Research article
DOI: https://doi.org/10.21202/jdtl.2023.43

Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism

Yassin Abdalla Abdelkarim

Luxor Elementary Court
Sohag, Egypt

Keywords

crimes against humanity,
cybersecurity,
cyberspace,
cyberterrorism,
digital technologies,
human rights,
international private law,
international public law,
jurisdiction,
law

Abstract

Objective: the development of wireless technologies and digital infrastructure has radically changed the human habitat, giving rise to a new type of space – a cyberspace. The uniqueness and peculiarities of this environment, including anonymity, boundlessness and problems related to the determination and establishment of jurisdiction, have become a breeding ground for the emergence of a new global threat – cyberterrorism. The latter is characterized by a high level of latency, low detection rate and incomparably greater danger than "real world" crimes. Countering new forms of crime has required the development of universal tools that overcome the limitations of traditional jurisdiction and allow states to prosecute terrorists in cyberspace. Identifying the relevant tools and identifying the political-legal obstacles to their implementation is the objective of this study.

Methods: to achieve the set goal the formal-legal method was used to analyze legal sources, including judicial practice, national legislation, and international acts. The doctrinal approach was also used, which allowed, on the basis of scientific works and theoretical constructions, explaining the complexity of the modern phenomena and predicting their future development. This said, the main focus is on criminals to prove their antagonism with humanity in accordance with theoretical views. Finally, the study analyzes the theories of universal and traditional jurisdiction and how they are applied to prosecute terrorists.

Results: the paper provides a critical analysis, reviewing and adapting the concept of jurisdiction as applied to a global, borderless and decentralized digital environment (cyberspace) and to the struggle against new forms of terrorism (cyberterrorism). Various jurisdictional models applicable in cyberspace are presented. The author bridges the gap between the main branches of law: international private law and public law by linking, in relation to cyberterrorism, the two theories: the "responsibility to protect" (R2P) theory and the application of universal jurisdiction. The trends of universal jurisdiction development are revealed.

Scientific novelty: the study develops the accumulated scientific knowledge while justifying the introduction of foreign jurisdiction in a state territory to prosecute cyberterrorists. It also establishes a link between the theory of universal jurisdiction in private international law and the "responsibility to protect" (R2P) theory in public international law, recognizing the latter as a relevant basis for the introduction of universal jurisdiction over cyberterrorism. Such traditional concepts as sovereignty and jurisdictional independence are reviewed. The gap related to the consideration of cyberterrorism as a crime against humanity in international law is bridged.

Practical significance: the implementation of the proposed conclusions will contribute to the strengthening of international prosecution of cyberterrorism and harmonize the international and national legal tools to struggle against this crime.

For citation

Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. *Journal of Digital Technologies and Law, 1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

Contents

Introduction

International scholars acknowledge the duties entitled in the "Responsibility to Protect" theory to protect human rights. Also, they admit the global nature of cyber-terrorism destruction. Consequently, this theory is the appropriate reasoning for imposing universal jurisdiction regarding cyber-terrorism. The research introduces the "Responsibility to Protect" (further – R2P) theory as the pillar to impose universal jurisdiction regarding cyber-terrorism. It establishes a link between the two international law theories: Universal Jurisdiction from international private law and the Responsibility to Protect from international public law.

The research contributes to knowledge by providing the international community with the legal justification to impose foreign jurisdictions within a state territory to prosecute cyber-terrorists. It establishes a link between the universal jurisdiction theory in international private law and the responsibility to protect in international public law. Therefore, it bridges a gap between these major branches of international law. Besides, it recontextualizes traditional concepts, e.g., sovereignty and jurisdictional independence, to achieve prior humanitarian aims. Furthermore, it bridges the gap in knowledge by linking cyber-terrorism to the established concept of crimes against humanity in international law; it proves the applicability of the latter elements to cyber-terrorism as an international illegal activity. Thus, the R2P theory could be utilized to impose universal jurisdiction regarding it just as CAH.

The research analyzes the structure of cyber-terrorism and explores its camouflaged elements under cyberspace's ambiguity. The limitlessness of the latter requires developing a tool that transcends the odds of traditional jurisdictions. This tool is universal jurisdiction; it permits states to prosecute terrorists in cyberspace, regardless of their location. Yet, its application faces obstacles, legal and political. Therefore, a theory that includes obligatory concepts would be an effective tool to support it.

