**Inbar Yishai-Deri**

**ID No:** UD81199HLE90416

Course Topic:

**cybersecurity and Counterterrorism-**

**a multi-jurisdictional crime**

ATLANTIC INTERNATIONAL UNIVERSITY

**Month/year**

**TABLE OF CONTENTS**

**Introduction3**

**1.0 Terrorism as an international crime 4-5**

1.1 The Cyber borders 6

2.0 International or universal jurisdiction 7-8

2.1 multilateral cooperation ……...……………….....………...……..……………............…8-9

**3.0** **International organizations …………………...….……….…….....……………....……10-11**

3.1 United Nations ………………….…………………………………………….….……11-12

**4.0 Regional organizations …………………………………………………...…………………13**

4.1 The European Convention on the Prevention of Terrorism……………………...………..13

4.2 International Multilateral Partnership against Cyber Terrorism…………………………. 14

**Conclusions………..…………………………………………………………………….…….…15**

**Bibliography……………………………………………………………..………….…….….16-17**

**Introduction**

In light of the growing concerns surrounding cyber terrorism and its consequences, many international organizations have taken steps to deal with this global threat. Recognizing cyber terrorism as an international crime, it has become clear that domestic regulations alone are not sufficient to prevent such attacks; A common, transnational approach is needed. As a result, states affected by cyber terrorism turn to international law, evoking universal jurisdiction to seek retribution for any resulting damage. Without the support and coordination of international organizations, effectively preventing cyber terrorism remains a challenging task. These organizations play a critical role in determining which country or international court has jurisdiction to settle disputes[[1]](#footnote-1).

The threat at the theoretical level posed by cyber terrorism has indeed caused a great deal of concern. Many cyber and security experts have publicized the danger of cyber terrorists hacking into private and government computer systems that have the power to harm the military sectors, financial trade centers and services of advanced economies. A combination of political, psychological and economic factors contributed to the dispersal of fear around cyber terrorism. From a psychological point of view, the term "cyber terrorism" contains two of the most well-known fears in today's society. It seamlessly blends the fear of arbitrary and violent victimization with the prevailing skepticism and fear of computer technology[[2]](#footnote-2).

It also highlights the idea of cyber-terrorism not only as a local matter but as a transnational crime and international threat, requiring a more collective and unified approach to prevention and protection. This work aims to examine why cyber terrorism should be treated as a cross-border crime that justifies universal jurisdiction through multinational cooperation. This view is considered the most appropriate and correct strategy for dealing with future transnational crimes, including cyber terrorism[[3]](#footnote-3).

1. **Terrorism as an international crime**

The rapid advancements in technology have undoubtedly brought numerous benefits to humanity. However, this progress has also led to the emergence of cyber terrorism, which stands as one of the most concerning global threats. The rise in cyber-attacks targeting critical information infrastructures of sovereign states has highlighted the necessity for a comprehensive international response. While regional and bilateral agreements, as well as local legislation, have been implemented, they alone are insufficient in deterring cyber threats. Consequently, the application of international law has become indispensable in addressing these challenges across various jurisdictions. Effective solutions to counter transnational cyber threats require a comprehensive examination of existing international treaties. The challenge of prosecuting cyber-attacks conducted in multiple states emphasizes the need for a stronger foundation in international law[[4]](#footnote-4)

In this context, the principle of universal jurisdiction assumes particular significance, serving as a mechanism for invoking international law to seek justice for the damages caused. The authority of multilateral organizations becomes essential in the exercise of universal jurisdiction when a sufficient number of states accede to these international agreements. As cyber terrorism transcends national borders, collaborative efforts among nations and multilateral organizations become vital in combating this global menace. Notably, the Council of Europe Convention on Cyber Crime has emerged as a pivotal international treaty, ratified by numerous states, effectively addressing the complexities associated with cybercrime at the present time[[5]](#footnote-5). The term "cyber terrorism" has gained widespread usage, yet there is still no universally agreed-upon definition. Existing definitions range from being overly inclusive to overly restrictive. A narrow definition might overlook critical components of large-scale cyber-attacks, while an overly broad definition might encompass regular cybercrimes within the category of cyber terrorism.

