect that it had happened because their system was not linked to the internet.[27] The attack also showed the progress of the development of cyber weapons, which can damage not only computer systems but hardware as well.[28] Cyber weapons have affected many States' elections by changing the outcomes to make the losers of elections actually the winners, such as what happened in the 2020 US elections and the 2014 Ukraine elections. Even in 2016, the US Intelligence Community (USIC) claimed that Russia was responsible for hacking political organisations to influence the outcome of the US elections.[29] In this case, the hackers' success resulted in consequences both within and outside the US, undermining democracy and international law.[30] For these reasons, cyber weapons must be given urgent attention by the international community.

V. The position of international law

a. The use of force in international law and cyber warfare

In Article 2(4) of the UN Charter, the prevention of the use of force is mentioned as the main principle of international law. It mandates that

> all members [of the United Nations] shall refrain in their international relations from the 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.

The international community admits that the use of force in Article 2(4) covers the prohibition of the use of conventional and non-conventional weapons such as 'bacteriological, biological and chemical devices and nuclear and thermonuclear weapons'.[31] However, the term 'force' as mentioned in Article 2(4) is not precisely defined and its exact meaning remains unclear.

The definition of force is important for international peace and security, as leaving it undefined makes international law unable to maintain international peace by preventing new generations of weapons from being used in international conflicts. Neither the UN Charter, the International Court of Justice (ICJ) nor the General Assembly have clearly defined whether the use of force is limited to armed force or whether it can include other forms of warfare.[32] This unclear definition has led to a debate between scholars to define the term, some of whom have defined force as 'any action by a state in breach of the norms of international law as stated in the UN Charter and in other international conventions.

---

27 Singer (n 21) 82.

28 ibid 83.

29 'Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security' (*Homeland Security*, 7 October 2016) <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> accessed 5 January 2024.

30 David P Fidler, 'The US Election Hacks, Cybersecurity, and International Law' (2016) 110 American Journal of International Law (2016) 337.

31 Christopher C Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12(5) European Journal of International Law 825.

32 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War, Vol. 92* (Cambridge University Press 2012) 40.

This may include the use of military, financial, or political methods'.[33] However, the term 'force' is mentioned in the UN Charter's preamble and Articles 41 and 46 as an armed force. Although in some of the articles of the UN Charter (such as in Article 44), the term has been expressed as 'force' without the adjective 'armed', the force in this Article means armed force.[34] Article 51 of the UN Charter authorises the Security Council to take the necessary measures to 'maintain international peace' and security as an inherent right to self-defence in case of any armed attack against the member States. In this Article, UN members' authorisation to use force is clear: the meaning of 'force' here is armed force.

In several cases, the ICJ has interpreted the use of 'force' as meaning armed forces, such as in the *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*.[35] In this case, the ICJ considered that the US violated Article 2(4) of the UN Charter and customary international law when the US supported the *contra* rebels against the legitimate government in Nicaragua and mined Nicaraguan ports. The ICJ considered the US as responsible for any direct and indirect involvement in the use of force. However, the ICJ determined that providing funds to the *contra* rebels was not a breach of the UN Charter, or of customary international law.[36] This case confirms that 'force' as defined in the UN Charter refers to armed force: the ICJ determined the mining of Nicaraguan ports to be a violation of Article 2(4), but the provision of funding to the rebels was not.

Therefore, the question arises: can cyber weapons such as Stuxnet, Trojan horses, viruses, or worms be considered as 'armed force' under current international legal rules and be covered by Article 2(4) of the UN Charter? Cyber warfare is interwoven with conventional weapons and the use of cyber weapons in the cyberspace can cause physical damage, just as damage is caused by the use of armed force in the physical space. Both can be considered to be armed attacks. To explain when the use of cyber weapons can be covered by Article 2(4) of the UN Charter, the next section will discuss the use of cyber weapons from the perspective of international law.

b. The use of cyber weapons and international law

From the perspective of international law, the question of whether cyber operations can be considered a use of force under Article 2 of the UN Charter is a matter of complexity and significance. In 1996, the ICJ considered the prevention of the use of force as applying 'to any use of force, regardless of the weapons employed'.[37] This opinion seems to make the point that there is no limit to the definition of the use of force, which means cyber operations could fall within the definition. However, there are differing opinions. In 2021, François observed that almost all commentators ended up with three main approaches for cyber operations that qualified as a use of force according to Article 2 of the UN Charter.[38] These three main approaches are based on the target, the instrument, and the consequences of the cyber operation. Under the target approach, to consider a cyber operation use of

---

[33] Oxford Dictionaries, *Oxford English Dictionary, Vol. 7* (Oxford University Press 2013) 235.

[34] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 45.

[35] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14.