The research enhances international prosecution of cyber-terrorism as it justifies utilizing global legal toolkits against it. It proves that cyber-terrorism is a crime against humanity that triggers international intervention under the R2P theory, which it presents as a regulative legal norm. So, it manifests global solidarity to prevent those serious

crimes under the UN Charter rules by harmonizing international and domestic legal toolkits concerning this crime. Consequently, international jurisprudence encircles cyber-terrorism and eliminates its evil in cyberspace.

Regarding the methodology, the research adopts a theoretical approach to achieve its objectives. It is established on a doctrinal method to examine legal sources to analyze the legal prepositions found in primary and secondary legal resources. It includes case laws, domestic legislation, and international instruments. The analysis depends on logical reasoning. This approach analyses the norms that the legal materials included to elaborate the legal understanding of the research question. Besides, argumentized reviews of case laws and primary law resources contribute to extracting the relevant approaches.

The research reviews the relevant scholarships to disclose the gap in knowledge that the research bridges. It discusses the contextualization of the R2P theory, emphasizing its purpose, which is to defend humanity against atrocities. Then, the research explores the concept of cyber-terrorism to extract its theory from academics. Mainly, it focuses on the perpetrator's side of this activity to prove its antagonism to humanity according to the theorists' views. At last, the research refutes the outstanding literature on universal jurisdiction theory and how jurisdictions adopt it to prosecute terrorists.

Besides, it analyzes international and domestic law sources to study how they handled universal jurisdiction as they prosecute cyber-terrorists. Also, it reviews the relevant literature to set out the trending attitudes about universal jurisdiction.

1. The Preventive Nature of the R2P Regarding Crimes Against Humanity (CAH)

International law includes obligations on states to protect humanity against atrocities. These obligations are binding according to their legal roots. The International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICSECR) mention fundamental human rights as the subject of protection. Beforehand, the 1948 Genocide Convention imposed a duty on states to prevent genocide crimes[1]. Also, the UN Charter adopts these duties to defend humanity by securing international peace. Indeed, the evolution of the UN doctrine tended to adopt this responsibility as protection from CAH[2]. It is clear in the 2005 World Summit report that a global theory of international community responsibility should be enacted to achieve the UN aims. These legal instruments include the threshold to trigger the state's obligations. The binding force of these obligations reflects their enforceability in the global legal system and the nations determination to protect humanity. So, the concept of responsibility to protect is rooted in international law.

1 The 1948 Convention on the Prevention and Punishment of the Crime of Genocide, Arts 3, 6 and 8.

2 The UN General Assembly. Resolution Adopted by the General Assembly: 60/1 (UN, 2005), para. 139 and the Resolution A/75/277 (UN 2021), para. 6.

1.1. The Universalization of the R2P to Prevent CAH

This doctrine affirms the R2P as an international legal norm that aims to prevent inhumane atrocities. It was mentioned in the UN Security Council resolutions (UNSC) to justify intervention in preventing CAH[3]. This attitude shifts the R2P from an innovative idea to an acknowledged legal principle in international law. Then, it introduces a systematic legal foundation to intervene in preventing CAH (Cantini & Zavialov, 2018). CAH imply the accountability of the international community to act, regardless of sovereignty considerations. Thus, the R2P implies facilitating the CAH prevention measures undertaken by the international community or a foreign jurisdiction (Cantini & Zavialov, 2018).

Royer claims that states' political will and the traditional understanding of their sovereignty hinder the international community intervention to prevent CAH (Royer, 2021). So, he emphasizes that states should integrate the R2P into the interpretation of their national interests regarding CAH (Royer, 2021). He argues that the R2P does not manifest a valuable reference for state politics that they might oppose its application. This fact implies reconceptualizing the international community's endeavors to combat evil in a political framework. Yet, while the R2P represents a moral norm, doctrine should review it as a preventive procedure to protect humanity (Royer, 2021). This integration supports the R2P in international politics as it eliminates extremist patriotic odds that oppose foreign intervention. Royer's reframing of the R2P underlines the severity of CAH as a common evil that requires global collaboration to suppress it.

