International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



# The Concept of Electronic Terrorist Acts in International Criminal Law

Dr. Nibras Salim Khudhair Department of Law, Al-Kunooz University College Iraq, Basra nibras.s@kunoozu.edu.iq

#### **ABSTRACT**

The study aimed to identify the role of technology in spreading terrorism, Identify cybercrime sanctions in international public law, and Identify gaps in international public law in reducing cyber terrorism by identifying weaknesses. Of the most important findings of the study include: current global developments show that terrorism is unlikely to be terminated in the coming few years, despite the cooperative efforts by the United Nations, the international community and its Member States. Through the "war on terror", the United States has taken the lead in this regard. The invasion of Afghanistan in 2001 was carried out as consequence of the terrorist strikes of September 11 in the United States America. Since then constant unrest continued in the Middle East. The case law on terrorist organizations in these three authorities, and particularly the legal values resulting from the proportion or jurisdiction of these provisions, indicates that, despite tariff variances, there seems to be a similarity of legitimate values arising from jurisprudence. A relative examination of the judicial principles arising from the proportions of each of the Supreme Court's rulings on terrorism discloses an extensive variety of principles of law which, in some cases, apply in particular to the legal system of their State. What is more clear is that these lawful principles are similar, and if they are considered as a whole, they are perfectly consistent. These legal values seem to show a similarity rather than a difference in this area of crucial importance to domestic criminal law. This supports both transnational and global counterterrorism policies, laws and strategies because it suggests that what seems to be developing is a public comprehending of what creates terrorism, at least through these three main jurisdictions of public law. Courts recognize the obligation to abide by legitimate principles and domestic and global rules when applied.

**Keywords:** Electronic, Terrorist Acts, International Criminal Law.

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



#### I. Introduction

The Middle East is considered one of the best and most active areas in order to be the preferred theater for the implementation of cybercrimes, without deterrence or any law that protects these installations. After the United States and its allies came to the Gulf War, the region was provided with technology. In addition, for those who are not worthy and this is the whole point, It was necessary to manage the war and the operation of the launchers, the operation of the missile orders, and all this depends on the electronic programs, and the networks, in order to reach the orders to execute, the war was conducted almost without the presence of forces on the ground, for example, It is launched from the high seas from a very remote area on the back of a warship and military, and with the clear instructions target, cutting thousands of kilometers to hit his goal? Was the absolute present? Has the information store reached the target? Slowly it has not happened

Since ancient times, humanity has tried to put an end to the evil impulses of man. Therefore, the religions, the heavenly laws, and the statutes have sought to refine these arguments and the judgments and punishments that have been established have led them to bear the wrongdoers responsible for them regardless of who is the perpetrator. A civilized human society where it cannot stand idly by in front of what may be subjected to individuals who violate their rights and freedoms. This has developed until the so-called international community, whose members have tried to put an end to crimes that jeopardize worldwide peace and safety, With serious harm, with the possibility of impunity for the impunity enjoyed by most of them before the courts (Waidan, 2015), The great expansion of the 1970s and 1980s in the usage of data and communication technology has resulted in the expansion of the use of the Internet in e-commerce transactions. Previous developments have led to the thought of payment systems and systems commensurate with e-commerce. Of new money that began to lose its tangible physical form to become just a stream of electrons saved in the memory of smart cards, which is known as electronic engravings and other electronic payment methods, and commensurate with modern electronic transactions Where communities are usually keen to take advantage of technological developments in the development of financial and commercial systems in order to reduce the time and cost of total exchange to the lowest level possible (Qara,2012).

Cybercrime is a modern pattern of crime patterns that have not been seen in ancient societies. They have emerged in contemporary societies as a result of technological development encompassing all spheres of life. Although the crime has emerged in an unprecedented fashion, it is a traditional crime, which is an illegal act punishable by the state or power. The difference is that it is made using modern technology such as computers, the Internet, applications and programs related to it. Are carried out in the absence of electronic security, and since these crimes are carried out with a great deal of human intelligence coupled with the use of complex techniques, investigating them is a very complex task compared to conventional crimes (**Kaur,2018**), The connection of this type of crime to technology is the result of enabling individuals to carry out any activity from anywhere easily, regardless of distance, whether it is legal,

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



such as selling, buying, exchanging information and social communication, or non-legal such as fraud, trade in pornography, infringement of intellectual property and identity theft, Or infringe the privacy of digitized documents from ADP systems and several electronic devices (**Dacey**, & **Gallant**,1997).

There are various types of cybercrime, including targeted individuals and others targeting public and private institutions; the use of vulnerable people of information technology with the availability of hacking tools that do not require much experience and skill make the electronic world at great risk cannot be avoided only by taking all safety measures (Choi et al.,2007), Police officers were deeply disappointed that the legislators are unable to preserve cyber-crime regulation ahead of the fast-moving technological curve (Jain & Shrivastava,2014).

The criminal investigation and the collection of evidence and conclusions from the security activities that top the attempts to confront the crimes developed through the development of methods and improve the investigators and provide them with modern science and technology. Technology has been a fundamental pillar in the scientific and technical development of States as a whole and forensic investigation in particular. It has helped to provide advanced mechanisms and modern communication systems, but to include new ways of working to uncover the truth and extract it from the clutches of truth to find the right path, (Al-Balawi 2009), This will be achieved only through familiarity with the methods of forensic research in accordance with advanced technology, especially in the crimes that have been created for the relationship between the methods of committing modern science and technology (Jamal, 2018).

And the involvement in criminal responsibility was said: The real attribution of illegal responsibility to each individual committed terrible mass crimes – like those that require the consultant of the International Criminal Court (ICC) – is one of the challenging cases that the global society has had to deal with for the past 60 years, if not longer. In spite of the enormous complications related to the "macro-criminal" dimension of worldwide law-breaking activities, it quickly turned out to be clear that only the timely attribution of individual illegal responsibility to those involved in numerous levels in committing crimes could be an effective response to the severe violations of civil rights. It was also directly obvious that the necessity to bring single persons to justice was mainly vital with regard to those holding positions of power, the "most senior commanders", that is to say those with authorities to give orders. In this introduction, I see that international criminal law has evolved to include cybercrime also under the section: n the strict sense, leadership's responsibility instead refers to the criminal liability of the high-ranking leader for criminal acts committed by his assistants. The expression was originally used in the martial environment and

\_

<sup>&</sup>lt;sup>1</sup>This paper has been written for the 'CTC WestPoint 2014 Cadet/Student Conference on terrorism, insurgency, cyber and asymmetric conflicts'. My gratitude goes to the CTC to provide me with this opportunity to write and present this paper.

