ABSTRACT

Objective: The problem of international electronic terrorism has spread rapidly and affecting nations adversely. However, International Law continues to view the crimes of international terrorism through the Internet and global cyberattacks as ordinary conventional crimes. This perception created an international legal vacuum. Hence, the existence of this legal vacuum in international law to criminalize these acts, which harm the security and sovereignty of states and affect global peace and security, needs to be addressed. Specifically, the study is aimed at answering the following questions: In the event of armed Cyberterrorism, does International law justifies legitimate self-defense? What are the lacunas Regarding Cyberterrorism in International law?

Methods: This study used an empirical approach. An analysis is made in determining whether cyberattacks may be regarded as an armed assault legitimizing the victim states' right to self-defense. Relevant legal text and resources were pulled together to achieve the aim of this research. Hence, a qualitative descriptive analysis of related legal texts and other relevant documents has been conducted.

Results: The research finds that cyberattack is similar to terrorist attack but the medium of the attack is carried out in cyber is on the computer via the internet while the conventional terrorist attack is physically carried out between or among terrorist members and government troops. However, in the cyberattack, the attacker and his location are not known. The international community has not been able to incorporate cyberattack law into International law because there is no consensus from member states on cyberattacks. Shortly, a coordinated cyberattack carried out through the Internet could cause catastrophic destruction to nations that depend on the Internet, particularly in crucial target areas such as transportation, power supply, and telecommunication infrastructures. Consequently, it has been pointed out that cyber warfare operations can fall under the scope of the international crime of aggression.

Conclusion: An existing legal literature on cyberspace terrorism is exposing a conundrum. There are possible avenues for international legal action relating to terrorism. Still, because these attacks have not occurred, states lack opportunities to improve the impact that international law can make proactively. Options, especially enhancing cybersecurity in critical infrastructure, have appeal because they are strategies against cyber intrusions that are ‘all hazards.’ By comparison, there is a lack of reliable solutions for foreign legal activities related to the terrorist use of the Internet and social media. At the same time, this issue has become a concern, and there are opportunities for governments, businesses, and civil societies to mitigate it. This challenging background, which shows no signs of fading, may increase interest in integrating offensive cyberattacks into counter-cyber-facilitated terrorism strategies.

a Jamal Awwad Alkharman, b Isyaku Hassan

a Doctor of Philosophy (PhD), Lecturer, Faculty of Law, Jadara University, Jordan, E-mail: j.alkharman@jadara.edu.jo, Orcid: https://orcid.org/0009-0004-3056-9748
b Doctor of Philosophy (PhD), Lecturer, Faculty of Languages and Communication, Universiti Sultan Zainal Abidin, Malaysia. E-mail: isyaku87@gmail.com, Orcid: https://orcid.org/0000-0002-8260-2894
Keywords: cyberterrorism, international law, self-defense.

CIBERTERRORISMO E AUTODEFESA NO ÂMBITO DO DIREITO INTERNACIONAL

RESUMO

Objetivo: O problema do terrorismo eletrônico internacional se espalhou rapidamente e afetou negativamente as nações. No entanto, o Direito Internacional continua a considerar os crimes de terrorismo internacional através da Internet e os ataques cibernéticos globais como crimes convencionais comuns. Essa percepção criou um vácuo jurídico internacional. Por conseguinte, a existência deste vazio jurídico no direito internacional para criminalizar estes atos, que prejudicam a segurança e a soberania dos Estados e afetam a paz e a segurança mundiais, tem de ser abordada. Especificamente, o estudo visa responder às seguintes perguntas: Em caso de ciberterrorismo armado, o Direito Internacional justifica legítima autodefesa? Quais são as lacunas em relação ao ciberterrorismo no Direito Internacional?

Métodos: Este estudo utilizou uma abordagem empírica. É feita uma análise para determinar se os ataques cibernéticos podem ser considerados como um ataque armado que legitima o direito dos estados vítimas à autodefesa. Foram reunidos textos jurídicos e recursos relevantes para alcançar o objetivo desta investigação. Por conseguinte, foi realizada uma análise qualitativa descritiva de textos jurídicos conexos e de outros documentos relevantes.