Furthermore, Watt argues that the R2P should be constitutionalized in international law under the authority of the UN institutions (Wyatt, 2019). He claims that the R2P is an extension of UN humanity protection since it imposes a collective responsibility on member states to prevent CAH (Wyatt, 2019). In addition, it would overcome the strict Westphalian view of state sovereignty[4], pointing out it from the responsibility aspect. So, a moral relationship is established between it and cosmopolitan human protection. Moreover, he considers the UN organs the effective bodies to enforce the R2P legal order. So, they should surveil the application of the R2P. This constitutional order guarantees the effective integration of the R2P duties into a firm establishment of international commitments. It manifests a global level of the solidarity obligation included in the UN Charter. It provides international diplomacy and doctrine with a harmonized concept of solidarity to maintain peace and security[5]. He seeks, through

3 Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

4 'Supreme authority within a territory', ibid, p. 99.

5 Ibid, p. 156.

his interpretation, to consolidate the R2P in international law and diplomacy. Trying to impose the constitutional nature of the R2P on states requires their clear consent of them as it might contradict their interpretation of sovereignty. Besides, the mentioned harmonization implies unifying the views of states on their responsibilities to prevent CAH from considering the solidarity obligation of the Charter. In practice, politics frustrates the R2P efforts by considering it a Western imperialism that should be patriotically resisted. Despite that the NATO intervention in Libya was approved by the UNSC under the R2P norms[6], it was criticized as it violated state sovereignty and led to political chaos therein. It might be overseen exploitation of international justice for political aims. To overcome this odd, international jurisprudence should contextualize the R2P legally according to each case separately to ensure its impartiality.

CAH by a third party, e.g., terrorists, on a group of local population trigger international responsibility to intervene to prevent them if the host state did not respond (Soler, 2019). External intervention could utilize foreign jurisdictional tools to prosecute these crimes. This responsibility consists of both state and international community duties to prevent severe atrocities which violate fundamental human rights (Park & Switzer, 2020) through the transnationalism of legal procedures[7]. Therefore, the R2P aims are guaranteed by this intervention as its humanitarian aspects overwhelm sovereignty claims. This duty of the international community is sustained by the non-fulfillment of the host state of its responsibility to protect fundamental human rights. Also, CAH must not exploit state sovereignty as a shield to avoid prosecution (Soler, 2019). Moreover, international law permits humanitarian intervention to prevent human rights violations even by use of force, though its rare cases (Azubuike, 2023). A fortiori, judicial intervention is an appropriate solution to defend these rights. These rights are rooted in international law that grants them continuous protection.

Remarkably, the R2P norms could be utilized in cyberspace to suppress terrorist activities by promoting the collaboration of internet giants and national bodies to enforce responsible measures to achieve this aim (Park & Switzer, 2020). This supports the R2P's existence in cyberspace since it presents this theory as a shield against cyber-terrorism.

6 The United Nations Security Council S/RES/1973 (2011), para. 4.

7 Kosiba, K. (2018). Is R2P the Remedy for Illegal Deforestation? A Case Study Based on the Systematic Human Rights Violations in Peru. Master of Arts Dissertation submitted to the Brussels School of International Law. University of Kent. https://clck.ru/36ksvy

1.2. International Jurisprudence Utilization of the R2P

The International Court of Justice establishes the R2P as the collective obligation to maintain international peace and security[8]. So, states must utilize the reasonably available methods to achieve this purpose. The R2P represents, at its core, a due diligence obligation since states are not obliged to succeed in preventing those crimes completely[9]. This jurisprudence proves the flexibility of the R2P in international law that makes it suitable reasoning for applying universal toolkits, i.e., universal jurisdiction, regarding CAH.

Establishing accountability for CAH enhances the ICC agenda to ensure effective human protection (Bellamy, 2018). At this point, the R2P accords with the Rome Statute objectives as it could be employed to provide a legal pillar of the ICC tools. The R2P utilizes non-military preventive measures of the ICC to suppress CAH under Article 7 of the Statute (Holvoet & Mema, 2015). Indeed, the ICC proves efficient to achieve this purpose because of its preventive and permanent characteristics (Holvoet & Mema, 2015). Thus, this integrated establishment of the ICC tools and the R2P constitutes a shield that protects humanity against CAH.