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



was extended to the non-military sphere. In this respect, the term "superior responsibility" is more proper, because it also has something to do with characters in military and non-military position such as cybercrime (Werle,1997).

This study focused on the structural impact of terrorist groups. The scholars of criminal research, policy abusers and rapporteurs in countries in sensitive locations have determined that the success of any terrorist science depends in the first instance on material financial resources, such as written scientific materials, places of access to money such as digital currency, The focus on finite detail is a failure in the work of any terrorist organization, which is defined in the structure of the tandem in assigning the organizational and leadership roles and assigning the roles of the authorities and responsibilities and controlling the control and coordination. As a result, The structure is influencing strategic control in carrying out terrorist acts, as well as weakness and weakness in operational and tactical centers in carrying out these terrorist acts, the operative and strategic susceptibilities about actions of terrorism. This academic paper will examine the indispensible mechanisms of any organizational building, i.e. 'membership', 'operational space and time', 'formalization' and 'centralization', and their particular influence on the dimensions of a terrorist organization (CTC WestPoint,2014).

Nevertheless, the question is whether digital criminality has an organizational capacity that we can hear or see on the ground. Alternatively, what else is digital terrorism? How to use or trade? What laws limit it? Alternatively, meet him to prevent him? These and other questions will be answered in this study, In this part of the quote, we are talking about the jurisprudence that can be adopted or practiced by countries and regional organizations such as the European Union. And this jurisprudence is linked to the strength of the law of the State practice and what is the link of these belongings, if any, and is what is required of this state to apply its laws to criminal cases and persons? This jurisdiction is an aspect of the authority of the State on its region and because this sovereignty is the absolute right to apply, enforce and enforce laws is a fundamental element in the implementation of this applicable State, and it is a quasi-condition to ensure at the same time that no State interferes in these matters (1), and here we say that the idea is no longer strictly applied if it has been applied, and there are also some exceptions that allow for limited jurisdiction outside the territory of the applicable state of law, Z Therefore, the principle of territorial restriction is somewhat free in section (2), and So high credibility, some countries use a law strictly binding, assuming the legislature only to be laws so that you cannot replay in the application outside the borders of its own state, but this assumption does not define very precisely the powers (Ryngaert, N.D.).

## II. Objectives of the study:

The aims of the study are as follows:

- 1. Identify the role of technology in spreading terrorism.
- 2. Identify cybercrime sanctions in international public law.
- 3. Identify gaps in international public law in reducing cyber terrorism by identifying weaknesses.

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



#### **III.** Study questions:

The questions of the study are:

- 1. What is the role of technology in spreading terrorism?
- 2. What is the penalty for committing an electronic crime in public international law?
- 3. Are there gaps in public international law that help a terrorist commit electronic crimes?

#### IV. The address analysis:

The address are includes many sides like what is the concept if Electronic terrorist and under it there are many branches like – Internet- soft programmers- visa – connections – communication's, Society sites, mobiles, and computers - In civil use and others sides like what is the criminal that's are come from these part of Technology that's mean there aren't laws organize the operation of using and the rights of people information and details about joining and using.

The other part is international, is there and any international legal body regulates this process in international and domestic use. If there any legal or laws that activity outside the stats and globally that work ad a big international body to stop all the murders and criminal persons the use without any rights to use so to take them to the court and arrested then the jails them like any murders.

### V. The concept of cyber terrorism:

Cyber terrorism points to deliberate, politically driven assaults by subnational groups or secret representatives against data, CPU systems, computer programs, and documents that lead to violent actions against non-combat aims (Conway,2003).

Cyber terrorism is the merging of terrorism and Internet. It includes the usage of the cyberspace as a mechanism of empowerment and support. It has the ability to create a postmodern form of disorder. Making Use of computer properties to threaten, damage or disturb vital infrastructure such as electricity, transport, oil and gas, banking, financial, water and emergency facilities (Matusitz, 2007).

Cyber terrorism is generally perceived as illegal assaults and intimidations to hack computers, systems and data kept in it when it is done to threaten or force the regime or its people to achieve governmental or societal goals. Moreover, for rehabilitation as electronic terrorism, the attack must lead to violent acts against individuals or belongings, or at least create sufficient hurt to create panic. Examples include deadly attacks, physical harm, detonations, aircraft accidents, water pollution or serious financial loss. Severe attacks on vital infrastructure can be terrorist acts online, depending on the damage they cause. Outbreaks that disrupt non-essential facilities or are a major inconvenience will not (SEissa et al.,2017).

## **Types of cyber crimes:**

1. **Manipulation of computer source documents:** The process of intentional, concealment, destruction or alteration of any source code of the computer utilized for

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



a computer, computer software, computer network or computer system, where the computer source code is required to be retained or maintained by law (Kumar,2000).

- 2. **Hacking with computer system:** From the point of view of the average citizen, piracy means overcoming the security of any system to enter without permission. This is usually done by stealing or guessing a password or cheating a program that is looking for a password with some smart answers (**CRID,2005**).
- 3. **Publishing obscene information electronically:** refers to the publication or transmission in electronic form of any obscene material (**Raj and Rajan,2018**).
- 4. **Secured system:** Anyone who access or tries to secure access to a confidential system without permission will be sentenced to 10 years' imprisonment and also a fine. The Government can declare that all the sites of the certification authority are almost protected because all these sites are important to the nation because they will serve as engines of trade (**Eagles et al.,2006**).
- 5. Violation of Secrecy and Solitude: Anyone who uses any document, book, letters, data, file or any other material without the approval of the owner or accesses electronic document, book, record, letter or information of another person shall be sentenced under the IT Act (**Hao and Gao,2017**).

#### VI. What is the idea of electronic terrorism? Does it already exist?

As individuals, technological developments have affected various aspects of our lives. These scientific developments have changed the way national institutions and organizations are functioning. Technological advancements have altered our lives and how things work. These developments have resulted in the emergence of new concepts in different areas of ICT. Examples electronic education, digital school, digital amusement, digital business, and digital arts and so on. By virtue of the technological developments we are having a virtual world similar to the actual world (Jwaifell et al.,2019).