Resultados: A pesquisa revela que o ataque cibernético é semelhante ao ataque terrorista, mas o meio do ataque é realizado no computador via internet, enquanto o ataque terrorista convencional é fisicamente realizado entre ou entre membros terroristas e tropas do governo. No entanto, no ataque cibernético, o atacante e sua localização não são conhecidos. A comunidade internacional não tem sido capaz de incorporar a lei de ataques cibernéticos ao Direito Internacional porque não há consenso dos Estados-membros sobre ataques cibernéticos. Em breve, um ataque cibernético coordenado realizado através da Internet poderá causar destruição catastrófica em nações que dependem da Internet, particularmente em áreas-alvo cruciais como transporte, fornecimento de energia e infraestrutura de telecomunicações. Por conseguinte, foi salientado que as operações de guerra cibernética podem ser abrangidas pelo âmbito do crime internacional de agressão.

Conclusão: Uma literatura jurídica existente sobre terrorismo cibernético está expondo um dilema. Há vias possíveis para uma ação judicial internacional relacionada com o terrorismo. Ainda assim, como esses ataques não ocorreram, os estados não têm oportunidades para melhorar o impacto que o direito internacional pode causar de forma proativa. As opções, especialmente para melhorar a segurança cibernética em infraestruturas críticas, são atraentes porque são estratégias contra intrusões cibernéticas que são “todos riscos”. Em comparação, faltam soluções confiáveis para as atividades jurídicas estrangeiras relacionadas ao uso terrorista da Internet e das mídias sociais. Ao mesmo tempo, esta questão tornou-se uma preocupação e há oportunidades para os governos, empresas, e sociedades civis a mitigarem. Este cenário desafiador, que não mostra sinais de enfraquecimento, pode aumentar o interesse na integração de ataques cibernéticos ofensivos em estratégias de combate ao terrorismo facilizado pela cibersegurança.

Palavras-chave: ciberterrorismo, direito internacional, autodefesa.
1 INTRODUCTION

The definition of any phenomenon makes its characteristics exposed to subjective decisions either in terms of acceptance or rejection. However, in the case of terrorism, there has not been a universally accepted definition which if used could have allowed the possibility of determining the position of customary law concerning the use of force against the acts of terror which could have made it easier to be prevented, challenged and punished if universally criminalized (Borichev et al. 2022). This development could make the offender of terroristic acts subjected to face the wrath of the law (Greenberg et al. 1998). Efforts have been made to combat terrorism at both local and international levels (Mohd, Yunus, Hassam, 2020). It was made known that the pressure required to extradite a terrorist offender on international terrain to face the law on the committed acts of terrorism if found guilty exceeds the pressure to extradite a common criminal as cited in (Shiryaev, 2012).

Some studies show that academics had made suggestions on the definition of Cyberterrorism but those definitions of the concept are found to be partially overlapping and range from those including social aspects (terrorism is motivated by “egoism, intolerance, lack of dialogue and inhumanity, greed, and accountability (Medhurst, 2000) or psychological ones (“terrorism is a tactic to coerce a behavioral change in an adversary (Dobrot, 2007) to very thorough legal approaches (“one must distinguish between attitude [and] methods (Sorel, 1996) of terrorism. This was further complicated by the definition recommended by the United Nation’s high-level panel in its report on threats, challenges, and change of 2004. The panel concluded that a definition in the upcoming comprehensive convention on international terrorism should include:

‘A description of terrorism as “any action, in addition to actions already specified by the existing conventions on aspects of terrorism, the Geneva Conventions and Security Council resolution 1566 (2004), that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a Government or an international organization to do or to abstain from doing any act”(UN General Assembly Document A/59/569, (2004 December 2).

The study establishes some correlation between the cyber-attack and how it is committed in the general international law and the use of elements that are available in such an attack, which determines the states’ right of defense under the provisions of
Article 39 of the Charter of the United Nations. He further develops certain tools to link it to other types of armed attack considering it as a non-indirect armed attack that may harm states according to Article 4 (2) of the Charter of the United Nations and how it harms the strategic interests of countries and weakens its electronic infrastructure, particularly as information technology and the Internet have become the basis for the development of the modern state.