This humanitarian end justifies the utilization of these tools even for non-party states, particularly under the approval of the R2P in the UNSC resolutions. Yet, the R2P, to be effective, should instrumentalize diplomatic and humanitarian mechanisms (Bellamy, 2018). This approach includes employing legal toolkits from foreign jurisdictions. For instance, the ICC imposed its jurisdiction in Kenya and issued an ultimatum to the government about establishing an ad hoc court for post-election violence (Bellamy, 2018). The ICC's legal efforts, in this case, represented the R2P theory as it tended to protect the local population against violence. Bellamy concludes that both the R2P and the ICC system are integrated humanitarian establishments to prevent CAH. Despite the skeptics, the implementation of non-military measures under the R2P introduces them as alternatives to military operations (Fehl, 2015). They are intermediate stages before waging wars. Thus, their prominence in the R2P theory is unneglectable, which endorses the judicial intervention measures to prevent international crimes.

Notwithstanding the ICC and the R2P's mutual role in preventing CAH, utilizing the court's universal toolkits should be subordinate to the Statute's aims (Holvoet & Mema, 2015). This restriction guarantees the effectiveness and trueness of the ICC measures regarding CAH since it creates judicial surveillance on ICC practices. This mechanism, consequently, enhances the trustworthiness of the ICC's role against CAH and limits the

[8] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

[9] Ibid.

perpetrators' impunity. As Ercan elaborates, the R2P toolkit defends international justice and security because it endorses international intervention to guarantee global compliance with international law (Ercan, 2022).

To sum up, scholarships and jurisprudence agree on establishing the R2P on the need to maintain peace and security. In this view, it introduces a legal norm that justifies jurisdictional intervention concerning serious CAH. Thus, it is an appropriate justification to employ foreign legal rules, particularly universal jurisdiction, within the state of crime location. Hence, it overcomes sovereignty claims that might hinder defending human security and encourage the international community to fulfill their duties to protect humanity.

2. The Legal Foundations to Profile Cyber-Terrorism as "Other Inhumane Acts" under the Rome Statute

It is non-debatable that cyberspace establishes international connections between separated nations. Because of its technical nature, terrorists exploit its advantageous facilities to achieve their aims. It enables them to avoid prosecution measures of national law enforcement authorities. Therefore, they operate globally, threatening world peace. Cyber-terrorism is an established inhumane activity that imposes international legal efforts to frustrate it.

Maintaining international peace and security is a leading purpose of international legal bodies, i.e., the International Criminal Court. It is the competent authority to prosecute global perpetrators because of its international legal capabilities. Yet, the Rome Statute, which organizes it, mentions the acts of the court's jurisdiction exclusively. It does not mention cyber-terrorism among them. Though, it notes that the court jurisdiction extends to non-mentioned inhumane acts under certain conditions[10].

Therefore, the article introduces the legal pillars to consider cyber-terrorism a crime against humanity under the Rome Statute of the ICC. The deal of evil of this activity suffices to profile it with this classification, which drops if under the ICC jurisdiction. The article analyzes cyber-terrorism and reviews the literature on it to extract its core elements. Then, it reconceptualizes international law doctrine on crimes against humanity to prove the applicability of this concept to cyber-terrorism. This objective contributes to knowledge by providing the legal basis to extend the ICC's jurisdiction to prosecute cyber-terrorists. This global criminal activity requires a global legal mechanism to hinder it. Consequently, the international community cuts off cyber-terrorism, enhancing world peace and security.

[10] The Rome Statute of the International Criminal Court (2002), Article 7 (1) (k), A/CONF.183/9.

2.1. An Analysis of Cyber-terrorism

In the era of information, terrorism has penetrated cyberspace, shaping a modern threat to humanity. Cyber-terrorism is the utilization of the Internet to target a group with terror for political or radical aims (Broeders et al., 2021). It is a distinctive sort of terrorism that should be analyzed from a broad aspect. Cyber-terrorism exploits the uncontrolled outreach of the internet that strengthens the ties between nations. The French national defense glossary adopts the "risk of terrorism" factor concerning illegal cyber activities (Delerue et al., 2019) to characterize cyber-terrorism. Thus, terrorist groups can act transnationally, transcending geographic proximity (Albahar, 2019). This feature drives scholars to study cyber-terrorism from an international aspect. Accordingly, Alexandra Perloff-Giles profiles cyber-terrorists as "an enemy to mankind" (Perloff-Giles, 2018). She justifies that by the common features between cyber-terrorism and piracy crimes since they both threaten international trade interests. She emphasizes that these attacks jeopardize critical cyber services for a considerable while, which points out the severity of this activity. In addition, she argues that transnational cyber offenses have three concretes:

– the intentional act that harms innocents, as it should be a deliberate attack on national infrastructure or governmental, or private, computer systems. This applies to both governmental and non-state actors. The latter include cyber-terrorists.