However, among the many proposed definitions of cyber terrorism, there are some common elements that contribute to a common understanding of the concept. One prominent definition, offered by Dorothy Denning, combines the motive, purpose, and goals of the attack. Denning defines cyber terrorism as "the convergence of terrorism and cyberspace". This definition focuses on the illegal attacks or threats of attacks on computers, networks and the data stored in them. These actions are intended to intimidate or coerce a government or its people in pursuit of political and social goals. Such a definition provides a comprehensive framework for understanding the complexities surrounding cyber terrorism[[6]](#footnote-6).

Denning's commentary emphasizes that cyber terrorism can have a similar effect to traditional terrorism. In addition, scholars such as Pollitt define cyber terrorism as a premeditated attack, coming from a political view of information systems and computers, which brings to mind violence against non-combatant targets by subnational groups and secret agents[[7]](#footnote-7).

His emphasis lies in the requirement that an act of cyber terrorism must culminate in violence, an aspect not explicitly mentioned by Denning, which distinguishes it from her definition. Examining different definitions of cyber terrorism, the conclusion is that the factor that distinguishes cyber terrorism from other cyber crimes is the motive and intention of the perpetrator or the group behind the attack. Cyber terrorism has been characterized as a contemporary form of traditional terrorist activity, using new technologies. Terrorist groups have moved from physical attacks to cyber attacks, taking advantage of the ability to carry out attacks from a distance, regardless of geographical barriers. These attacks are carried out through cyberspace, and may yield far-reaching and more serious consequences compared to conventional terrorism. While traditional acts of terrorism are usually limited to specific locations, cyber terrorism can be carried out across vast areas or networks through information and cyber attacks, using computers located remotely from the site of the attack[[8]](#footnote-8).

1.1 The Cyber borders

Organizing around cyber threats and information security has already worried professionals in both fields ahead of time. Many criminals and other foreign actors have been using cyber methods to bypass sophisticated security measures and cross physical borders for many years. According to the latest information, almost every threat that exceeds the definition of crime or homeland security that once required a physical connection with a country's traditional borders is carried out or facilitated by a cyber agent. Vulnerabilities in cyber security have caused panic and insecurity, in many respects, certain aspects of traditional border security, making them less effective. This merger of border security and traditional cyber should be thoroughly examined and a policy advocated for the integration of the cyber domain into the concept of border security should be proposed. Drawing on the policy work that began over a decade ago during her tenure as director of the US Customs Service's National Cybercrime Program, a description of the process of defining and enforcing a national cyber border can be seen[[9]](#footnote-9).

In the virtual world, cyber criminals and cyber terrorists use computers as tools to target other computer systems. Terrorists use different methods to launch their attacks, the consequences of which can extend beyond the virtual realm, resulting in the destruction of property and loss of life in the real world. The inherent anonymity provided by the Internet poses a significant challenge in attributing attacks to specific countries, making it essential for countries to cooperate and share information to identify the perpetrators. Terrorist groups have increasingly shifted from traditional physical attacks to cyber-attacks, leveraging the borderless nature of cyberspace to carry out their operations and evade detection. The ability to hide their identity and location allows them to spread fear, cause widespread casualties, and coerce targeted countries into compliance. As a result, the international community must recognize cyber terrorism as an international crime, requiring a unified global response. The transnational complexity associated with cyber-terrorist activity poses significant challenges in terms of prosecution and legal investigation, prompting attacked states to seek justice through international law[[10]](#footnote-10).

**2.0 International or universal jurisdiction**

Universal jurisdiction applies to the most serious crimes. These crimes fall under universal jurisdiction for two primary reasons: first, due to their egregious nature and widespread impact, involving severe breaches of humanitarian law; and second, because they occur in territories not subject to the authority of any particular country's legislation. Universal jurisdiction can be established through treaty regimes or as a matter of customary international law[[11]](#footnote-11).

The treaty regimes are legally binding on the member states. However, in some cases they also serve as evidence of customary international law. The concept of universal jurisdiction allows the international community, in defined jurisdictions, to override national law with international law. As a matter of customary international law, universal jurisdiction applies to cases of cyber terrorism. This principle is supported by both legal judgment and state practice. Many treaties have addressed various forms of terrorism, including cyber terrorism, which serves as a significant aspect of state practice. Moreover, terrorism is generally considered a serious crime against humanity (opinion juris). These elements together provide a legal basis for the application of universal jurisdiction in the issue of combating terrorism, including cyber terrorism, and subjecting it to international legal responsibility[[12]](#footnote-12).