Nowadays, information and communication technologies are an integral part of our lives, and societies and countries are relying on this technology to perform their multiple activities (Abdelatia, Alsohbo, & Hassan, 2023; Hassan, Azmi, & Abdullahi, 2020). Cyberspace, such as digital and international communications and information infrastructure, can offer enormous benefits to individuals and communities and can also be the source of many threats because of the dependence of modern societies on electronic technology (Hassan et al., 2020), which has become one of the priorities of the States at present. As cyberspace is a new source for conflict, it is necessary to research the right to self-defense against some activities that violate individual, organization, or state’s rights within cyberspace with legal guides and preferences that could be incorporated into International Law. This research is important in the wake of the proliferation and availability of arms seen to have possibly motivated individuals, groups, or one UN member state to intrude and assault the territorial sovereignty of another. This development is based on the claim of justification for the case of legitimate self-defense by one state against the aggressor states. Some argued that the right of legitimate self-defense applies in the face of direct armed attack while studies argue that the effect or implications of some cyberterrorism attacks could be devastating and pose monumental damage to the security and economy of any victim nation.

Therefore, we can include this type of violence under indirect armed attack in comparison to the above, since electronic operations exceed armed attacks in some cases that may force countries to defend themselves, and against electronic power under Article 51 of the UN Charter. The concept of armed attacks ought to include electronic operation attacks that can destroy strategic and service facilities that may result in physical harm or death.
2 LITERATURE REVIEW

The Charter of the United Nations was restricted in its Article 2, paragraph 4, which prohibits states from the threat or use of force against the territorial integrity of a politically independent state or in any other way inconsistent with the purposes of the United Nations and the inclusion of the use of electronic force against States whether directly or indirectly. Article 51 in Chapter vii of the UN Charter also indicates that:

“Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary to maintain or restore international peace and security”

The study investigates the need for the adoption of the rights of self-defense by the UN Member States against the attack of cyberterrorists and the need for the incorporation of the right of self-defense in international law if Article 2(4) of the United Nations Convention:

“Members 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”

Article 2(4) above is an indication that the UN does not want any of its member states to be under the threat of any other member and vice versa. Of course, it is rational, but if one state or collective states act contrary, the UN convention suggests measures in the form of sanctions against defaulters. At this juncture, before self-defense could take place under necessity, article 39 gave the Security Council the power to determine the existence of the threat to the peace, breach of peace, or act of aggression after which the Council makes recommendations or measure to be taken to restore international peace and security under Articles 41 and 42. The latter are measures devoid of the use of force such as military attack or any attack consistent with what the article prescribed.

Provision for the state to stage self-defense or collective defense by the attacked state is found in Article 51 of the Charter which regulates the rights of the state to use force in individual or collective self-defense. The first part of Article 51 in the Charter of the United Nations states that:
“Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security.

If under the given pieces of evidence, State cannot achieve a reasonable settlement of a dispute through peaceful means, therefore, self-defense against cyber-attack will meet the requirement of necessity (Hadji-Janev and Aleksosk, 2021).

Article 2(3) of the UN states that “All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered” (UN Charter). From the latter, it has been clearly shown that the peaceful coexistence of states and the entire globe is the main objective and prime focus of the UN.

The issue of proportionality (threshold) in the use of force constitutes a problem as well because there is no benchmark or standardized measure to determine or measure proportionality between the amount of force involved in the attack and the self-defense except the kinds of hacking or cyber-ware applications used as weapons that were used in an offensive attack that is predominantly virtual.

Many legal experts argued that Cyberterrorism should be classified as an armed attack because of the force associated and the identified destruction resulting especially on state public infrastructure. Attacks taking an ICT central system could result in sustaining injury or death of the victims of the cyber met devices attacked are electronically connected, for instance, to live supporting machines and other types of sensitive medical devices used for assisting patients in hospitals. Eventually, significant destruction of policy issues saved in soft copies may ensue because of the entailed force applied to targeted public infrastructures. On the other side, the perpetrators of the cyberattack have a rational intention for embarking on such a destructive attack that violates the sovereign rights of the victims with monumental destruction of or distorting national statistical data stored in the system devices for future or consistent use not to mention the time and capital intensive information destroyed or stolen or spied for whatever reason of the attackers.

In some cases, the purpose of cyberattack crime is not to steal a piece of information discovered in the computer system but to change the data or programs contained in the computer of the victims. The terrorist may intentionally plant a strong virus to prevent normal service or prevent the victim’s accessibility to open and operate
the computer system, some viruses may be in the form of messages to prevent access (http://aspireip.com/cyber-crimes-space-and-so-forth-a-concept-of-cyber-laws/). A good example is in a business operation attack where criminal accesses a network system of the company to control the delivery and destination of customers and business information neither for financial gain but in most cases for disrupting the operation of the business in an organization or public sector’s bureaucratic framework of the government while recovery from the attack entails a lot of financial expenses.