Cybercrime can be implemented at several different levels. The attack can be as simple as anyone on a computer against someone else or a government agency attacking another government. These sources or attack targets are not limited to personal computers only, but may include computers from routers and switch to control systems. Data acquisition systems when looking at cyberspace, there must be an internal focus on what the attack can acquire in order to know what and how to defend it. Intelligence obtained by a foreign entity may be critical to future planning, which may involve limited, conventional, nuclear and strategic planning against our country. Cybercrime has become the easiest and most effective way to gather intelligence in modern times. Communications, computer systems, intelligence, systems of vulnerability and surveillance, because of cyber-terrorism, have become a double force for the enemy. Access to these systems gives the enemy the ability to plan and implement the strategic targeting of the enemy's vital infrastructure (**Pope,2008**).

Any act of terrorism must be driven by a governmental, religious or ethical motive; its purpose is to influence the government by intimidating or intimidating a segment of the public; in the case of cyber-attack, it must be seriously interfered with the

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



electronic system. The Titstorm process, or any other similar attack, is likely to meet these positive requirements. Although the Titstorm process is also likely to meet the exception of political protest, in other cases the prosecution only needs to overcome a low burden to prove that this exception does not apply (**Hardy,2010**).

The international organization workplace of medication and Crime (UNODC) significantly contributes in offering assist to the Member States, in fostering of its authority, to reinforce the capability of national criminal laws of justice to enforce the laws of the international legitimate rules against the terrorist acts, and will therefore in agreement with the principles of Rule of law and the standards of the international human rights. Particularly, in 2011, the National Assembly, in its resolution 66/178, confirmed the authority of UNODC to still advance specified legitimate info among the house of counter-terrorism and relevant thematic zones, also due to the utilization of the net for terrorist functions, International confessions have increased in recent years, and there is not yet a scientific document to address and address this wide range of serious terrorist activities. Furthermore, limited professional tuition is existing on the legitimate and functional parts of the enquiry and trial of act of terrorism cases including the utilization of the net. The current publication enhances the prevailing resources advanced by UNODC within the limits of anti-terrorism, cybercrime, and rule of law. It also addresses the importance of developing integrated.

## VII. The nature of jurisdiction:

In public international law, the concept of jurisdiction has a strong traditional relationship to the concept of sovereignty. The jurisdiction of States allows for the exercise of the sovereign independence granted to them in a world order of formally equal States, by defining what law applies to persons or activities in which they have a legal interest. However, sovereignty not only served as the concept of empowerment with respect to the exercise of jurisdiction, but also as a restrictive instrument: it was aware of the adoption of international rules restricting the exercise of the jurisdiction of the State. States may already adopt laws governing issues that do not exclusively concern the country and thus violate the sovereignty of other States. In essence, the laws of jurisdiction define powers between States and thus serve as the basic "rules of passage" of the international legal order (Ryngaert, N.D.).

Jurisdiction of courts the legal basis and type of jurisdiction granted to the court determines the approach that the court must follow to determine the enforcement of any legitimate barriers to the application of law, like immunity and amnesty, and will also govern the law enforcement system. Court orders there are many accepted grounds for state jurisdiction under international law. This section shall consider any grounds or rules of jurisdiction that provide(s) the source of authority consulted upon international and mixed courts, and the means by which such authority is vested. There are four potential bases of jurisdiction: the principle of the local rule of a court performing a national institute of the local State; the assigning of authority from the State - usually the national State - to an international court; the rule deliberated by the international community on the Law court; and the rule conferred in an international court by the Security Council carried out under Chapter VII of the Charter. However,

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



it determines that the third choice, the so-called "floating" global rule, is not currently reinforced as a principle of worldwide rule. Consequently, given the present case of advancement of international law, the authority of an international tribunal needs to be either in rules acceptable to the application of law by a State or in the application of power by the Security Council (Williams, 2009).

## **VIII.** The use of the Internet by terrorist:

The development of human life has successfully determined the development of multiple epochs with specific characteristics. We live today in the modern digital age, many computers, services and networks are already important. At the same time, these new scientific and technological achievements are classified as good and bad for their users. Digital progress is visible and useful to terrorist organizations (**Rusumanov,2016**).

Technology growth has provided a wealth of jobs. One of the areas in which ICTs, the Internet in particular, have developed to play a vital part in the terrorist acts. The Internet offers a great deal of information and enables immediate and quite immediate contact around the world. Thus, the traditional vision of several old terrorist organizations has changed to adopt the usage of technology in their operations. The purpose of this paper is to characterize the tasks and procedures on which terrorist groups have relied on ICT infrastructure. The discussion highlights the technical and practical role of ICT infrastructure in helping terrorism. The utilization of Internet helped terrorist groups to develop from the traditional usage of the Internet to the more creative use of both old and novel Internet tasks. International terrorist groups can nowadays by electronic means target many possible addressees, conscripts and opponents. The purpose of the paper is to demonstrate the way the Internet might be utilized to assist terrorism, and to produce technological examples of support and use. This paper summarizes the high-level operations, procedures and examples used by terrorists in the Internet. This paper examines the usage of the Internet as a one-way, bi-directional instrument to provide jobs such as recruiting, advertising, training, finance and actions. Further, it examines particular systems such as online literature publishing, societal networking devices, anti-forensic and fundraising schemes. Other examples, such as masking and coding procedures, are stated. In order to analyze the way the ICT infrastructure might be utilized to support terrorism, the direction of communication is determined to communicate with old Internet services and techniques, as well as to new Internet serices and methods (Veerasamy and Grobler, 2011).

Using the Internet by a terrorist organization has become a major concern for law enforcement agencies trying to isolate, deter and destroy this global threat. Because of openness and ease of use, the Internet has become the main tool for spreading propaganda and deception by Islamic extremists. Al Qaeda asked its supporters to download articles from their sites and publish them through their own websites, discussion forums and email lists. This will provide continuity in their publicity efforts because when law enforcement authorities close another site, the same information is opened as the latter (**Blair,2006**).

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



The use of Internet terrorist organizations is similar to the use of the medium by traditional political organizations - for example, fundraising and publicity dissemination. However, other uses are unusual and distinct like hiding instructions, manuals and directions in encrypted messages or encrypted files. Although non-governmental Internet actors have exploited the Internet in all possible ways, the following are seven categories by which all Internet uses of terrorists can be included (Dilipraj,2015):

- 1. Communicate with the organization.
- 2. Advertising and publicity.
- 3. Psychological war.
- 4. Fundraising.
- 5. Data collection and dissemination of information.
- 6. Recruitment and mobilization.
- 7. Planning and coordination.