Crimes against humanity, including genocide, often fall under universal jurisdiction. Considering the serious crime nature of cyber terrorism, which represents a contemporary form of traditional terrorism, the principle of universal jurisdiction can be applied to cyber terrorism cases. The seriousness of acts of cyber terrorism is similar to that of genocide and other crimes against humanity, which are subject to universal jurisdiction. Given the cross-border nature of cyber-terrorism, it is clear that the application of universal jurisdiction is the most appropriate method to effectively address this issue. Therefore, the appropriate response to cyber terrorism should be targeted and international. Similarly, the efforts of international organizations in the fight against cyber terrorism should center around the application of universal jurisdiction and less on technical definitions[[13]](#footnote-13).

Ultimately, the implementation of universal jurisdiction in cases related to cyber terrorism should be carried out through international organizations and their respective tribunals, such as the International Criminal Court and the International Court of Justice, which have been established by the Rome Statute and the United Nations, respectively. International organizations serve as a legitimate platform, established through treaties, to exercise universal jurisdiction over cyber terrorism. It is important to note that the application of universal jurisdiction can be conducted through both the international community and individual states, although the international community holds precedence over national courts in the process of adjudication[[14]](#footnote-14).

Cyber terrorism is indeed a transnational and cross-border crime that extends beyond geographical boundaries. Consequently, the most effective response to combat cyber terrorism should also be transnational in nature. Several treaties have been enacted to address terrorism, and since cyber terrorism is a part of traditional terrorism that utilizes the internet as a means of attack, these treaties may encompass cyber terrorism as well. Moreover, the ease with which the origins of cyber-attacks can be concealed and the fact that these attacks can originate from any location worldwide highlight the truly international nature of cybercrime and cyber terrorism[[15]](#footnote-15).

2.1 multilateral cooperation

Recent statistics have highlighted the effectiveness of multi-party cooperation in responding to transnational cyber terrorism. Given that countries have varying regulations governing extradition, legal assistance, and laws related to computer crimes, a global effort is crucial in preventing and deterring cyber terrorism. Therefore, it is evident that the most effective approach for international cooperation in addressing cyber-attacks has been predominantly multilateral in nature[[16]](#footnote-16).

Put plainly, a treaty carries several political implications that can further the fundamental objectives of security, prevention of particular offenses, facilitating prosecution and extradition, and ultimately strengthening deterrence against cyber terrorism. By addressing jurisdictional challenges in the investigation of such crimes, treaties can discourage cyber offenders from engaging in cybercrime and cyber terrorism. Furthermore, the collaboration stemming from a treaty fosters cooperation among the signatory nations, as well as technical collaboration, extending beyond the scope of the treaty. Despite the fact that some of the international instruments were not initially designed to address cyber terrorism, their general language is often adequate. While most cyber terrorism activities fall under the purview of these international organizations, certain significant challenges still persist[[17]](#footnote-17).

International cooperation relies on the harmonization of national substantive cybercrime laws that criminalize cybercrime, as well as national procedural cybercrime laws that establish the regulations for evidence and criminal proceedings (as discussed in Cybercrime Module 3 on Legal Frameworks and Human Rights). Furthermore, the harmonization of bilateral, regional, and multilateral instruments on cybercrime, where necessary, can also facilitate international cooperation. Accession to or ratification of regional and multilateral cybercrime instruments is necessary to enforce the legal obligations outlined in these instruments. For more comprehensive information on international cooperation to combat transnational organized crime in general, please refer to the University Module Series on Organized Crime, particularly Module 11 on International Cooperation to Combat Transnational Organized Crime. Bilateral, regional, and multilateral cybercrime treaties (discussed in Cybercrime Module 3 on Legal Frameworks and Human Rights) play a crucial role in fostering international cooperation, provided that the concept of dual criminality is observed. Dual criminality necessitates that the alleged conduct be considered illegal in the cooperating countries. In the absence of dual criminality and harmonized laws, cybercrime safe havens can emerge, shielding perpetrators from prosecution[[18]](#footnote-18).

**3.0 International organizations**

Convention laws established by international organizations offer a legitimate framework for exercising universal jurisdiction over limited aspects of cyber terrorism. However, this scenario presents several challenges. Therefore, achieving a broad consensus is very important for an effective fight against cyber terrorism. Second, the lack of procedural guidelines for investigation and prosecution prevents possible convictions. States must cooperate through multilateral cooperation. This part will focus on the most effective organizational structures, emphasizing efforts aimed at dealing with cyber terrorism on the international stage. While there are many international organizations (including multilateral, bilateral, and regional entities), this article will focus exclusively on multilateral organizations. Examples to be examined will include the European Convention on Cybercrime. Multilateral organizations will be emphasized as they offer the most effective approaches in responding to international cybercrimes and cyberterrorism, addressing the central issue of the lack of an international response to cyberterrorism[[19]](#footnote-19).