[36] Dinniss (n 32) 50.

[37] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226.

[38] François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' (paper presented at the 13th International Conference on Cyber Conflict (CyCon), 2021) 288 <https://ccdcoe.org/uploads/2021/05/CyCon_2021_Delerue.pdf> accessed 5 January 2024.

force, the target penetrated must be critical national infrastructure. This is based on the legal doctrine of self-defence, since when critical infrastructure is attacked, the State can consider the attack as a use of force against its territory. In such cases, the State can use force for self-defence.[39] However, the question here is how to determine 'critical national infrastructure'.

For instance, Section 1016 of the 2001 US Patriot Act defines critical infrastructure as

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[40]

Here, it is clear that any attack against US interests, whether in physical or virtual space, is a use of force. Under international law, the US has a right to self-defence when this occurs. In August 2012, there was a cyber attack virus launched on the Saudi oil company *Aramco*, which destroyed data on almost 30,000 computers.[41] While *Aramco* is one of the largest oil producers in the world and the attack caused a lack of oil leading to global power shortages, some scholars argued that the destruction of data did not qualify as a use of force.[42] In this instance, the target approach was used, and the cyber attack was not considered a use of force because the oil company did not meet the definition of 'critical national infrastructure'.

As previously discussed, the instruments used in cyber operations are viruses or codes (malware) used to attack computers and cause damage to the data or physical damage to the hardware. These instruments are very hard to identify, especially with the rapid development of technologies, which makes it difficult to determine which software should be counted as a weapon that qualifies as a use of force. Therefore, focusing on the consequences of a cyber attack helps determine whether a cyber operation qualifies as a use of force.

Adopting the consequences of cyber operations as the determinant is a good strategy when considering cyber operations as a breach of Article 2 of the UN Charter. This strategy is based on whether the cyber operation caused virtual damage, physical destruction, or death. If any of the aforementioned types of destruction happened, the operation will be considered a use of force that breaches Article 2 of the UN Charter, as the US and most scholars have adopted.[43] As technology is currently part of everyday life, and systems such as health systems, power stations, and other things required for human life could be affected by cyber operations, then a cyber attack could indirectly cause death, injury, or physical damage. The indirect effect does not mean that the cyber operation is not a military intervention, because 'in the Nicaragua judgment, the ICJ expressly recognized that intervention that uses armed force can occur either directly or indirectly'.[44]

---

39 Delerue (n 38) 288.

40 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001 (2001) 115 STAT 273.

41 'Saudi Aramco says Cyber Attack Targeted Kingdom's Economy' (*Alarabiya News*, 9 December 2012) <http://www.alarabiya.net/articles/2012/12/09/254162.html> accessed 5 January 2024.

42 Michael N Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (The National Academies Press 2010) 151, 164.

43 Delerue (n 38) 288.

44 *Nicaragua v United States of America* (n 35); See also Roscini (n 34) 50.

This judgment clearly explains that the member States of the UN are prohibited from being involved in any kind of threat or use of force. So long as a cyber attack has the ability to cause physical damage, breach information privacy, or cause economic damage, it is prohibited under Article 2(4) of the UN Charter. However, the question here is whether the cyber attack can come under the jurisdiction of international law regardless of the accused, or whether it must be committed by a State to be considered a use of force according to Article 2(4) of the UN Charter. In this case, the attack must be launched by a State, as non-State actors are not subject to international law, and the cyber operation must have the potential to cause physical damage, breach information privacy, or cause economic damage as mentioned above. In addition, the use of cyber weapons must be used in international relations in order to be a breach of Article 2(4) of the UN Charter.

VI. Russian cyber operations on third-party countries

a. Overview of Russia's cyber operations during the war with Ukraine

At the beginning of an armed conflict between Russia and Ukraine, offensive cyber operations may hold significant importance.[45] However, when the situation turned on hostilities and the shooting war started, the role of cyber warfare diminishes and becomes an 'auxiliary role'.[46] This is unlike traditional military weapons, as the traditional weapons can physically occupy territory or consistently cause widespread destruction on an industrial scale. While numerous scholars and intelligence staff described the cyber operations as 'failed strategically in disabling Ukraine's defences'.[47] Western government officials argued that Russian cyber operations were extensive and strategically effective, which resulted in the destabilisation and intimidation of the Ukrainian government, armed forces, and civilian population.[48] Jon Bateman mentioned the views of several officials regarding the impact of Russia's cyber operations in the war against Ukraine.[49] In April 2022, David Cattler and Daniel Black, acting intelligence officials with NATO, contended that cyber operations had been Russia's most significant military success in the war against Ukraine. Jeremy Fleming, the director of the UK's General Communications Headquarters (GCHQ), dismissed the notion that cyber operations had not played a role, calling it a fallacy. Additionally, Matt Olsen, the US Assistant Attorney General for national security, went so far as to describe the situation as 'a hot cyberwar carried out by the Russians'.[50] The impact of Russia's cyber operations during the war against Ukraine highlights a significant aspect: Russia reduced its cyber operations directed at Ukraine while intensifying them against third-party countries. This shift in cyber operations allowed Russia to pursue its foreign policy objectives by attempting to minimise or restrict any

---

45 Ariel Eli Levite, Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict (*Carnegie Endowment for International Peace*, 18 April 2023) 10 <https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544> accessed 5 January 2024.