In the event of an armed Cyberattack, does International law justify legitimate self-defense? As a result, an attempt to step up action for self-defense may constitute a legitimate action to avert a threat or to prevent escalation hence, international law should be allowed to decide the punitive reward against any perpetrator and the appropriate redress for the inflicted damage on the victim state or organization for the sake of justice and prevention of future anarchy. The absence of an international legal regime on cyberspace is derived from the actor’s complexity and jurisdiction in the cyber realm. The latter has been further complicated by the fact that, in the past, few years of several international actors, mostly state actors, promote the idea of digital sovereignty to promote their interest to take back control of information, communication, data, and infrastructure related to the internet (Gueham, 2017). Consequently, this situation creates harder challenges to the possible enactment of appropriate international law not only against the perpetrators of cyberterrorism but also against the state actors perpetrating cyberterrorism. How would international law incorporate cyberterrorism law and the rights to self-defense by the victim states of armed attack that involved an application of force in the future of international law on cybersecurity? Can some loopholes in international law be critically addressed while states and treatment of their affairs as members of the UN be upheld with equality for the sake of justice? Hence, these puzzles require answers that would be addressed in this research. The study posed the following specific research questions to the participants RQ1: In the event of armed Cyberterrorism, does International law justifies legitimate self-defense? RQ2: What are the lacunas Regarding Cyberterrorism in International law?
3 METHODOLOGY

The study employs a qualitative method in which interviews were conducted with experts in the field of study. The participants of this study are members of the security and military intelligent experts including some academics who have studied, taught, and published academic works on international studies and cyberspace-related crimes. The study selected the participants' bases adopting purposive sampling techniques as one of the non-probability samplings in the qualitative method to source empirical data.

The above model Figure 1.0 is the framework of the fieldwork through which the researcher sourced data for the study under context in line with the qualitative method to find facts and useful information on the phenomenon. It includes the analysis of the data, findings that lead to the discussion, and from which the result of the study eventually emerged in the research.

The sampling technique is part of the applied method for data collection. A purposive sample, also referred to as a judgmental or expert sample, is a type of nonprobability sampling and is also named judgmental sampling. Owing to the attributes the agent possesses, it is the conscious preference of an informant. It is a non-random strategy that does not require a fixed number of informants or underlying theories.
Purposeful sampling helps the researcher to determine what needs to be learned and sets out to find individuals who, because of expertise or experience, can and can supply the data (Bernard 2002, Lewis & Sheppard 2006). The key reason for purposive sampling is that it provides the researcher with the right to select the participants who are knowledgeable with huge experience in the study as the sample, logically assumed as informants for the study. In such a situation, this group of participants was selected based on their unique experience and deep knowledge in line with the phenomenon to be studied.

The sample population interviewed consisted of security intelligence officers, legal practitioners, Constitutional lawyers, and the leading professors in legal studies in academia. Braun and Clarke (2013) explain that a range of 10-20 is the appropriate number of participants for data collection in the case of the qualitative study. Therefore, there are 10 participants on the interview list, engaged with the same semi-structured questions written on the interview protocol. However, some were technically probed on different occasions along the interview process when observed to either evade answering the question or for providing inadequate information during the interview session.

In the qualitative research method, the researcher is allowed to explore ideas and experiences of a phenomenon in depth (Manipol, 2023). The method applied for data collection in the qualitative method includes observation in which the researcher either observes an individual or a group of people or objects in a setting while taking note of actions and behaviors of the group particularly about the phenomenon the researcher focuses on a series of time to get full nature, character, changes, in the actions about the phenomenon and study the note and analyses the content of the note taken. However, in the case of the current study, the data is sourced through interviewing the selected participants face-to-face to respond to questions drawn on the objectives of the study after which the researcher transcribed the information and analyzed it into themes to figure out differences, similarities in the information and their relevance to the core values investigated about the phenomenon concerning the past studies and the problem statement of the study.