The United Nations Office for Combating Terrorism (UNOCT) has spearheaded various initiatives in the field of cyber security and emerging technologies. Dedicated to strengthening the capabilities of member states and private organizations in preventing cyber intrusions orchestrated by terrorist entities targeting very important infrastructure. Aimed at reducing the consequences of cyber attacks, such as Also facilitate the recovery and recovery of targeted systems in the event of such attacks.

In 2022, UNOCT/UNCCT, in collaboration with INTERPOL, launched the CT TECH initiative, the main objective of which is to improve law enforcement and criminal justice authorities in designated partner countries to combat the misuse of new and emerging technologies for terrorist activity. Moreover, the initiative supports the member states in harnessing new technologies in the fight against terrorism. The CT TECH initiative is supported by the European Union and is part of the UNCCT's International Counter-Terrorism Program on Cyber Security and New Technologies.

Also, the office provides specialized knowledge in international forums concerning the utilization of unmanned aerial systems (UAS). Furthermore, it provides assistance in building capacity related to open source intelligence (OSINT), the dark web, cryptocurrencies and digital forensics. Previous projects led by UNOCT focused on leveraging social media to collect open source information and digital evidence, with the aim of successfully dealing with terrorism and extremist and violent acts while maintaining the principles of human rights[[20]](#footnote-20).

3.1 United Nations

The United Nations plays a central and important role in coordinating and expanding cooperation in dealing with the challenge of international terrorism. Its ultimate goal is to maintain global security and peace. To achieve this goal, the UN has established many special agencies and programs. In addition, Resolution 55/63 (2000) and Resolution 56/121 (2001) emphasize the significance of the Group of Eight Principles in combatting the criminal misuse of information technology. Member states are encouraged to take these principles into account[[21]](#footnote-21).

Moreover, other resolutions have urged member states to foster the multilateral examination of current and potential threats in the realm of information security and to contemplate possible measures to mitigate these threats[[22]](#footnote-22).

Following the tragedy of September 11, the UN Security Council's decision to initiate and advance the global fight against terrorism. It gave renewed approval to international peace and security and ordered all UN member states to actively fight terrorist financing, as well as to criminalize terrorist financing operations, and not to give Support for terrorist activities. It also required all member states to cooperate with other governments and international organizations to eliminate all terrorist hideouts. The decision described various aspects of the fight against terrorist activities[[23]](#footnote-23).

According to this resolution, states are obligated to freeze terrorist assets, prevent terrorist activities, cooperate on legal issues and extradition, and coordinate efforts to combat transnational crime, illegal drug trafficking, and arms trafficking. The UN International Convention on Combating and Suppressing the Financing of Terrorism, adopted by the UN General Assembly in Resolution 54/109 in 1999, further encourages international cooperation. According to Article 14 of this treaty, requests for cooperation cannot be rejected for political reasons[[24]](#footnote-24).

The United Nations established a Counter-Terrorism Committee (CTC) to oversee the implementation of Resolution 1373 and provide assistance to countries in developing the necessary capabilities. The CTC, often referred to as the "hub of global efforts to combat terrorism," imposed comprehensive legal obligations on UN member states to address threats Global terrorism. Its scope goes beyond other existing deterrence agreements that bind only those who have voluntarily become parties, in that they require each country to stop the activity of financial assets belonging to terrorists and their supporters[[25]](#footnote-25).

Resolution 1566 of the UN Security Council (2004) compels states to cooperate fully and without reservations in the fight against terrorism, while Resolution 1624, issued a year later, urges states to legally prohibit incitement to carry out acts of terrorism. These two resolutions will be carefully examined. Resolution 1535 of the UN Security Council establishes the Director of the Committee on Combating Terrorism (CTED) to facilitate technical assistance to all countries. Promotion of cooperation between governmental bodies and between regional bodies. In addition, it offers expert advice to the CTC on all issues covered by resolution 1373[[26]](#footnote-26).