– it must occur in cyberspace, exploiting its ambiguity to gain anonymity and advantageous low-cost attacks,

– and it is transnational modus operandi because the perpetrators operate beyond national borders. Perloff-Giles indicates that the malware codes they send need no passport to cross borders. Also, the impacts of their offenses affect several jurisdictions (Perloff-Giles, 2018).

Moreover, Perloff-Giles claims that cyberattacks, regardless of the perpetrators, constitute an illegal use of force, triggering the right to self-defense under Article 51 of the UN Charter. This leads to the application of international humanitarian law, which is a suitable legal set to organize the consequences of cyber conflicts. Yet, she determines the following provisions to apply it:

– the severity and scale of the attacks. Though, she requires a threshold to qualify them for the description "an armed attack",

– and identifying the perpetrators to establish their responsibility. Still, she admits the difficulty to determine this attribution regarding cyber offenses (Perloff-Giles, 2018).

Therefore, Perloff-Giles points out the prominence of cyber offenses as a unique pattern of aggression by terrorists. This activity elevates to application of International Humanitarian Law (IHL) the same as conventional armed conflicts. Thus, this applicability denotes that cyber-terrorism is a severe threat to humanity that requires the utilization of international doctrine efforts to crystallize its dimensions and propose the appropriate legal sets to combat it.

Likewise, in her book "Defining International Terrorism", Stella Margariti claims that terrorism threatens the universal interests of the international community by degrading fundamental human rights concerning international security and peace (Margariti, 2017). She sheds light on the international pillar of terrorism as she claims that its impacts transcend national borders to the international community (Margariti, 2017). Then, since cyberspace exceeds states' geographic borders, the international theme overwhelms its nature. This theme implies the surpassing of criminal acts in cyberspace beyond domestic limits. Consequently, cyber-terrorism generates inevitable impacts on international security.

Because of its limitlessness, terrorist groups utilize cyberspace to achieve their purposes. It is recorded that militants like ISIS exploit social media websites to spread their terror by broadcasting their video content. Besides, they use these websites as recruitment platforms. Thus, they can operate globally beyond geographic borders (Awan, 2017). This utility grants terrorists an advantage over law enforcement and security measures. Also, it emphasizes the need to study cyber-terrorism as an independent criminal activity that combines terror and technology.

Notably, Victoria Correia defines cyber-terrorism as a "cyber-enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to threaten or facilitate damage against the public, properties, and/or systems. Cyber-terrorism has the potential to coincide with traditional terrorism" (Correia, 2022). She introduces a dynamic concept of cyber-terrorism to suit its rapid changes. Also, she requires a particular mens rea, which refers to the radical motivations behind the conduct. The definition clarifies that physical impacts are not the sole requirement of cyber-terrorism; it mentions systems damage that has no physical shape. Thus, she intends, through this definition, to facilitate international legal collaboration to prosecute and counter cyber-terrorism. She, also, points out the impacts of cyber-terrorism on inner society, arguing scholars to study this activity from a collaborative approach to suit the terrorists' illicit use of technology (Correia, 2022).

Conversely, non-violent methods do not reflect cyber-terrorism as it is established that it should result in physical damage regardless of its purposes. As Henschke indicates, the terrorists' mere use of the internet to recruit members or spread their radicalism constitutes a broadcasting activity to deliver their threats to the targeted community (Henschke, 2021). The absence of physical damage deprives these activities of being profiled as cyber-terrorism. Remarkably, Henschke admits that cyberattacks on IoT[11] actuators

[11] The Internet of Things, which means controlling physical equipment by artificial intelligence codes.

impose effects on the victims physically (Henschke, 2021). So, it constitutes cyber-terrorism as it penetrates the connection established by the IoT between the informational internet and physical life. Besides, he argues that the Tallinn Manual prerequisites that the cyberattack impact in the physical world should be perceptible to the present use of force (Schmitt, 2013). The Manual indicates that non-destructive cyber activities are not a use of force, regardless of their moral consequences (Schmitt, 2013).

Dennis Broeders determines that a cyberattack that caused physical damage is not recorded yet (Broeders et al., 2021). He claims that terrorists do not own the required technical and financial skills to accomplish cyberattacks. Besides, the UK legislation requires violence to consider an act as "terrorist"[12] which excludes non-violent acts of this description. In this regard, Stoddart emphasizes that cyber-terrorism threatens national infrastructure in the US since it might include state-supported activities. Also, it might constitute espionage activities which shed light on its gravity though it might not include a violent manner (Stoddart, 2022).