In the case of the current study, a face-to-face in-depth interview technique is adopted to source the data on the phenomenon. The interview was conducted on an individual basis where the participants are not many as the minimum of less or near 10 was recommended by many studies on qualitative research methods. The interview
instruments acquired for use to conduct the interview were reviewed by the supervisor in charge and a PhD holder in the field. This research tradition is employed for validity purposes (Alotaibi, & Al Rabee, 2023). The experts’ suggestions and guidance were welcomed and heeded. The selected participants gave consent to participate through the replied emails and endorsement on the letter of invitation sent to them. During the interview, the participants were allowed to be independent in their choice of venue, date, time, and the provided information while the researcher granted them absolute confidentiality on their personality as well as the information provided. The semi-structured interview questions enlisted on the interview protocol were administered. The study asked all the participants the same semi-structured questions but probed further where any of the participants attempted to parry a question or provided inadequate information.

The data were later transcribed while certain codes were used to identify each of the participants and a narrative thematic form of analysis was adopted to exhume relevant, empirical facts from the huge data that were applied to achieve the objectives of the research.

4 RESULTS AND DISCUSSIONS
The study posed the following question to the participants:
RQ1: In the event of armed Cyberterrorism, does International law justifies legitimate self-defense?
One of the participants, who happens to be an expert in international law responded:

The criminalization rule must be taken into consideration at the level of international law. The basis is that acts are not criminal unless there is a legal text or an international treaty regulating them. There must be internal law. The problem with international law is that the treaty does not bind only its parties, unless the treaty has reached a degree of universal acceptance so that it becomes part of customary international law. There is no one now who says that the issue of cyber terrorists and cyber-attacks are criminal matters at the level of international law. This is the starting point for talking about this issue (DAK-ICJ) June 2021 5:00pm).

According to the participant DAK-ICJ, he responded keenly that, it is not enough to criminalize an offense or a group of offenses until it is determined by the law and the criminal court of law enforces it. In the case of the above research question, cyberterrorism is an international criminal offense as the study has shown that its perpetration takes place across social networks and designated websites. It is considered
as a predetermined attempt to coerce millions of internet users to mandatory compromise when their profiles, data, information, and webpage are subject to malware attacks. This situation prevents normal function of the radar, websites, or Internet or it is meant to destroy public or organizational facilities as a way to prevent normal operation to take place so that the victims could experience disruption of duties. At this point, not only individuals and organizations that involve in the acts of perpetration of cyberterrorism, that state is more pronounced and capable of causing warfare when attacks get to the stage that a victim is provoked to prepare for a counterattack which would mean self-defense even though it a contradiction regarding certain aspects of violation of international law. However, the participants argue that there can be no penalty without a law against violation of certain regulations. It means, until the international community defines and prohibits cyberterrorism in a strong term, it would continue to be regarded as a non-violation of either human rights or sovereignty rights of other states and any other victim concerned. Following that statement, the international community has not hit the nail on the head to effectively enact a law that could prevent cyberterrorism before an uncontrollable proliferation across the globe.

Another participant, RAS-PIL could not hide his feeling when asked the same question, he mentioned that:

In fact, cyber terrorism has not been accurately defined in public international law, and therefore, as there is an attack against a country, this allows the country that was affected by this attack to include the concept of legitimate defense under it, because in this attack there is a use of force even in international humanitarian law the use of unjustified force is prohibited, because it affects the most important aspects of life and vital fields necessary for the state. The general principles of law are the principles common to the laws of all countries of the world, such as (person is presumed innocent until proved guilty), and (there can be neither offence nor penalty except as specified by the law). These legal rules that exist, whether in the Charter of the United Nations or in international conventions or other sources, are not a “Holy Qur’an” in the sense that the law reflects reality. If the law was established in 1945 in the Charter of the United Nations and the laws of other countries, which occur on it from time to time also modify and develop to keep pace with the changes that occur. There is an interest, necessity, and a need to reconsider many of the facts or changes that have occurred in recent years, including cyber-attack issues, including those that are directly stipulated in international laws. The reason for this is obvious/*s and that such technology (means used for committing Cyberterrorism) was not known 50 years ago or less or more in this sense. Therefore, it is considered a turn of event that required new approach.