**4.0 Regional organizations**

Recognizing the pressing threat of terrorism and acknowledging the limitations of multilateral treaties, regional conventions aim to establish a practical and valid framework for combating terrorism. At the national level, cooperation emphasizes the need for collaboration between the public and private sectors in order to effectively address cyber threats[[27]](#footnote-27).

The Council of Europe established the Convention on Cybercrime, which is discussed in the "International Organizations" section as it has international implications, and the Convention on the Prevention of Terrorism to combat cyberterrorism and other terrorist activities on the internet. However, these conventions, along with other Council of Europe conventions, do not sufficiently address the significant threat of cyberterrorism. This gap in coverage is not adequately addressed by other international organizations[[28]](#footnote-28).

4.1 The European Convention on the Prevention of Terrorism

The Council of Europe has adopted the Convention on the Prevention of Terrorism to enhance the effectiveness of current international measures in the fight against terrorism. The Convention's primary objective is to bolster member states' endeavors to prevent terrorism by establishing specific criminal offenses, including public provocation, recruitment, and training. Additionally, it emphasizes the need for both internal (national prevention policies) and international cooperation on prevention. Notably, this Convention stands out from other European Union framework decisions as it upholds the foundation of human rights in the context of counterterrorism efforts. Despite its strengths, the Council of Europe's Convention on the Prevention of Terrorism encounters limitations due to the absence of comprehensive provisions pertaining to terrorist offenses, thereby necessitating reference to existing treaties[[29]](#footnote-29). What distinguishes this treaty from others is its prohibition not only of incitement but also of "public provocation" when the act of terrorism poses a threat[[30]](#footnote-30)

4.2. International Multilateral Partnership against Cyber Terrorism (IMPACT)

The multi-party cross-border partnership against cyber threats is a breakthrough in the field of cyber security with the support of the United Nations established in 2011, fully cooperating with the United Nations Special Agency for Information Technologies which provides a neutral global platform, bringing together representatives of institutions and governments, to strengthen and advance the world's ability to manage cyber threats.[[31]](#footnote-31)

The Multilateral International Teamwork Against Cyber Threats supported by the United Nations International Telecommunication Union (ITU) and the International Criminal Police Organization (INTERPOL), stands for a joint global private and public agreement directed against cyber threats. Its global headquarters was inaugurated in Cyberjaya, Malaysia on March 20, 2009. IMPACT aims to bridge the gap between domestic and international domains in the fight against cyber threats and fosters increased cooperation in combating such threats. Serving as a centralized cyber terrorism intelligence center, IMPACT provides timely alerts to its 191 member states regarding potential cyber terrorist threats. This includes alerts on potential attacks targeting critical systems such as the global financial network, power grids, nuclear facilities and air traffic control systems[[32]](#footnote-32).

**Conclusion:**

The fight against cyber terrorism and the misuse of the internet by terrorist groups has prompted various suggested solutions, rather than a unified approach. Given the transnational nature of cyber terrorism cases, it becomes imperative to establish a broad international consensus and joint effort to criminalize terrorist activities through the exercise of universal jurisdiction by international courts. Such an approach would ensure that cyber terrorists are brought to justice and that a functional legal framework covering all related issues is put in place. Establishing a common legal definition of "cyber terrorism" based on its unique characteristics not only streamlines the investigative process but also fosters cooperation among countries.

The necessity for a global and concerted response underscores the need to declare cyber terrorism an international crime against humanity. While several treaties exist, few provide binding regulatory jurisdiction, with most dealing with limited regional areas. Efforts by the United Nations and Interpol aim to promote security and prevent cyber-related crime on an international scale. The Convention on Cyber Crime, although considered a regional effort, holds significance as many non-member countries have ratified and joined it. However, it does not currently cover cyber terrorism, emphasizing the need for a protocol specifically addressing this issue.

Multilateral organizations strive to enhance security through the harmonization of legislation, coordinated law enforcement efforts, and the use of direct and indirect anti-cyber terrorism measures. The highlighted measures underscore the necessity for harmonized laws to prevent transnational criminals from exploiting jurisdictional and legal gaps among countries, minimizing opportunities for such activities to thrive.

**Bibliography**

A.D. Sofaer & S.Goodman, Past as Prologue: International Civil Aviation Agreements as Precedents for International Cooperation against Cyber Terrorism and Cyber Crime (1st ed, Hoover Institution Press, (2003).

