Advances in Economics, Business and Management Research, volume 215
Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)

The Legal Dilemma and Countermeasures of the Attribution of Cyber Terrorism Attack

Yajie Wang[1, *]

[1] *School of law, Guangxi Normal University, Guilin, Guangxi, China*
[*] *Corresponding author. Email: 2019211443@mail.chzu.edu.cn*

ABSTRACT
With the continuous globalization of network information, it is urgent to prevent terrorist attacks in the field of non-traditional security. Because cyber terrorist attacks will occur in a very short time, it will become very difficult to establish the subject identity of belligerents in cyber terrorist attacks and the application of the basic principles of war law in cyber terrorist attacks. It is very important to clearly define cyber terrorist attacks and find a way to deal with them.

Keywords: *Cyber terrorist attacks, International humanitarian law, Imputation of legal liability*

1. INTRODUCTION

The first to put forward the term "cyber terrorism" was Berlin Colin, who was engaged in intelligence and security research. Berlin Colin understood cyber terrorism as "the product of the combination of cyber and terrorism."[1] (The Future of Cyberterrorism, Crime and Justice International.) For the first time, the UN Security Council clearly strengthened the fight against cyber terrorism and the relevant discourses are corresponding to Resolution 2129 adopted by the Security Council To reflect.[2]The European Council's "Convention on the Prevention of Terrorism" on terrorist crimes, and the United Nations Security Council Resolution 1624 on incitement to commit terrorist acts all have relevant provisions on the criminal record of combating cyber terrorism.The center for strategic and international studies of the United States defines cyber terrorism as the use of computer network tools to shut down key national infrastructure (such as energy, transportation, government operations) or force or intimidate the government or civilians [3].

To sum up, the definition of the connotation and extension of "cyber terrorist attack" has not yet formed a unified conclusion in theory and practice. However, to explore the problem of responsibility identification in cyber terrorist attacks, the first thing to be solved is to judge what activities constitute "cyber terrorist attacks". Therefore, this paper will first define the concept of cyber terrorist attack based on the definition of cyber terrorist attack in current international law, and then put forward corresponding countermeasures on this basis.

2. INTERNATIONAL LAWS RELATED TO CYBER TERRORIST ATTACKS

"The majority of states and scholars do not recognize a customary crime of terrorism, but Antonio Cassese argue that terrorism is already a crime in customary international law."[4] Because there are not many international conventions related to cyber terrorist attacks, the author decided to sort them out by finding sectoral conventions against terrorist attacks.

In Article 3(a) of Article 1 of the International Convention for the suppression of terrorist bombings, it is mentioned that an explosive or incremental wapon or device that is designed, or has the capability, to cause death, serious body injury or material damage.When the explosive or explosive weapon is triggered through the network and may cause an explosion of nuclear facilities. Then such terrorist attacks can be regarded as cyber terrorist attacks. "Investigators probing the Paris attacks have found video footage of a senior Belgian nuclear official, a Belgian prosecutor confirmed." [5] This news shows that terrorist attacks may be carried out through the Internet, and the target of attacks may be nuclear power plants, which will lead to very serious consequences.

Of course, cyber terrorist attacks may also be carried out by attacking civil aircraft, endangering the aircraft itself, passengers and staff on the aircraft. So in this case, it may violate Article 11(1) of the "Convention on Crimes and Certain Other Acts Committed on Board Aircraft"

Copyright © 2022 The Authors. Published by Atlantis Press International B.V.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/

(Tokyo Convention) signed in Tokyo on September 14, 1963.[6] The contracting state can take measures to stop such terrorist attacks using the network.

Therefore, in my opinion, cyber terrorist attacks actually belong to a sub branch of terrorist attacks, and their acts are illegal. Such activities may also target ordinary civilians, and terrorist attacks do not deliberately distinguish between civilians and attack everyone. Such cyber terrorist attacks often have political purposes and create fear through organized and planned terrorist attacks. So as to achieve the purpose of realizing its political intention. Therefore, cyber terrorist attacks must be dealt with and resisted through the joint efforts of all countries.

3. LEGAL DILEMMA OF LIABILITY ATTRIBUTION OF CYBER TERRORIST ATTACKS

The essence of responsibility for cyber terrorist attacks is to assign such wrongful acts to one or more countries, so as to require them to bear international legal responsibility."Attribution in the law of state responsibility determinants are moulded by how the state is defined, which in the law of state responsibility is reduced to the structures, entities and functions that make up its legal-political order. This makes the legal determinants of attribution requiring an identifiable, direct and close link between a state and an entity or between a state and the impugned conduct. This occurs when an institutional, functional or agency link between a state and an entity or conduct is established."[7]Therefore, in this case, it is particularly important to find the subject who launched the cyber terrorist attack.Regardless of whether the main body of the cyber terrorist attack is led by the government of a country, or by a non-state actor outside the country's leading factor. At the same time, it is also a very important thing to find the relevant laws to attribute the responsibility for cyber terrorist attacks. International humanitarian law is undoubtedly the most appropriate if the victim country wants to adopt laws to hold the cyber terrorist attacks accountable.Therefore, in the following analysis and combing, these problems mentioned above are discussed one by one.