### IX. How does international terrorism happen?

The war against international terrorist organizations has been a main topic in the political field since the September 11 attacks on New York and Washington, DC,. The direct and indirect damages of terrorism - from loss of human lives and ruin of resources to low financial growing and contentment with life - are countless, that developing sound counter-terrorism strategies is a must now. However, the previous years have revealed that there is no global anti-terrorism strategy. This is relatively due to the different and covert features of terrorist organizations, partially because of misconceptions, absence of detailed knowledge and differing interests, and prioritization by policy makers. This chapter aims to provide a logical overview of the way of dealing with terrorism (international), taking into account the perspective of law and economics. More specifically (**Krieger and Meierrieks,2017**).

Global terrorism is a response for some societal, racial and ethnic parties to the developments of globalization. The civilization and the modernization of traditional societies of some of these groups made them feel that their rights are have been violated. With no chance to fight for their own interests, they resorted to terrorist acts as a strategy of fighting for the weak against the dominant. It is crucial to note that violent act is not as significant to terrorism as to the sense of terror and weakness that emerges in the general public after a new terrorist attack. Based on this, terrorism can be seen as threat directed at the Regimes of democratic States (Vavrenyuk, 2018).

## X. The concept of Crimes against Humanity:

The term "humanity", when taken in the latter sense, refers to humanity - the group of individuals - not humanity. Under this interpretation, "crimes against humanity" indicates that the distinguishing feature of these crimes is the party concerned. In law, some mistakes - especially civil errors - such as damages - are thought to affect only victims and their dependents. Other mistakes, committed with the same number of victims, also violate important community standards, and society will seek to establish these rules independently of the victim. These mistakes are crimes, not harm

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



or other civil violations, and society, not just victims, has a distinct interest in punishment (Luban, 2004).

The vagueness of the concept of criminal acts against innocent civilians means that the first basic phase in the process of creating a clear definition of the term, as Grass acknowledged, must be the reforming of the term. The implementation of this reconstruction process is not a mission that can be achieved in a vacuum or on the basis of formal principles - instead of all interpretation; this reconstruction might be achieved only by referring to the guidelines, with more unity and clearness in these principles leading to greater unity and clarity. This paper proposes a "centralized approach to photography", fully defined in below, as the main fundamental principle in light of the reconstruction process (William et al.,1981).

The concept of crimes against humanity is applied in many areas of international law to establish the individual criminal responsibility of its perpetrators in international humanitarian law (IHL) and international criminal law ("ICL") and to define State responsibility in international human rights law (IHRL) (CMN, 2017), Cites the concept of crimes against humanity as a de facto justification for American intervention in the European front of World War II as a justification for dropping nuclear bombs on the Japanese Empire (Ólafsson,2012).

To analyze the evolution of crimes against humanity in international criminal law, it is essential to define and understand the concept of crime. The term "crimes against humanity" broadly describes "anything that is committed on a large scale".

- 1. Prior to the activation of criminal behavior, it is necessary to recognize the legal concept of crime that comes, but also differs from, its concepts contained in various international documents.
- 2. Professor David Le Pen provides a detailed philosophical and legal analysis of the concept of crime. Following the thinking of various credible voices such as Mary Ann Glendon and Hannah Arndt, among others.
- 3. It is indeed possible to observe that the concept of understanding crime itself is the term "humanitarian".
- 4. Thus, consideration of the various concepts of crime and the importance of the term "humanity", which denotes the "party of interest" in the crime.
- 5. The concept of crimes against humanity can be restricted in a few distinct respects.
- 6. Behavior must be violent and severe. This first aspect presents the international character of this crime. Abhorrent acts, in fact, focus on the whole society.
- 7. The development of criminal acts against humankind in international criminal law, Asun Solodovirie, is a person who is entitled to prosecute crimes against humanity, despite the place of any wrongdoing, nationality of the offender, victims or national legislation.
- 8. Although it is an international crime, it is not necessary to commit such acts across State borders.
- 9. The act must be part of a extensive or organized attack. As part of a broader attack, criminal behavior is a matter of international criminal law. The existence of a plan or policy is a controversial point that divides the world arena. It is undoubtedly a simple

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



requirement because it will determine the broad scope or methodological nature that characterizes the violation of humanity for all humanity, but it is not necessary. In Koranak and others, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY) stated that "it is not necessary to show that [the attacks on civilians] were the result of a policy or plan."

- 10. The Appeals Chamber, however, according to Sherif Bassiouni, "completely ignored an article of the Rome Statute and various comments supporting the requirements of State policy".
- 11. As can be seen from this last quote, State participation also plays an important role in the debate on policy requirements. However, this was not an explicit legal requirement. Politics, in fact, does not need to come from a central government.
- 12. Victims must be civilians, whether nationals or foreigners. This fundamental aspect distinguishes between crimes against humanity and war crimes that regulate attacks against civilians during armed conflict. It can therefore be argued that crime is not necessary in relation to an armed conflict, as is evident, inter alia, through the ICTY Trial Chamber ruling in the Tadić case and ICTR trials (crimes against humanity).
- 13. Victims are generally chosen because of their common humanity rather than individual characteristics. Humanity here refers to the "human group" and therefore, "individuals on a non-individual or collective basis".
- 14. The Trial Chamber of the International Criminal Court for the Former Yugoslavia also stated. The Evolution of Criminal acts against Humanity in the International Criminal Law Assunta Soldovieri According to Erdemovic, these crimes "go beyond the individual, so it is essentially the concept of humanity as a victim that characterizes crimes against humanity."

#### **XI.** The Evolution of the Global Prosecution of the Crime:

Crimes against humanity are a fixed crime with a limited definition. However, its presence in the international criminal arena has always been relevant. As described in this writing, for the first time, the Nuremberg Charter effectively criminalized and tried crimes against humanity, even though they were already present in customary international law. Since Nürnberg, however, many international documents have adopted different concepts of crime to adapt the behavior to time. In fact, the Tribunals for the past Yugoslavia and Rwanda, as courts and other special tribunals in past decades, have adapted the conditions required to define crimes with the specific events they have encountered. Article 7 of the International Criminal Court Statute provides for the broader and broader define of crimes against humanity. The ICC, in fact, is not concerned with a particular situation, but is supposed to adopt a wide range of inhumane behaviors all over the world. Despite the ambiguities and ambiguities, the general elements of crime highlighted in the Rome Statute are: (1) the existence of a widespread or systematic attack, which may be supported by a State or regulatory policy, (2) against any civilian population C) knowing the circumstances. The International Law Commission has chosen these latest standards and incorporated them into the draft Treaty on the Deterrence and Penalty of Crimes against Humanity.