These views reflect a prima facie analysis of cyber-terrorism since they neglect the fact that the moral impacts of this activity exceed their physical counterparts. The national demoralization that cyber-terrorism causes generates hazardous economic and social results that consider it a mala in se activity. Furthermore, cyber-terrorism generates anger among the targeted community that it drives them to demand retaliation by use of force (Shandler et al., 2021) and to respond politically similar to conventional terrorism (Shandler et al., 2021). Also, both sorts of terrorism are motivated by the same psychological incentives.

Ad idem, the Crown Prosecution Service (the UK) stipulates the terror motivation of conduct to consider it "terrorist"[13]. Likewise, the Egyptian Combating Terrorism law decides that the mere mental terrorizing of innocents constitutes a terrorist act, regardless of its physical damage[14]. It decides that the intention of terrorizing civilians to realize the perpetrators' objectives suffices to criminalize their acts under this law. Therefore, national legislations prioritize security concerns by disregarding the condition of physical impacts that Henschke requires (Henschke, 2021). In addition, the Common Position 2001/931/CFSP considers attacks on national infrastructure or governmental facilities terrorist acts, subjecting the perpetrators to counter-terrorism measures[15]. Also, the Austrian Cyber Security Strategy requires the intention to terrorize civilians to inflict damages to national

12 The Terrorism Act 2006, c.11. 2006. https://clck.ru/34Chci

13 Crown Prosecution Service (2021), Terrorism. https://clck.ru/36kt3Z

14 Law No 94/2015, Art 2 para 1.

15 Article 1(3) of Common Position 2001/931/CFSP, see The EU list of persons, groups and entities subject to specific measures to combat terrorism, Factsheet on 14 January 2015. https://clck.ru/36kt4j

infrastructure or economic services to profile an act as a terrorist[16]. Hence, domestic legislations concentrate on the psychological aspect of terrorism since they stipulate the intention to intimidate innocents into this category of criminal acts; it is the distinctive theme of cyber-terrorism that might not cause physical damage and the determinant factor of this category.

Similarly, Margariti argues that the intention to spread terror qualifies an act as a terrorist, regardless of its motives (Margariti, 2017). This element distinguishes terrorism from ordinary crimes. It is a specific mens rea that represents the threshold of this classification. She adopts this standard as a cosmopolitan determinant of the actus reus of international terrorism, which is required to impose a universal legal framework upon it (Margariti, 2017).

So, the non-requirement of the physical impacts to consider an act a terrorist enhances an inclusive theme of cyber-terrorism studies, which aligns with Correia's definition discussed above (Correia, 2022). Although its mere moral consequences, cyber-terrorism threatens world peace and security as it might ignite an armed dispute. Unlike conventional terrorism, individuals can resort to no shelters against cyber-terrorism; the codes that cyber-terrorists employ to jeopardize computing systems within the targeted community penetrate numerous layers of protection. Therefore, this cyber insecurity destabilizes international peace and security. Cyber-terrorism can be elevated to be an enemy to mankind as Perloff-Giles describes (Perloff-Giles, 2018).

2.2. The Contextual Elements of Crimes Against Humanity: Other Inhumane Acts

The Rome Statute includes the term "other inhumane acts" in Article 7(1) (k) to establish the ICC's jurisdiction on these severe acts. This term passed through historical processing by both doctrine and jurisprudence. Yet, the objective of this paper implies focusing on reviewing other inhumane acts elements to construct the comparison required to prove their applicability to cyber-terrorism, as an international illegal activity. Since this term was drafted within international law, it is a must to review its elements from the perspectives of international doctrine and jurisprudence.

Initially, Article 7(1) (k) of the Statute establishes that the classification "other inhumane acts" is a part and parcel of CAH it prohibits (Broeders et al., 2021). This article constructs this act on these pillars: inhumane acts, the intention to cause suffering, mental or physical. They are built on the essential elements of CAH. Still, they show an inclusive approach to prevent disability to prosecute innovative non-included acts.