RAS-PIL June 2021 11:00 am
In reality, the general principle of law is unique and common to the law of all countries. Therefore, there can be no punishment without a law and its violation by the accused persons and punishment based on specification made by law hence, it is not an assumption but reality in respect of crime and the corresponding specified punishment by the law. International law is a statutory legal doctrine that encompasses all crimes classified as international with the corresponding punishment or reward to that effect. That is the principle of law and not like the “Holy Book” such as Al Qur’an is not subject to reform. Therefore, the participants believe that international law should have been reformed to reflect trends in technology, economic, social, political, and other sectors of human endeavors.

The study asked the participant PM-PSGY the same question above and he gave his contribution by saying:

When we address the phenomenon of cyber-attack, it is one of the new and emerging phenomena that are not of a historical dimension, and this raises the very important questions: Has it become a phenomenon that all countries suffer from? Has it become a global phenomenon so that there is thus, an international consensus in order to enact a law and a legal reference for such phenomenon?

When we talk about this phenomenon, it is a new phenomenon that was not crystallize in a very large way, unless many countries were subjected to these attacks, especially the major countries, and we have very many examples. There are allegations such as the allegations of the United States of America that Russia carried out some electronic attacks in the elections that took place in 2016. So, this phenomenon has begun to put all its forces to create pressure on the international community, which will constitute an international situation, I think, in the near future.

PM-PSGY June 10, 2021 - 10:00 am

The participant, PM-PSGY raised an important observation that the phenomenon of cyberterrorism has not been frantically and collectively addressed, possibly because, it is a new phenomenon, secondly because many countries have not been subjected to cyberterrorism attacks across the globe and more importantly, majority of the powerful countries have not been attacked.

These observations are very important to this study. In reality, the law is law, however, wherever and for which society it is made once it is enacted, gets the support of the majority of the stakeholders. It becomes enacted, implemented, and enforced to address the problem for which it is created and punishment started to be issued to reduce the prevalence of the crime in context in the community. The observation is pointing to the emerging weaknesses in the international community whose member states have not
assented to the law against cyberterrorism as a crime that should be criminalized while some of the major powers have not been destructively hit with cyberterrorism attacks. Had it been some members of the UM security council been destructively affected by cyberterrorism, a constructive move and enactment and immediate implementation of the laws against it may have been put into effect. The law of self-defense as in UN Charter 2(4) is not yet regarded as binding because the term “force” prohibited as an exclusion in the Charter could not be guaranteed or explicitly determined in any offensive or counterattack cyberterrorism, unlike the kinetic attack. Once a law is established against a crime, attention is created by perpetrators either on how to circumvent the law and the punitive measures or how to virtually abstain from committing such crime punishable by that law any further especially if the punishment is aligned with life-threatening effect as the assumed outcome of the crime.

However, where any of the major countries are attacked by the state or non-state actors, they have applied force to make a counterattack and that should be applied to all other member states of the International Community. The law is interpreted but the elements of force in the Charter remain ambiguous.

If we want to talk about the subject of cybersecurity in general, then we have to know the means by which states in general, individuals or organizations use it because it is a new method on the international scale, because it is customary when there is military aggression or war between states, it is resorted to using military power, but with technological development, this means has become effective and powerful for countries, especially countries that own these means because they can take an advanced position on any armed conflict through electronic means from a distance and without the need to clash on the land of infantries. If we want to talk about the Charter of the United Nations or the laws and conventions applied in armed conflicts or in international humanitarian law or the Geneva Conventions, we note that the concept of cybersecurity does not exist.

The participant, DAO-IHL believes that the issue of legitimacy in the counterattack against the phenomenon of Cyberterrorism is a new study within the international crimes, it is therefore, requires careful assessment and collective effort to put it in the right perspectives so that it would not be abused by the state, organizations or individuals. To DAO-IHL, the issues of conventional wars are the responsibility of the state’s military to confront the aggression from other states but in the case of technological devices, the UN conventions or the international law have not fully addressed it. When the law is silent on a particular action, every perpetrator of such action
would go scot-free irrespective of the affected state by the use of the phenomenon. The concern is, that cyberterrorism may be cheaply used against the poor or developing countries by the advanced counties who have these technological devices. Hence, a law should be enacted to control cyberterrorism through the consensus and valid agreement of all nations under the UN umbrella and be incorporated into international law so that a level ground is adopted in threading all perpetrators of cyberterrorism.