International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



Drafting began in August 2015, following the initiation of the Crimes Against Humanity Initiative. The International Convention will be a comprehensive approach to crime, aimed at unifying and promoting the prosecution of similar behaviors at the national and international levels (**Soldovieri,2015**).

# XII. The victimasation and abuse concept in the international criminal law:

The victims shall be victims only if they (i) suffered a significant or unjust loss or loss of well-being; in this way they were unable to prevent the loss; (2) the loss had a specific cause; and (3) the legal or moral context of the loss was awarded Suffering from the loss of social attention, the concept of victim requires that the suffering loss should not only be disposed of but also be acted upon by a specific agent. Caesar, who died of stab wounds, was the victim of an assassination. Plato, who died in his sleep, was not a victim. Caesar's operation was carried out, moreover, acted upon a specific cause. Plato was not dealt with. His body stopped working. The owner of the house and her house acted because of the flood. The ticket-holder was not disposed of: he lacked something. To be a victim, something or something must act on it. Bad luck alone does not make the victim (Sank and Caplan,1991), The victim is a psychological state for an individual who views himself as a victim and feels victimized (Tal et al.,2009)

The victim is a person suffering from devastating, harmful, severe, chronic, emotional, mental, and / or physical abuse, which derives from real or perceived threats or acts and is therefore traumatized. The victim may continue to engage in trafficking or may not be involved in it, but it is still traumatized in some or all of the following ways: continuing dysfunctional professional or personal relationships, moving to other dysfunctional relationships, or living in recurrent crises, Lack of adequate attention to health, lack of desire or inability to reflect or foresight in their lives and situation, lack of targeted movement towards recovery or change, large deficits in positive and non-community relations, or formal support systems (Williamson,2017).

The definition of harm includes physical harm, but it also includes psychological or emotional distress, discomfort, and economic and social deprivation (Williams,2000), and the Merriam-Webster Dictionary (Harm definition,2016) defines damage as "physical or mental injury or injury: something that causes injury or injury to a person or something or is broken, less valuable or successful, etc.".

## XIII. Harm and the precept of authorized things:

As revealed previously, 'harm' formulates the conceptual foundation of up-to-date ICL. However, a relative examination of local criminal legitimate systems plainly indicates that a description of victim could also be built on the distinctive notion of authorized goods. For example, Article (1) of the Code of Criminal Procedure of Poland requires that the injured party (the aggrieved person 18) 'is either a natural or a legal person whose legal interest was infringed or threatened by an offence'. Therefore, it is not the notion of harm in general that it matters but of the 'harm' that

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



magistrates in Poland rely on to decide if somebody has earned the victim description (i.e. is the injured person). A close look on international criminal law (ICL), specifically if it contains not merely current law, but 'the law of yesterday' as well, reveals the continuous normative instability of conceptions and notions originated either inside (i.e. by courts of law themselves) or outside the province of already standing international legitimate context through the 'judicial activity' of the subjects of global law (i.e. federations). This includes also theoretical modifications and advances that have been progressively presented into the model of international criminal system in the former 75 years of its improvement. Today, international criminal tribunals are not based upon the binary or triangular configurations, which were accustomed to be the tradition in the 1940s and 1990s, when records went exclusively around juries, prosecutors and the suspect (CTC WestPoint,2014).

A significant normative modification happened in this regard thanks to the adoption of the Rome Statute of the International Criminal Court (hereinafter ICCSt.) in 1983. It presented a novel player, mostly unnoticed in practice for long years, to the stage of international criminal law. This player – the victim of international crimes to be precise – has been given not merely the right to contribute and to be safe in the actions before the Court (Art. 68 ICCSt.), but also the privilege to demand compensations for the suffered injury (Art. 75 ICCSt.). At least in theory, therefore, giving victims legal recognition as 'victims of international crimes', and not merely as 'witnesses' whose only role has traditionally been to deliver (Karski,1993).

Proof either to the prosecutor or to the defense, changed international criminal justice into a further comprehensive environment for the articulation of conflicting welfares between different sides in international criminal tribunals. Therefore, in the late 1990s what was either a binary or a triangular model for so long turned into a 'square model' of the international criminal court. It currently includes liberated and unbiased judges deciding the guilt of the suspect, public prosecutors appearing before the Court on behalf of the entire global community and representing the welfares of international fairness by bringing accusations to the Court, the alleged person granted many ritual rights in order to defend his or her position, and finally but importantly sufferers of international crimes expressing their own interests like those whose suffering (damage) provides reason for international criminal prosecutions (**Done at Rome,2002**).

However, because of impartial limits resultant from the Court's order (i.e. deficiency of resources, extensive jurisdiction), the prosecutor's action is characterized by certain discrimination, which explains the view that the Office of the Prosecutor signifies the sample of 'discriminating justice' (**Kaczynski,2015**).

# XIV. Electronic Evidence (E-Evidence) Concept from the perspective of Evidence Law in Criminal Procedure

The twenty-first century witnessed a revolution in technology that fascinated not merely India but the whole world. Using computers is not restricted to organizations but is accessible to everybody with the touch of your finger. IT has eased nearly every single human act. In the time of this Internet world, where the use of computers turn

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



out to be more common, there was an increase of technology growth. The development of information technology (IT) has evolved into cyberspace where the Internet offers equivalent chances for all human beings to access any info, store or analyze documents, etc. using advanced technology. This increased dependence on electrical connections, e-commerce and digital information storage has surely triggered the necessity to change the law on information technology and rules for the acceptance of electronic proof in both civil and illegitimate problems in India. The spread of computers and the impact of information technology on the entire humanity, together with the capacity to save and collect information in numerical system, all required alterations to Indian law to include requirements for digital evidence assessment. The Information Technology Act 2000 is based on the UNCITRAL Model Law on Electronic Commerce. The Information Technology Act of 2000 was revised to permit the acceptability of numerical proof. The modification of the Indian Evidence Act of 1872, the Indian Penal Code of 1860 and the Banker Book Evidence Act of 1891 provide the legislative framework for transactions in the electronic world (Dubey, 2017).