[16] Federal Chancellery, 'Austria Cyber Security Strategy', 2013, 21. https://clck.ru/36kt6E

Accordingly, Rustam Atadjanov argues that the systematic nature of crimes against humanity distinguishes them from ordinary local criminal behavior (Atadjanov, 2019). So, being an organized behavior reflects the element of context required to profile an act as a crime against humanity. Besides, this systematic nature drives Hobbs argues to argue that CAH express "extraordinary evil" (Hobbs, 2017). Thus, this element represents their severity on humanity's legal interests and their large scale. Nevertheless, Seada Hussein Adem claims that the CAH term suffers a normative gap in the international doctrine that the Statute seeks to bridge by counting the elements that qualify an act as CAH (Adem, 2019). She concludes that the evolution of CAH jurisprudence, as well, bridges this gap since the ad hoc tribunals and the ICC developed an inclusive approach that settled the dilemma (Adem, 2019).

The International Law Commission (ILC) requires the systematic approach of deeds and their widespread to be considered CAH[17]. Besides, it argues that they could be committed by non-state actors[18]. Therefore, the ILC permits classifying the acts committed by groups, or organizations, as CAH, according to the provisions of the Rome Statute. CAH are not perpetrated by states exclusively but by independent bodies or individuals as well. Besides, the ILC requires the multiplicity of victims as a major element of this crime. This condition enhances the widespread requirement and deprives individuals of limited acts of this classification.

Concerning jurisprudence, the term "inhumane acts" reflects the continued evolution of crimes against humanity classification, which was used in 18 cases before the ICC as an alternative response to the legal vacuum (MacNeil, 2021). In Prosecutor v Jean-Pierre Bemba Gombo[19] argues that crimes against humanity have four pillars: a targeted civilian community, scope of the attack, the acts included, mens rea[20]. Besides, the ICC considers inhumane acts that cause mental damages crimes against humanity[21]. In Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui[22] the judges decide that severe violations of fundamental human rights, as established in the international human rights law, are inhumane acts under Art 7(1) (k) of the Statute[23]. John Quigley concludes that this ICC

17 The International Law Commission, Draft Code of Crimes against the Peace and Security of Mankind, 1996 UN Doc. A/51/10 article 18 (k), p 47. https://clck.ru/36kt7d

18 Ibid.

19 Case No. ICC-01/05-01/08.

20 Ibid para 117 and (Park & Switzer, 2020).

21 Ibid, see 'The Elements of Crimes' Published by the International Criminal Court (2013), ISBN 92-9227-232-2, ICC-PIOS-LT-03-002/15_Eng. https://clck.ru/36ktC8

22 ICC-01/04-01/07.

23 Ibid, para 448. The ICC adopts the same principle in Request for authorization of an investigation pursuant to article 15 regarding the situation in the People's Republic of Bangladesh and the Republic of the Union of Myanmar, ICC-01/19, para 128.

Chamber affirms that the contextual elements of other inhumane acts are: intentional great suffering or mental or physical injury (Quigley, 2023). It is an independent category of criminalization that does not require a connection to other included crimes (Quigley, 2023).

Moreover, the International Criminal Tribunal for the former Yugoslavia (ICTY) decides that acts that injure human dignity are "inhumane acts" under the Statute[24]. Thus, the Tribunal extends the interpretation of that term to exceed the Statute, covering novel criminal acts. The Tribunal opinio juris is a result of a doctrine vacuum regarding a disciplined definition of "inhumane acts". Besides, the ICTY stipulates these elements for an act to constitute an inhumane act:

– serious behavior,

– the harm, which may be mental or physical or injury to human dignity,

– and the mens rea[25].

It, also, concludes, in Prosecutor v Milorad Krnojelac[26], that inhumane acts compromise deliberate deeds that inflict severe mental or physical damage to innocents[27]. This jus cogens qualifies perpetrators' acts to be crimes against humanity because of the severity of their impacts. The European Court of Human Rights (ECHR), in Liu v Poland[28] and M.T. and Others v. Sweden[29], utilize the term inhumane to describe acts that degrade a person's dignity and violate his fundamental rights.

Thus, international jurisprudence establishes that these acts are CAH, precisely under the "other inhumane acts" category. It adopts this term as a residual clause to broaden its jurisdiction concerning the prosecution of crimes against humanity to provide effective protection to humanity. Hence, it expresses a flexible jurisprudence to utilize the included legal terminology to contextualize the non-included atrocities under the Rome Statute.