B. David, A Survey of the Effects of Counter-Terrorism Legislation on Freedom of the Media in Europe, European Digital,(2006).

E. Rosand, The UN-Led Multilateral Institutional Response to Jihadist Terrorism: Is a Global Counterterrorism Body Needed, 3 JCSL 399 (2006).

E. Tikk & R. Oorn, Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, in Responses to Cyber Terrorism 89e92 (Centre Of Excellence Defence Against Terrorism, (2008).

["ITU-IMPACT establishes first Cybersecurity Innovation Centre for Arab region"](https://web.archive.org/web/20140222052518/http:/www.connect-world.com/~cwiml/index.php/press-releases/item/18721-itu-impact-establishes-first-cybersecurity-innovation-centre-for-arab-region?ml=1). Archived from [the original](http://www.connect-world.com/~cwiml/index.php/press-releases/item/18721-itu-impact-establishes-first-cybersecurity-innovation-centre-for-arab-region?ml=1) on 2014-02-22.

G. Weimann, **“How Real Is the Threat”?** United States Institute Of Peace, (2014).

Pardis Moslemzadeh Tehrani, Nazura Abdul Manap & Hossein Taji, **“Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”,** Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia, (2013).

Raphael F. Perl, Head, Action Against Terrorism Unit, Org. for Sec. & Coop’n in Eur., Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation, Remarks at the Second International Forum on Information Security ,(2008).

Rights, Digital Civil Rights in Europe (Dec, 3. 2008). available at <http://www.edri.org/edri-gram/number6.23/speaking-of-terror> (Last Visited April, 23. 2012).

R. Miyawaki, The Fight Against Cyber Terrorism: A Japanese View, Paper Presented to The Centre for Strategic and International Studies ,June, 29 ,(1999).

S.Suleymasn, Cyber Terrorism and International Cooperation: General Overview of The Available Mechanisms to Facilitate an Overwhelming Task, in Responses to Cyber Terrorism 74e75(1st ed, Centre of Excellence Defense against Terrorism, (2008).

S. Wilske & T. Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, **50 Fed. Comm**. L.J. 170e171, (1998).

The UN International Convention for The Suppression of The Financing of Terrorism of 1999, Un treaty series Reg. No.38349,adopted by the General assembly of the United Nations in resolution 54/109 on 9.12.1999.

**Website:**

About The Anti-Defamation League, http://www.adl.org/Terror/tu/tu\_38\_04\_09. (2011).

<https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html>

<https://www.un.org/counterterrorism/cybersecurity>

1. Pardis Moslemzadeh Tehrani, Nazura Abdul Manap & Hossein Taji, **“Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”,** Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia(2013). [↑](#footnote-ref-1)
2. G. Weimann, **“How Real Is the Threat”?** United States Institute Of Peace,(2014). [↑](#footnote-ref-2)
3. Pardis Moslemzadeh Tehrani, Nazura Abdul Manap & Hossein Taji, **“Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”,** Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia(2013). [↑](#footnote-ref-3)
4. G. Weimann, **“How Real Is the Threat”?** United States Institute Of Peace,(2014). [↑](#footnote-ref-4)
5. L. Bantekas, **International Criminal Law**, Routledge-Cavendish Publication, 265 3rd Edn, (2007). [↑](#footnote-ref-5)
6. D.E.Denning, Statement of Dorothy E. Denning (2000), available at [www.house.gov/hasc/testimony/106thcongress/00-05-23denning](http://www.house.gov/hasc/testimony/106thcongress/00-05-23denning). htm.(Last Visited July. 17, 2012). [↑](#footnote-ref-6)
7. M.M. Pollitt, Cyberterrorism fact or fancy?, 2 Comput. Fraud Secur (1998), available at <http://cosc.georgetown.edu/denning/> infosec/pollitt.html (2012). [↑](#footnote-ref-7)
8. D.E. Denning, Cyber Terrorism, 7 (2000), available at http:// www.nautilus.org/rchives/infopolicy/work shop/paper/denning.html. (2012). [↑](#footnote-ref-8)
9. O, Phillip. “Cyber Border Security – Defining and Defending a National Cyber Border. **“Homeland Security Affairs 13”**, Article 5 (October 2017). [↑](#footnote-ref-9)
10. C. Ernest, Cyber Crime: **“New Threat and Global Response”** , Expert Group on Cyber Crime, Department on New Challenges and Threats, (2011) [↑](#footnote-ref-10)
11. L. Nadya Sadat, Universal Jurisdiction: Myths, Realities, and Prospects: Redefining Universal Jurisdiction, 35 New Eng. L. **Rev. 242** (2001). [↑](#footnote-ref-11)
12. International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction, (2008). [↑](#footnote-ref-12)
13. Nadya Sadat, **Supra note 8**, at 243, (2007). [↑](#footnote-ref-13)
14. S. Wilske & T. Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, **50 Fed. Comm**. L.J. 170e171 (1998). [↑](#footnote-ref-14)
15. R. Miyawaki, The Fight Against Cyber Terrorism: A Japanese View, Paper Presented to The Centre for Strategic