Although electronic evidence is obtained, tuned, analyzed and displayed before arbitration is conducted in diverse means in every Member State. In November 2005, a team of European interdisciplinary specialists began to identify the diverse ways in which electronic proof is presented in the tribunals of sixteen Participant Countries. Belgium, Austria, Denmark, Finland, France, Germany, Greece, the Netherlands, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden and the United Kingdom all of them viewed all notes on the Electronic Evidence Acceptance Project. Earlier study on electronic evidence in European countries is not famous and is very partial in nature because not a single country of them have been doing comparative studies. None of them dealt with "admissibility". The project was intended to offer an solution to the present state as absence of awareness in this area hinders criminalization of cybercriminals. The study was monetarily supported by the European Commission in the AGIS framework program. The basic goals of the action were to comprehend the present organizational state and practice and how to improve them. The other objectives were to categorize gaps in the various procedures on the acceptability of electronic evidence and to establish a European network for collaboration in admissibility procedures and performs. It is an ambitious and new project accomplished by a group of interdisciplinary researchers: police officers, attorneys, sociologists, engineers, businessmen, scholars and criminological specialists (Insa,2007).

# Electronic Communication Infrastructure: "Electronic communications":

Electronic Communication implies any transmission of symbols, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by an electronic system. This component have something to do with comprehending the variability of virtual communication methods like electronic mail, direct electronic messaging, Facebook traveler, the variability of apps, then forth. There is a customary

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



rule related to every medium, Electronic communications require free electronic access of everybody to participate in the Net. Therefore, to have full electronic participation in an electronic society helping to run and develop electronic access must be an aim of all electronic societies (US Electronic Communications Privacy Act,2013).

#### **Electronic Economical Infrastructure:**

An electronic society needs an electronic economy. It means all business and markets (electronic purchasing and marketing of goods and services) should be done electronically, So, Netizens must gain an understanding of how to be operative customers in a new electronic economy. This is the capability for users to be aware of Infrastructure: Cultural issues of Electronic that much of t Electronic Cultural Citizenship known as "Electronic Literacy" or "Etiquette". Electronic literacy refers to the process of educating and learning about technology and the usage of technology. Since technologies of cyberspace develop, Netizens must gain some knowledge of how to properly and appropriately use that technology. Electronic Citizenship implicates teaching people in a novel way— these persons require a high degree of information learning skills, Therefore, Electronic literacy is dealing with the comprehending of how to utilize numerous digital devices. (For instance, the way to properly look for one thing on a quest engine vs. a database). Electronic Etiquette also refers to electronic standards of conduct or procedure (i.e., appropriate conduct). Individuals often perceive this area as one of the most pressing difficulties when dealing with Electronic Citizenship. Although rules and regulations are created or the technology is simply banned to stop inappropriate use but it is not t enough to create rules and policy. Every Netizen must teach to become a responsible electronic citizen in the society of Net. Moreover, another related issue that should be considered under the subsection of Cultural Infrastructure, is Electronic or Digital Health and Wellness, which talks about physical and psychological well-being in cyberspace.1Digital citizens should bear in mind of the physical stress placed on their bodies by web usage. They must bear in mind to not become to a fault obsessed with the web inflicting fatigue, headaches, stress issues, and so on Eye safety, repetitive stress syndrome, and sound engineering science practices are problems that require to be addressed during a new technological world. Beyond the physical problems are those of the psychological problems that are getting a lot of current like net addiction, Users need to be taught that there are inherent dangers of technology. Digital Citizenship includes a culture wherever technology users are educated the way to shield themselves through education and coaching. He economy is regulated on-line (Aksel, 2014).

Electronic Legal Infrastructure: Legal subtraction of information technology can be considered as the most important element of an electronic society. In any society, there are individuals who infringe the laws of society and rights of others by committing criminal conducts or doing civil wrongs. The same is true for an electronic community; Therefore, the establishment of electronic citizenship law requires a legal framework to ensure the rights and responsibilities of individuals in

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



cyberspace. Cyber law generally deals with security of electronic environment, which means that citizens must take measures to be safe by practicing using difficult passwords, virus protection, backing up data, and so forth. It also deals with rights and responsibilities of citizens such as privacy, speech, and so forth. Netizens should know that the cyberspace is not free from laws and regulation, so they must help how the information technology is to be used in an appropriate and legal manner (self-protection) (**Dutton,2011**).

#### The Netizn: An Electronic Citizen:

The word "Netizen" comes from combining two words, "Net" (or network) and "Citizen" which means: a Net (work) Citizen or it is a mixed of the words "Internet" and "Citizen" which means: "citizen of the net" (Hauben,2008), The conception of Netizen is additionally ordinarily cited alternative expressions like: "Internet Citizen", "Network Citizen", "Digital Citizen" or "Cyber Citizen" that square measure used identically and synonymously. Netizen has given definitions in diverse attitudes. Some are as follows:

- 1. A Netizen allude to resident (of the actual space) using or utilizing information technology as a device in order to take part in society, political affairs, and government contribution (Mossberger et al.,2011).
- 2. Netizen means inhabitant of an internationally linked Internet (Aksel, 2014).
- 3. Netizens or electronic residents might be defined as "those who use the Internet regularly and effectively" (Wellborn,2013).
- 4. Netizen is a person who is responsible and cares for the Net (**Rebecca,2012**).
- 5. A Netizen is one who has the abilities, understanding, and the right to use the Internet by electronic devices to interact with others (Naavi,2004).

#### XV. Rights And Responsibility of Electronic Citizen:

The world has become completely dependent on the virtual world in its dealings, especially the Internet world, has entered all walks of life, and cannot be separated from modern life. This expansion has created two different worlds, one unrealistic and the other virtual. Here, the challenge and the conflict between the two worlds began, which dominated the other and the basis of the dealings, and through this debate, infiltrated another world is the world of crime or reality world Criminal.

In order to identify the virtual image of this person or the DNA of this electronic character, each person must have his or her own clear identity, which reveals an indication of the deviation of the use from the known line and the tendency towards electronic crimes.

The e-community is an integrated virtual society that reaches each other by default without encountering it. But the end is to deal with and need community laws, whether virtual or real, to resist the tyranny of criminal and irresponsible behavior towards others and to preserve the rights of others and to leave legal distance between individuals Some of them and some to follow the people's realism and unrealistic any hypothetical.

Any society with rights and duties for every individual is free and free. He cannot be deprived of his freedom. He is not subject to any rules or regulations. This requires

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



electronic police, electronic law, and court to regulate relations as accurately as any society.