46 ibid.

47 Jon Bateman, 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications' (*Carnegie Endowment for International Pe*ace, 16 December 2022) 5 <https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657> accessed 5 January 2024.

48 ibid.

49 ibid.

50 ibid.

support to Ukraine, to undermine international opposition to its actions and achieve its military goal on the ground in Ukraine.

b. Targeting third-party States

The Russian government has engaged in harmful cyber activities for cyber espionage, suppressing specific social and political entities and harming regional and international third-party States due to their support of Ukraine.[51] During the war with Ukraine, Russia launched cyber attacks against third-party States. In first quarter of 2023, the Cyber Peace Institute stated that 575 cyber attacks targeted three main sectors, ie public administration, transportation, and financial sector, which were mainly located in Poland, the US, and Germany.[52] Russia attacked these States and others in the cyberspace to deter their support for Ukraine, and to let the Russian troops on the ground gain advantage in the war. Russia strategically utilised cyber attacks as a means of launching war by subverting the infrastructure of third-party States. This approach provides an alternative to traditional diplomacy, producing outcomes akin to warfare but with reduced costs and risks. Specifically, subversion plays a significant role in cyber operations targeting third-party countries actively supporting the war in Ukraine against Russia. These cyber operations, backed by Russia, leverage cyberspace to deter and weaken these third-party countries, thereby alleviating pressure on Ukrainian resistance forces and allowing Russia to gain an advantage on the ground. In addition, cyber warfare has appeared as a powerful weapon in the recent Israel-Palestine conflict, with digital attacks paralleling physical combat.[53] The conflict saw cyber attacks on crucial infrastructure, media websites, and emergency services on both sides of the crisis. During this war, different cyber groups, including some of these groups linked to Russia, actively targeted Israeli government systems. Some attacks were ideologically driven, while others were aimed at financial gain. Notably, the Israeli cyber police froze Hamas' cryptocurrency channels to disrupt their funding, as Hamas had received around $21 million in cryptocurrency since 2021.[54] This underscores the evolving role of cyber warfare in contemporary conflicts.

VII. Ethical consequences

The development of computer technology showed the need for the international community to have ethics regarding cyber conflict and the use of computers in general[55] due to the potential dangers and instability caused by the use of cyber weapons. These ethical policies could range from the 'no first use' of cyber weapons (like any other dangerous weapons), to allowing the use of cyber weapons for proportionate response to other cyber attacks, or the complete prohibition of cyber weapons, as their potential impact could be equal to weapons of mass destruction.[56]

---

51 'Cybersecurity and Infrastructure Security Agency' (*Cybersecurity & Infrastructure Security Agency*, 2023) <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia> accessed 5 January 2024.

52 Cyber Peace Institute (n 3).

53 Ante Batovic, 'Middle Eastern Conflict Reflects Global and Evolving Nature of Cyber Warfare' (*Crisis24*, 13 October 2023) <https://crisis24.garda.com/insights-intelligence/insights/articles/middle-eastern-conflict-reflects-global-and-evolving-nature-of-cyber-warfare> accessed 5 January 2024.

54 ibid.

55 Neil C Rowe, 'Ethics of Cyber War Attacks' in Lech Janczewski and Andrew Colarik (eds), *Cyber Warfare and Cyber Terrorism* (IGI Global 2007) 105, 109.

56 John Arquilla, 'Ethics and Information Warfare' in Z Khalilzad, J White and A Marshall (eds), *The Changing Role of Information in Warfare* (RAND Corporation 1999) 379, 396.