    and International Studies (June, 29 .1999). [↑](#footnote-ref-15)
16. S.Suleymasn, Cyber Terrorism and International Cooperation: General Overview of The Available Mechanisms to Facilitate an Overwhelming Task, in Responses to Cyber Terrorism 74e75(1st ed, Centre of Excellence Defense against Terrorism, 2008). [↑](#footnote-ref-16)
17. A.D. Sofaer & S.Goodman, Past as Prologue: International Civil Aviation Agreements as Precedents for International Cooperation against Cyber Terrorism and Cyber Crime, in International Approaches

    to Cooperation against Cyber Crime and Cyber Terrorism (1st ed, Hoover Institution Press, 2003). [↑](#footnote-ref-17)
18. <https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html> [↑](#footnote-ref-18)
19. Pardis Moslemzadeh Tehrani, Nazura Abdul Manap & Hossein Taji, **“Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”,** Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia(2013). [↑](#footnote-ref-19)
20. <https://www.un.org/counterterrorism/cybersecurity> [↑](#footnote-ref-20)
21. United Nations (1945) (UN), available at http://www.un.org/en/aboutun/index.shtml (2011). [↑](#footnote-ref-21)
22. L Xingan, International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene, 4 webology (2007),http://www.webology.ir/2007/v4n3/a45.html (2010). [↑](#footnote-ref-22)
23. About The Anti-Defamation League, http://www.adl.org/Terror/tu/tu\_38\_04\_09. (2011). [↑](#footnote-ref-23)
24. The UN International Convention for The Suppression of The Financing of Terrorism of 1999, Un treaty series Reg. No.38349,adopted by the General assembly of the United Nations in resolution 54/109 on 9.12.1999. [↑](#footnote-ref-24)
25. E. Rosand, The UN-Led Multilateral Institutional Response to Jihadist Terrorism: Is a Global Counterterrorism Body Needed?, 3 JCSL 399 (2006). [↑](#footnote-ref-25)
26. Raphael F. Perl, Head, Action Against Terrorism Unit, Org. for Sec. & Coop’n in Eur., Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation, Remarks at the Second International Forum on Information Security 2 (Apr. 7e10, 2008), available at http://www.osce.org/documents/cio/2008/04/

    30594\_en.pdf. [↑](#footnote-ref-26)
27. Ibid. [↑](#footnote-ref-27)
28. E. Tikk & R. Oorn, Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, in Responses to Cyber Terrorism 89e92 (Centre Of Excellence Defence Against Terrorism, ed. 2008). [↑](#footnote-ref-28)
29. Council of Europe, Cyber Terrorism: The Use of the Internet for Terrorist Purposes 75 (1st ed, 2007). [↑](#footnote-ref-29)
30. B. David, A Survey of the Effects of Counter-Terrorism Legislation

    on Freedom of the Media in Europe, European Digital (2006)

    Rights, Digital Civil Rights in Europe (Dec, 3. 2008). available at <http://www.edri.org/edri-gram/number6.23/speaking-of-terror> (Last Visited April, 23. 2012). [↑](#footnote-ref-30)
31. ["ITU-IMPACT establishes first Cybersecurity Innovation Centre for Arab region"](https://web.archive.org/web/20140222052518/http:/www.connect-world.com/~cwiml/index.php/press-releases/item/18721-itu-impact-establishes-first-cybersecurity-innovation-centre-for-arab-region?ml=1). Archived from [the original](http://www.connect-world.com/~cwiml/index.php/press-releases/item/18721-itu-impact-establishes-first-cybersecurity-innovation-centre-for-arab-region?ml=1) on 2014-02-22. [↑](#footnote-ref-31)
32. Ibid. [↑](#footnote-ref-32)