3.1. It is difficult to establish the subject identity of belligerents in cyber terrorist attacks

Cyber terrorist attacks, generally speaking, will be completed in an instant. "To spot a cyber attacker from all the normal cross-border data flows would be like picking out a single person with more luggage than usual from the thousands of passengers that pass through Airport daily."[8] The network system of the attacked country will trigger the corresponding self-defense system for defense. In this case, because both offensive and defensive sides complete the transformation in a very short time. At the time of boundary, it is difficult to accurately distinguish which party is the subject of attack and which party is the subject of defense. Therefore, if the identity of the belligerent cannot be confirmed, the subject of responsibility attribution cannot be found. In other words, in this case, the evidence has been lost. If no state takes the initiative to be responsible for such acts, the attacked state can only deal with and deal with the aftermath of the terrorist attacks.

In addition, there is another possibility that the subject of cyber terrorist attacks is not a national government. In other words, it is not directly authorized by the government. Then, some countries can secretly achieve the purpose of cyber terrorist attacks on the pretext that they are not carried out by themselves. Moreover, in the process of doing so, the country launching cyber terrorist attacks will deliberately transfer or hide its positioning system. In this case, it will be very difficult for the initiating state to recognize its own cyber terrorist attacks, or for the injured state to find and pursue responsibility for cyber terrorist attacks.

3.2. The basic principles of international humanitarian law are difficult to apply in cyber terrorist attacks

3.2.1. Application of basic principles of international humanitarian law in cyber terrorist attacks

Generally speaking, the basic principles of international humanitarian law can be divided into two aspects: the principle of wartime conduct and the implementation of the basic principles of international humanitarian law. Because the author discusses the attribution of cyber terrorist attacks in this paper, the author only analyzes and combs the application of the wartime behavior principle in international humanitarian law in cyber terrorist attacks.

According to the description of the principles of international humanitarian law in the 1996 advisory opinion of the International Court of justice on the legality of the threat or use of nuclear weapons, the main principles of international humanitarian law include: first, the protection of civilians and civilian targets, and the distinction between combatants and non combatants. In this principle, it is mainly emphasized that the weapons used shall not make it impossible to distinguish between civilian and military targets. Secondly, it is prohibited to cause unnecessary suffering to combatants. In this principle, it shows a problem that the means by which countries use weapons are not unlimited.

Firstly, when the principle of distinction is applied to international humanitarian law, it is consistent with the law of war to strike military targets and destroy the

enemy in a state of war. However, when the target is not a military target, it is inconsistent with the basic principles of international humanitarian law. For example, indiscriminate attacks have affected civilians, churches, schools, hospitals, the Red Cross and so on. Then, the attack, in this case, should be recognized as a wrongful act, and the consequences of its act should be investigated for responsibility in law.

Secondly, the principle of unnecessary sufferings is often used in international humanitarian law. This principle reveals the purpose of war and the way of fighting. Specifically, if the weapons or methods used in war can achieve military purposes, then we can no longer continue to fight uncontrollably. For example, if the method used makes it impossible for the enemy to continue the confrontation and achieve the established military purpose, it should be stopped at this time. In the cyber terrorist attack, when the initiator stops the attack, the adverse consequences of the attack continue. It even brings irreversible and irreparable suffering to combatants, civilians or anyone else. Then the combat mode in this case violates the principle of unnecessary pain, and its behavior should be required to bear corresponding responsibility.

3.2.2. The dilemma of the application of the basic principles of international humanitarian law in cyber terrorist attacks

Using the principle of distinction in international humanitarian law, the law can attribute the attacks for non military purposes, but the attribute of the technology used in cyber terrorist attacks is difficult to determine. Because it is not easy to confirm whether a technology is designed for military purposes or used for military purposes. For example, in the press release issued by the International Committee of the Red Cross on January 19, 2022, it was mentioned that the computer server of the International Committee of the Red Cross storing information was attacked by a network, which affected the personal data and confidential information of more than 515,000 people in at least 60 countries. The people involved in this information are extremely vulnerable groups, not military personnel. Then, this kind of cyber attack is still such a terrible consequence, not to mention the consequence of cyber terrorist attack.