There are numerous incidents that show the need for ethics. In 2010, the US and Israel developed and used Stuxnet to attack Iran's nuclear program, which was considered an attack on the sovereignty of Iran. This cyber attack was launched because both the US and Israel believed Iran was developing the program for military use, not just for civil purposes. This attack against the Iranian nuclear program was a breach of the UN Charter's prevention of the use of force. There was no evidence that the program would be for military use because Iran has the right to construct a nuclear program for civil purposes.[57] Therefore, to stop the program and avoid contravening Article 2 of the UN Charter, the US used a cyber attack, cleverly attacking and destroying the program without legal consequences as long as the attackers remained anonymous. Later, however, this cyber weapon became the basis for establishing a new generation of weapons that increased illegal activities all over the world. Discovering this cyber attack on Iran's nuclear program led cyber security researchers to begin research to design code that could be used for illegal activities. In addition, personal information became susceptible to cyber weapons as cyber criminals learned to easily hack the information and use it for illegal activities.[58]

The consequences of Stuxnet were unexpected. Both developed and developing third-nations began a race to create and use cyber weapons. Although the US and Israel tried to prevent Iran from building nuclear capability, neither country had anticipated that after the discovery of Stuxnet, Iran would begin to develop cyber weapons.[59] According to computer security experts, the Stuxnet attack did not prevent Iran from developing nuclear power, but it delayed the programme for two years at best. Stuxnet's discovery was a turning point and a revolution in the history of cyber weapons, as many States began to develop cyber weapons to curb future cyber attacks. This implies that the cyber attack resulted in an increase in activity overall. Another unexpected result was the possibility of out-of-control cyber weapons causing damage to other sectors, which occurred when Stuxnet, directed at Iranian nuclear facilities, infected other States' facilities.[60] According to Eugene Kaspersky, 'Stuxnet had "badly infected" the internal network of a Russian nuclear plant after the sophisticated malware caused chaos in Iran's uranium facilities in Natanz'.[61] This case shows how even the designers of cyber weapons can find it hard to control them.

The use of cyber weapons caused a delay in counterterrorism, and terrorists started to use these weapons in their activities. In June 2015, the first International Conference on Computer Security in a Nuclear World discussed the capacity of terrorist groups to use cyber weapons, and it was noted that the cyber capabilities of ISIS (the Islamic State in Iraq and Syria) had recently increased.[62] Furthermore, in 2015, the US official security department revealed that ISIS had attempted to hack the US power system. Hence, this is one of Stuxnet's main consequences: terrorists and other non-State actors can obtain the technology from private companies and use it to threaten a State's stability.

---

57 International Atomic Energy Agency, 'The Texts of the Agency's Agreements with the United Nations' (1959 October 30) UN Doc INFCIRC/11.

58 Arquilla (n 56) 216.

59 Farwell and Rohozinski (n 15) 24-35.

60 Phil Muncaster, 'Stuxnet Infected Russian Nuke Power Plant – Kaspersky' (*The Register*, 11 November 2023) <https://www.theregister.com/2013/11/11/kaspersky_nuclear_plant_infected_stuxnet/> accessed 6 January 2024.

61 ibid.

62 ibid.

VIII. Conclusion

This study concludes that the use of cyber weapons must be defined as a use of force in all operations because, although they are virtual weapons that perpetrators use in cyberspace, they are nonetheless used as weapons. Moreover, there must be a clear definition of 'force' in international law because leaving the definition uncertain may allow cyber weapons and other weapons developed in the future to remain outside the scope of international law. The current definition of 'critical infrastructure' leaves a gap that perpetrators could use when attacking any State. In addition, the use of force for self-defence is further complicated due to the lack of clarity as to whether or not the infrastructure attacked is considered 'critical infrastructure.' The use of cyber weapons will have consequences for international peace and security as these types of weapons are available for the use of both State and non-State actors.

The use and availability of cyber weapons for all States, whether developed or developing States, raises numerous genuine moral questions and international legal issues, given that they can cause enormous destruction at much less cost than traditional weapons. Fewer civilian casualties occur from cyber weapons in comparison to operations that use conventional weapons, such as Israel's operation in 1981 against Iraq's nuclear program by conventional weapons, which caused the death of 11 civilians and soldiers. On the other hand, the 2010 cyber attack against the Iranian nuclear program did not kill anyone but achieved the same result, which (when looking at the attack from a consequences approach) means the use of the cyber weapon should be considered equal to conventional weapons. However, their use by terrorist organisations undermines counterterrorism efforts, because terrorist groups and non-State actors find cyber weapons easy to use in their activities. Overall, the evolving role of cyber operations and Russia's targeting of third-party States during the war with Ukraine underscore the complex and multifaceted nature of modern warfare. These cyber operations have demonstrated the potential for significant impact beyond conventional military means, posing new challenges to international security and necessitating a comprehensive understanding of cyber warfare in the context of armed conflicts.

In addition, the discussion in this study shows an important point regarding the future of cyber weapons. Cyber weapons still need more legislation regarding ethics because they have the capacity to attack computer systems, leaving computerised systems (such as States' health systems) as well as human lives in a vulnerable state. Failing to consider cyber weapons as a high priority in ethics and law will directly endanger human lives.

****