The social changes have become very huge. For example, the social networking sites have been included instead of the social communication itself, and people are very close to each other, even special transactions such as illness, marriage and family relationships. Eid finds a father who brings his children, Including thousands of kilometers, but the virtual world facilitated this relationship.

And now you can imagine how there should be laws and relationships, for example, a man who wants to send money to his father from Europe, and the letter arrived to the dancer and blew up the amount in his favor, here must be put laws to follow this pirate and catch him and return the amount and subdue the thief.

This incident was not one country or two countries, for example, in Germany, and all the distances to reach Sudan and the thief from Egypt, for example, and the service provider from America, this broad community needs to legislate in Germany, then Sudan and Egypt, The same degree is the default group.

#### XVI. conclusion:

- 1- Cybercrime is a crime like the usual crime of the old age and practiced by criminals.
- 2- Criminals must be prosecuted everywhere, whether it be an electronic crime or a common crime.
- 3- States do not consider these crimes as if they are satisfied with them or they do not care.
- 4- The international community, according to the study, lacks a law or laws to regulate dealing with the virtual society.
- 5- The International Tribunal does not have any legislation dealing with electronic crime or the idea of cybercrimes.

### **XVII.** Results:

Of the most important findings of the study include

- 1- Current global developments show that terrorism is unlikely to be terminated in the coming few years, despite the cooperative efforts by the United Nations, the international community and its Member States. Through the "war on terror", the United States has taken the lead in this regard.
- 2- The invasion of Afghanistan in 2001 was carried out as a consequence of the terrorist strikes of September 11 in the United States America. Since then constant unrest continued in the Middle East.
- 3- The case law on terrorist organizations in these three authorities, and particularly the legal values resulting from the proportion or jurisdiction of these provisions, indicates that, despite tariff variances, there seems to be a similarity of legitimate values arising from jurisprudence.
- 4- A relative examination of the judicial principles arising from the proportions of each of the Supreme Court's rulings on terrorism discloses an extensive variety of principles of law which, in some cases, apply in particular to the

#### International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



legal system of their State. What is more clear is that these lawful principles are alike, and if they are considered as a whole, they are perfectly reliable.

- 5- These legal values seem to show a similarity rather than a difference in this area of crucial importance to domestic criminal law. This supports both transnational and global counterterrorism policies, laws and strategies because it suggests that what seems to be developing is a public comprehending of what creates terrorism, at least through these three main jurisdictions of public law.
- 6- The Supreme Courts recognize the obligation to abide by legitimate principles and domestic and global rules when applied.
- 7- Governments shall take measures to combat terrorism and apply them. Thus, these highest courts confirm that the actions of their governments are constitutionally right and legitimately effective. This might be far away from revelation or original, but it is nevertheless comforting given the fears that the magistrates may be unsuccessful to function as a bulwark or advocate for public rights, human rights and human self-esteem.
- 8- In view of the increasing wave of "fear" of terrorism over the past couple years, prosecuting terrorist cases is, for sure, one of the counterterrorism policies, the courts must, in all cases, be particularly attentive in guaranteeing that their administrations do not overstep their authority And ensure the rights of its citizens to the highest degree while protecting their safety simultaneously as far as possible.

#### **References:**

280

- 1. Aksel, B. S. (2014), Global Citizen: Challenges and Responsibility, Sense Publishers: Netherland.
- 2. Al-Balawi, Salem Hamid Ali (2009) Modern Techniques in Criminal Investigation and its Role in Crime Control, Department of Police Sciences, Graduate School, Naif University for Security Sciences.
- 3. Blair, Michael J. (2006). Research Paper on Internet Deception Tactics, Master of Science in Computer Information Systems, School for Professional Studies, Regis University.
- 4. Choi, Hyunsang, Hanwoo Lee, Heejo Lee, Hyogon Kim (2007). Botnet Detection by Monitoring Group Activities in DNS Traffic, in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007).
- 5. CMN (2017). Crime against Human, International Law Research and Policy.
- 6. Conway, Maura (2003). Cyberterrorism: The Story So Far, Department of Political Science 1, College Green, Trinity College, Dublin 2, Ireland.
- 7. CRID University of Namur (2005). First Analysis of the Personal Data protection Law in India, Report delivered in the framework of contract JLS/C4/2005/15 between CRID and the Directorate General Justice, Freedom and Security.

## **International Journal of Humanities and Social Sciences**

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



- 8. CTC WestPoint. (2014). Paper Cadet/Student Conference on terrorism,insurgency, cyber and asymmetric conflicts.
- 9. CTC WestPoint. (2014). Paper Cadet/Student Conference or terrorism,insurgency, cyber and asymmetric conflicts.
- 10. Dacey, Raymond, & Kenneth Gallant (1997). Crime control and harassment of the innocent, Journal of Criminal Justice, Elsevier, vol. 25(4)
- 11. Definition of Harm . (2016). In Merriam-Webster. Retrieved from http://www.merriam-webster.com/dictionary/harm
- 12. Dilipraj, E (2015). Challenges of Terrorism in Cyber Space, Defence and Diplomacy Journal, Vol. 4, No. 3.
- 13. Done at Rome (2002). on 17 July 1998, in force on 1 July 2002, United Nations, Treaty Series, vol. 2187, No. 38544, Depositary: Secretary-General of the United Nations, http://treaties.un.org
- 14. Dubey, V. (2017). Admissibility of Electronic Evidence: An Indian Perspective. Forensic Res Criminol Int J 4(2).
- 15. Dutton, W. (2011), Freedom of Connection Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet, UNESCO.
- 16. Eagles, Paul F.J., Angela M. Gilmore, Luis X. Huang, Denise A. Keltie, Kimberley Rae, Hong Sun, Amy K. Thede, Meagan L. Wilson, Jennifer A. Woronuk, Ge Yujin (2006). Tourism And Recreation System Planning in Alberta Provincial Parks, Proceedings of the 2006 Northeastern Recreation Research Symposium, GTR-NRS-P-14.
- 17. Hao, Jianlei and Bingbing Gao (2017). Advantages and Disadvantages for Nurses of Using Social Media, Journal of Primary Health Care and General Practice, Vol. 1, Issue 1.
- 18. Hardy, Keiran (2010). Operation Titstorm: Hacktivism or Cyberterrorism?, UNSW Law Journal, Vol. 33(2).
- 19. Hauben, Michael (2008). Net and netizen: the Impact the Net has on People's Lives, A netbook titled Netizens: On the History and Impact of Usenet and the Internet, columbia.edu and rh press: U.S.A.
- 20. Insa, Fredesvinda (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study, Journal of Digital Forensic Practice, 1:4, 285-289
- 21. Jain, Neelesh, & Vibhash Shrivastava (2014). Cyber Crime Changing Everything an Empirical Study, International Journal of Computer Application, Vol.1, Issue 4.
- 22. Jamal, Brahimi (2018) Criminal Investigation of Cybercrime, PhD thesis, Department of Law, Faculty of Law and Political Science, Mouloud Mameri University, Tizi Ouzou
- 23. Jwaifell, Mustafa, Sami F. Aljazi , Al-Mothana Gasaymeh (2019). The Digital Citizenship and Its Role in Facing Electronic Terrorism among Secondary School Students in Middle East: Jordan as an Example, International Journal of Learning and Development , Vol. 9, No. 1.