In addition, indiscriminate or disproportionate attacks or threats are prohibited under customary international law. Therefore, "when an object can be used for both military and civilian purposes, people may think that even if it is indirectly used for military purposes, it should be regarded as a military target."[9] Then, in this case, it will be difficult to use the basic principles of war law to regulate cybercybernetic attacks. "In particular, if the perpetrator of a given operation and thus the link of the operation to an armed conflict cannot be identified, it is extremely difficult to determine whether IHL is even applicable to the operation."[10]

As for the dilemma of the application of principle of unnecessary sufferings in cyber terrorist attacks, when the initiator of cyber terrorist attacks threatens the residents of the country of the attacked party in the spiritual field by spreading terrorist information, the attacked personnel cannot obtain spiritual cure for a long time after the terrorist attacks. In this case, it will become very difficult to attribute the wrongful act through the principles of international humanitarian law. Because in this case, it will be very difficult to prove the responsibility or bear the responsibility.

3.3. The different capabilities of network data security systems among countries can not be attributed

Due to the different information security capabilities of developed and developing countries. Therefore, when cyber terrorist attacks occur, those countries with poor network data security will not even realize how to distinguish whether their networks have suffered terrorist attacks. Poorly defended systems may, under pressure, leak information, buckle unexpectedly, or provide bad data to warfighters and other decision makers [11]. Then, in this case, it is likely that the victim country of the cyber terrorist attack is the initiator, and the real subject of responsibility cannot be determined.

3.4. Non state actors have difficulty attributing their actions

"Public international law primarily governs the relationship between states. This is no less true when considering its application to cyber activities involving non-state actors, such as individuals, private companies, hacker groups, criminal groups or terrorists."[12]"With non-state terrorist groups being inherently secretive, gathering evidence on terrorist activities is a complicated task."[13] When a country cannot effectively control the rebel organizations and armed conflict organizations in its territory, it is difficult for the organization to bear the responsibility for the terrorist attacks in cyberspace against other countries. Because the government of this country has not even really investigated the information of the originator of the terrorist attack. In other words, the country where the rebel organization is located has no ability to control the terrorist activities launched against other countries within its territory. In this case, even if the state is required to bear responsibility, it will not have any substantive effect. Because, in this case, the state required to assume responsibility is not able to fulfill its responsibility.

The second situation is that the injured state has successfully found the subject of cyber terrorist attacks through the data network. However, because this subject is a non-state actor. Generally speaking, an individual's

behavior cannot be directly attributed to the state. Similarly, the behavior of a non state actor cannot be directly attributed to the state. Only when sufficient evidence is found to prove that the subject who launched the cyber terrorist attack is instructed, ordered or controlled by this country. This non-state actor is required to launch cyber terrorist attacks on the target country. Or a state may take the initiative to show the injured state that it intends to take the initiative to bear the terrible consequences of the cyber terrorist attack launched by this non state actor. Then, in this case, the attribution of responsibility of non-state actors has a way out. However, it is clear that the possibility of requiring a state to be held accountable for the acts of non state actors within its territory is very small. Unless it can be proved by evidence that the behavior of a non state actor is closely related to the state. Otherwise, it will become very difficult to attribute the responsibility of this non-state actor.

4. COUNTERMEASURES TO THE RESPONSIBILITY ATTRIBUTION OF CYBER TERRORIST ATTACKS

4.1. Inversion of burden of proof after cyber terrorist attacks

As mentioned in the previous discussion, it is often difficult to establish the subject identity of belligerents in cyber terrorist attacks. It is also difficult to determine the behavior of a national government in the event of a cyber terrorist attack. Therefore, the inversion of the burden of proof can be used to solve the problem that it is difficult to confirm the identity of the subject of cyber terrorist attacks.

When a cyber terrorist attack occurs, if a country can prove that the source of the attack is caused by a specific country. Then the designated country of origin of the attack needs to bear the responsibility of proving the occurrence of the terrorist attack. That is because “if the harm can be seamlessly linked to the cyber act, a causal link will be established”[14] If it is unable to inform or is not responsible for the request made by the state where the attack occurred. Then, this country needs to assume corresponding responsibilities and fulfill corresponding obligations in international law. This is because the injured state has less evidence of liability than the state that initiated or helped to launch a cyber terrorist attack.