Regarding international law, we must distinguish whether we are in a state of war or peace. In a time of war, if the cyber-attack occurred as a type of attack that is considered as a weapon, then the international humanitarian law is competent to consider this issue. We must distinguish whether this attack caused great harm between civilians and among the military. If the harm to civilians is great, then we have entered into the issue of war crimes, which are under the jurisdiction of the International Criminal Court. There is also a responsibility for the state that carried out this attack towards civilians, which falls under the jurisdiction of the International Court of Justice. As for civilians, if the attack is weak or does not reach a high degree of force, we condition it on the grounds that it is a war crime, that the attack was against civilian targets.

If the attack was on a military target, then we are talking about a natural attack during an armed conflict, here the country that was attacked has the right to carry out a counterattack, as we consider the cyber-attack in this case as a weapon for self-defense.

Participant DGH-PIL is explicit in his response saying that the world would see cyberwar if the cyber-attack occurred as a weapon, then the international humanitarian law would become relevant and active as the competent aspect of international law that could deal with such phenomenon.

The issue of cyber security is a new topic now, and we cannot talk more about it. Countries are still working on organizing and putting in place legislation and laws to protect themselves in the first place against cyber-attacks, and as you know they are virtual attacks, there is nothing on the ground, all on the international information network.

Now, due to the tremendous technological development and digital transformation, most of the information and data for countries are present on computers and are exchanged through the country itself using means of communication through Cybernetics or microwaves, and thus are vulnerable to attacks. This is necessary to know because there are data related to the state and the sovereignty of the state in the Ministry of Interior or in the Ministry of Foreign Affairs or any other sovereign ministry. Because of its connection with the components of the other country, it becomes vulnerable to hacking or attack, hence most countries began to abide by international law, but in secret they are working to create a cyber-defense and cyber-attack on any country trying to attack it.

For example, Germany has a law before the House of Representatives to give it the powers to carry out cyber-attacks to defend its interests, therefore, every country has the right to defend itself, whether the attack is armed or in cyber-attacks that are a violation of state sovereignty as is the armed attack.

6. DGH-PIL

BGRA-MTC
The BGRA-MTC, a participant with military intelligence skills and experience agrees that cyberterrorism is a crime of warfare through cyberspace but countries of the world are still working frantically to legislate and incorporate it into law. There are data related to the state and the sovereignty of the state in the Ministry of Interior or the Ministry of Foreign Affairs or any other sovereign ministry, those data saved online are vulnerable to attacks by internet experts and the important information is accessible if it is intruded and that exposure could render the wealth and military strategies of any targeted country into risk under cyber terroristic attack.

The sovereignty is at stake and following successful cyberterrorism attacks on the affected nation, the participant DSAM-LCS says:

This is an issue in which there is a dispute because it depends on the actor and the force responsible for the issue. Some countries consider it as self-defense and some countries consider it a terrorist act. The defect begins with the agreement on defining terrorism in its traditional form, before we move on to defining terrorism in the cyber form. International law cannot consider this act as a terrorist attack or as self-defense. This issue is still a source of contention 1. DSAM-LCS

The absence of consensus among the member states over cyberterrorism offers the rights to victim states to be repelled with counterattacks including the use of force in self-defense. This controversial situation and absence of consensus among the states under the UN still deprived cyberterrorism of being considered for information in International Law

RQ2: What are the lacunas Regarding Cyberterrorism in International law?

Figure 3: Shows the results of RQ2

Of course, this issue is related to the main point which is the agreement on the

All countries must unite, without exception, to reconsider and set the legal rules that protect their

United Nations to adhere to such treaties related to cyber security,

There is no international agreement or specific definition for Cyberterrorism

Source: Prepared by Authors (2023)
There are instances of lacuna in international law that fail to address uniformity of purpose in the way some member states use power over others just for their interest while the major powers such as the members of the Security Council looked the other way, thus, indulged the state to act with apparent impunity. An example of this was observed when the United States of America attacked the State of Iraq even without the approval of The United Nations.