DOI: 10.33193/IJoHSS.18.2021.189

281

## International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



- 24. K. Karski, Realizacja idei ustanowienia międzynaro. (1993). K. Karski, Realizacja idei ustanowienia międzynarodowego sądownictwa karnego, "Państwo i Prawo.
- 25. Kaczynski, H. (2015). The Accusation Model before the International Criminal Court. Study of Convergence of Criminal Justice System, Heidelberg–New York–Dordrecht–London.
- 26. Kaur, Navneet (2018). Introduction of Cyber Crime and Its Type, International Research Journal of Computer Science, Vol. 5, Issue 08.
- 27. Krieger, T., and D. Meierrieks (2017). How to Deal with International Terrorism. In: Eger, T., S. Oeter, and S. Voigt (Eds.): International Law and the Rule of Law under Extreme Conditions. Mohr Siebeck, Tübingen, pp. 223-247.
- 28. Kumar, Rajnish (2000). Data Protection and Liability, National Academy of Indian Railways, Vadodara.
- 29. Luban, David (2004). A Theory of Crimes Against Humanity, Yale Journal of International Law, Vol. 29, Issue 1.
- 30. Matusitz, J. (2007). Cyberterrorism: Postmodern state of chaos, Information Security Journal: A Global Perspective, vol. 17, no. 4.
- 31. Mossberger, k. Caroline J.T., and Ramona S. (2011), Digital Citizenship: The Internet, Society and Participation, MIT Press: U.K.
- 32. Naavi, N.V. (2004), Cyber Laws for Every Netizen in India, Ujvala Consultants Pvt Ltd: India
- 33. Ólafsson, Garðar Steinn (2012). Crimes Against Humanity Emergence of a law of humanity, School of Social Sciences, Faculty of Law.
- 34. Pope, Lcdr Lonnie (2008). Cyber-Terrorism And China, United States Marine Corps, Command and Staff College, Marine Corps University.
- 35. Qara, Laila (2012), "The Impact of Electronic Money on Monetary Policy", Unpublished Master Thesis, Al-Arabi Bin Muhaidi University, Umm Al-Bawaki, Faculty of Economic Sciences, Commercial Sciences and Management Sciences, Finance and Banking, Algeria.
- 36. Raj, S. Praveen and Aswathy Rajan (2018). Comparison between Information Technology Act, 2000 & 2008, International Journal of Pure and Applied Mathematics, Vol. 119, No. 17.
- 37. Rebecca.M.K. (2012). the Netizen, Development 55(2), 201–204.
- 38. Rusumanov, Vase (2016). The Use of The Internet By Terrorist Organizations, Information & Security: An International Journal, Vol. 34:2.
- 39. Ryngaert, Cedric (N.D.). The Concept of Jurisdiction in International Law, International Law, Utrecht University.
- 40. Ryngaert, Cedric (n.d.). The concept of Juridiction in international Law. Utrecht University.
- 41. Sank, Diane and David I. Caplan (1991). To Be a Victim Encounters with Crime and Injustice, Springer Science, Business Media, LLC.
- 42. SEissa, Israa G., Jamaludin Ibrahim, Nor-Zaiasron Yahaya (2017). Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review,

## International Journal of Humanities and Social Sciences

website:www.ijohss.com Email:editor@ijohss.com ISSN: 2415 – 4822

العدد (18) يناير 2021 Volume (18) January 2021



International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Value (2015).

- 43. Soldovieri, Assunta (2015). The Evolution of Crimes against Humanity in International Criminal Law, Boletín mexicano de derecho comparado / Instituto de Investigaciones Jurídicas, UNAM 47(139):241-281.
- 44. Tal, Daniel Bar, Lily Chernyak-Hai, Noa Schori and Ayelet Gundar (2009). A sense of selfperceived collective victimhood in intractable conflicts, International review of the red cross, Vol. 91, No. 874.
- 45. US Electronic Communications Privacy Act, 2013, s.2510.
- 46. Vavrenyuk, Sergey Anatolievich (2018). International terrorism and the basic ways to deal with it at the present stage, CES Working Papers Vol. X, Issue 2.
- 47. Veerasamy, Namosha, Marthie Grobler (2011). Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure, Council for Scientific and Industrial Research, Pretoria, South Africa.
- 48. Waidan, Ahmad Abdullah (2015) "Criminal Responsibility of the Individual in Islamic Law and International Criminal Law Comparative Study", Ph.D., Faculty of Sharia and Law, Malaysian Islamic University, Nielay.
- 49. Wellborn, J. (2013). Cyber citizenship: Helping Teenagers Be Good Netizens, International Journal of Human and Social Science, 30(1):171-197
- 50. Werle, G. (1997). Menschenrechtsschutz durch Völkerstrafrecht, in Zeitschrift für die gesamte Strafrechtswissenschaft.
- 51. William Felstiner, Richard Abel & Austin Sarat (1981). The Emergence and Transformation of Disputes: Naming, Blaming, Claiming..., 15 LAW AND SOC. REV. 631, 635
- 52. Williams, Marie (2000). Ethical clearance just a rubber stamp?, Australian Journal of Physiotherapy, Vol. 46.
- 53. Williams, Sarah (2009). Hybrid and Internationalized Criminal Tribunals: Jurisdictional Issues, A Doctoral Thesis, Durham University.
- 54. Williamson, Celia (2017). Definition of Victim, Survivor, and Thriver, PhD in conjunction with the Lucas County Human Trafficking Coalition.