4.2. Counteract retaliation

Network data in each country is usually kept confidential. Therefore, countries can use this advantage to keep their own network systems confidential and fight back against acts that threaten their own cyberspace at an appropriate time. Specifically, if cyber terrorist attacks are led by a country. Then, the attacked country can use the method of national network data confidentiality to encrypt and transfer the data information threatening to enter its own national cyberspace. Next, the attacked country blocks its own cyberspace. In this way, the data information launched by the attacking country can not reach the network data center of the attacked country. Third, the attacked country moves the encrypted data to other unused data platforms, and then decrypts the data. If the data is the data of cyber terrorist attacks initiated by other countries, in the process of decrypting the network data, the attacked countries can directly launch a counterattack after decrypting the data and reverse programming. When the retaliated data is transmitted back to the attacking country, the data is again transferred by the data center of the attacking country. So as to realize a role transformation, that is, the country that launched the attack has also become the country that was attacked.In this way, offsetting retaliation is achieved. Thus, it is no longer necessary to attribute its responsibility. Although in this process, the first attacked country cannot find the subject of responsibility, this way ensures that the attacks of both countries have not achieved their goals.

5. CONCLUSION

This paper analyzes the cyber terrorist attack and puts forward the way to deal with it by reversing the burden of proof and offsetting retaliation. This is of great significance for comprehensively constructing the attribution principles and practical operation standards of cyber terrorist attacks. If it can be implemented, it will help to form a good global response system to cyber terrorist attacks centered on the United Nations. However, cyber terrorist attacks are complex. “The international community must absolutely strike a sensible balance between respecting state sovereignty, on one hand, and combating terrorism efficiently, on the other.”[15] In the wake of cyber terrorist attacks, it is worth considering that some countries may shift responsibility in order to avoid taking responsibility. It may also guide international public opinion, confuse evidence, and lead to problems in the process of accountability. Therefore, the response to cyber terrorist attacks is a problem worthy of further study.

REFERENCES

[1] Collin,B.(1997) The Future of Cyberterrorism. Crime and Justice International, pp. 15-18.

[2] Resolution 2129: “Expressing concern at the increased use, in a globalized society, by terrorists and their supporters of new information and communication technologies, in particular the Internet, for the purposes of recruitment and incitement to commit terrorist acts, as well as for the financing, planning and preparation of their

activities, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law."

[3] Kriangsak kittichaisaree, translated by Cheng Le, Pei Jiamin and Wang min. (2020) Public International Law Of Cyberspace. China democracy and legal system press, Beijing.

[4] See BEN SAUL (2011). Legislating from a Radical Hague: The United Nations Special Tribunal for Lebanon Invents an International Crime of Transnational Terrorism. Leiden Journal of International Law, 24, pp 678.

[5] See Guardian(2016). Paris attacks: suspects had video of Belgian nuclear official, says prosecutor. https://www.theguardian.com/world/2016/feb/18/paris-attacks-suspects-had-video-of-belgian-nuclear-official-says-prosecutor

[6] Article 11(1) of the "Convention on Crimes and Certain Other Acts Committed on Board Aircraft" (Tokyo Convention): When a person on board has unlawfully committed by force or threat thereof an act of interference, seizure, or other wrongful exercise of control of an aircraft in flight or when such an act is about to be committed, Contracting States shall take all appropriate measures to restore control of the aircraft to its lawful commander or to preserve his control of the aircraft.

[7] Tsagourias, N., Farrell, M.(2020)Cyber Attribution: Technical and Legal Approaches and Challenges.European Journal of International Law, Vol. 31 No. 3, 951–952.

[8] Shackelford, S.J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal of international law, Vol.27, No.1:200.

[9] Li,B.J.(2013) On cyber warfare and the application of war law . Law review,4: 63.

[10] International Humanitarian Law and New Weapon Technologies 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011: Keynote address by Dr Jakob Kellenberger, ICRC President, and conclusions by Dr Philip Spoerri, ICRC Director for International Law and Cooperation. (2012). International Review of the Red Cross, 94(886), 811.

[11] Libicki, M. C. (2013) The Broad Effects of Brandishing Cyberattack Capabilities. In Brandishing Cyberattack Capabilities pp. 9.

[12] Schmitt, Michael N. and Watts, Sean and Watts, Sean.(2016)Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. 21 Journal of Conflict and Security Law 1-17 (2016): 2.

[13] Monnheimer, M. (2021). Lessons to Be Learned from the Application of Due Diligence Obligations in Other Fields of International Law. In Due Diligence Obligations in International Human Rights Law,pp. 171.

[14] Nicholas Tsagourias,Giacomo Biggio.(2022) Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force.Cyber Peacekeeping Operations and the Regulation of Force,Vol. 99:58.

[15] Proulx, V.-J. (2017). An Incomplete Revolution: Enhancing the Security Council's Role in Enforcing Counterterrorism Obligations. Journal of International Dispute Settlement, 8:309.