The inability of the UN to incorporate in the international law a code of enforcement on member states to live up to committed responsibility on various issues of immense importance for global sustainability such as those that could save lives and properties or promote well-being for mankind. Issues of global warming, maritime issues, physical and cyber terrorism, food shortage and global pandemic, and many other issues should be a collective responsibility of all members. There are many lacunas in the activities and functions of the United Nations. Another important constraint against collective approval of decisions celebrated on the General Assembly floor of the UN for legal use is the inability of each state representative to unilaterally agreed on a celebration on behalf of the state. There is the need for three arms of the government of each state to celebrate issues proposed by the UN Assembly and evaluate them all around to see which of them could fit into the cultural, political, economic, and social requirements of their country. It is after rigorous examination of it that the legal arms of the government of each member state may agree to or not to sign the protocol as a binding international agreement on their country. The consensus thereafter makes it become a part of international law. That is the reason that the international law on any phenomenon takes a long time to receive acceptance from all member states and that delay in incorporating it into international law. The lacuna in international law on an issue would take more time to get overwhelming support from the general member states until a change is made to the method of creating law at the international level. In the same way, the participants of this study contributed in the form of information below:

(DoA- PIL: 12 June 2021- 11am
The first step is to resort to legal means, starting with the establishment of a legal adaptation of the cyberterrorism in terms of the elements, components and harmful consequences that take place after the occurrence of the cyber-attack. It requires the United Nations represented by the General Assembly to prepare draft treaties requesting the states members to the United Nations and non-members to the United Nations to adhere to such treaties related to cyber security, as the more countries acceding to these treaties, the greater the culture of spreading the concept of cyber security will be, and accordingly, these countries and their armies have a general and a clear idea about this dangerous
weapon, which is now being used without deterrence, becoming closer to the concept of proxy wars.

First, the concept of terrorism is a vague and vague word, and there is no definition of the concept of terrorism. The concept of terrorism differs from one country to another. For example, the resistance of the Palestinian people is considered as resistance and the right to self-determination. On the other hand, it is considered by the United States of America as terrorism. There is no international agreement or specific definition that clarifies the concept of terrorism. Before we develop directives related to the use of weapons by terrorists, whether classic or cyber, we must define the concept of terrorism in order to legalize the use of these weapons. These are some of the lacunas in International Law you just asked me.

DOA- PIL July 17, 2021

The participant DSA-EBD contributes and responds to the above question by saying:

Of course, this issue is related to the main point which is the agreement on the concept of terrorism in general, and if there is a loophole that currently exists, it is that cyber terrorism is now not covered in international law and for this reason the first step may be to reconsider the definition of terrorism so that it includes the use of electronic means. Thus, the areas of cyber terrorism are included so that the law can punish this act.

DSA-EBD: July 22 2021: 12 Noon
(RAS-PIL June 2021 11:00 am)
The law, as we mentioned, regulates a reality, and since reality is not fixed but changes continuously, the legal rules that existed, whether under traditional international law, contemporary international law or even in the United Nations Charter, were regulating a reality that existed.
No one could imagine an armed attack over the either. In light of this development, all countries must unite, without exception, to reconsider and set the legal rules that protect their sovereignty, and to hold accountable and prosecute any country that has been subjected to a cyber-attack that results in damaging property and killing people.... etc.
(RAS-PIL June 2021 11:00 am)

From the contribution of the above participants, it is evident that international law exists with lacunas that required urgent attention and involvement of stakeholders on how best to reform and possibly restructure some content of Acts, protocols, and conventions to acquire the required strength for effectiveness on global issues of concern. For instance, in a conference session, a key speaker asked “Does international law require us to wait until lives are lost or property damaged before we may engage in acts of self-defense? (Cebrowski 1999; Livson, et al. 2021). The latter is a single question that touches on the voluminous of the whole international law and exposes it to some controversial ambiguities.
5 CONCLUSION

The study collected data from selected 10 participants who were well-versed in the knowledge of security and cyberterrorism. The participants provided information under the drawn-up questions on the research protocol. The questions are in semi-structured form to make questioning more flexible to suit the level of understanding of each interviewee and to prevent and resolve any ambiguity during the interview. The analysis uses a thematic narrative approach while the main focus of each question represents the theme that was drawn out and followed by the sub-theme in the form of subsequent extraction of the responses in line with the question. All the information that was similar on each question was not repeated in the theme concerning the participant that provided it once the more relevant one or two are drawn out from the response of any other participant on the interview question. Special codes were used to denote the name of each participant and their marked comments formed the theme in the form of information provided for the question. Ethically, the interviewee complied strictly with the ethical standard to avoid being biased as their comments were left as provided except for making relevant statements that formed the themes.
REFERENCES