2.3. The applicability of "Other Inhumane Acts" to Cyber-terrorism

The literature on the contextual elements of the term "other inhumane acts" underlines their severity; it comes from their damage to the mental and physical well-being of innocents. The analysis of these elements reflects the unordinary evil of these acts. Thus, other acts that reflect the same evil should be classified as other inhumane acts if the contextual

---

24 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522.

25 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

26 IT-97-25-T.

27 Ibid, footnote 382.

28 Application no. 37610/18, on 6 October 2022.

29 Application no. 22105/18, on 20 October 2022.

elements apply. Put differently, the determinant factor of this classification to an act is the applicability of these elements to it.

Initially, cyber-terrorism violates the core principles of IHL (Werle & Jeßberger, 2014). It, first, threatens the minimum standards of humanity by spreading terror. Then, the civilian damages it causes transcend the proportionality standards, predominantly the terrorists' animus nocendi is non-discriminatory. Cyber-terrorists prioritize accomplishing their objectives regardless of innocent civilian sufferings. This nondiscriminatory theme of cyber-terrorism accords with the Rome Statute demonstration of crimes against humanity[30]. The Statute requires that an act should be collected against civilians to constitute a crime against humanity. International jurisprudence admits that the damage of these crimes is both physical and mental. It claims that the mere disregarding of human dignity considerable damage to establishing an accusation[31].

Furthermore, Stella Margariti victimizes the international community regarding cyber-terrorism since it targets international peace and security (Margariti, 2017). Besides, the systematic nature of crimes against humanity that Hobbs points out is shared between cyber-terrorism and crimes against humanity (Hobbs, 2017). Besides, they both have transnational impacts that ground for international involvement. They both constitute a threat to humanity which implies categorizing them in the same classification. Also, as Atadjanov indicates, the element of systematic nature applies to cyber-terrorism since it threatens international peace and security and constitutes a widespread nondiscriminatory organized attack on civilians (Atadjanov, 2019). Indeed, cyber-terrorism generates critical suffering for the international community because the perpetrators intend to jeopardize fundamental human rights. Their systematic manners disrupt the "peaceful cohabitation" (Atadjanov, 2019) of the targeted communities because they negatively affect the concretes of humanity, protected under the UDHR 1948[32]. Furthermore, the systematic nature of CAH, as a contextual element, applies to cyber-terrorism since it threatens international peace and security and constitutes a widespread nondiscriminatory organized attack on civilians.

This opinio juris supports the discussed claim that cyber-terrorism that causes nonphysical damages is a crime against humanity. This conduct targets civilians without discrimination and the perpetrators deliberately ignore civilian casualties to accomplish their objectives. Furthermore, the International Law Commission, in its draft of a convention on the prevention and punishment of crimes against humanity, considers mental harm

30 The Rome Statute, Art 7.

31 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

32 The Universal Declaration of Human Rights, the United Nations, GA-Res 217/1948. https://clck.ru/36ktDK

adequate to profile an act as a crime against humanity[33]. So, in international law doctrine, physical damage is not a core requirement of crimes against humanity. Similarly, international jurisprudence establishes that mental suffering suffices to qualify perpetrators' acts to be crimes against humanity under Art 7 (1) (k) of the Statute. This approach underlines the gravity of mental damage that cyber-terrorism inflicts.

Nonetheless, Maguir does not require the nondiscriminatory clause to describe an act as a crime against humanity (Maguir, 2022). He argues that they must be systematic against civilian groups with the aware deliberate mens rea of the perpetrators. Likewise, the Appeals Chamber of the UN Special Tribunal of Lebanon pointed out this mens rea should be the intent to spread terror through means that danger civilians[34]. It, also, mentioned that customary international law does not limit terrorism to certain means. Thus, it is admitted that terrorists can utilize cyber tools to achieve their aims. The determinant factor is the public terror intent, regardless of the criminal conduct's shape.

Moreover, Tsilonis addresses that the concept of "organizational policy", that Art 7 (2)(a) of the Rome Statute includes, expands to non-state actors, e.g., terrorists (Tsilonis, 2019). The terror activity might not be state backed but the ICC can prosecute the perpetrators. The purpose of this provision is to enhance humanity's protection against severe crimes. The legal aims of Art 7 implement transcending the literal interpretation of the mentioned term to entail terrorist conduct.

The pillars of inhumane acts coincide with the definition of cyber-terrorism that Correia proposes (Correia, 2022). Both international jurisprudence and doctrine argue that intentional grave acts that target innocent civilians, causing damage to their fundamental rights, regardless of their shape, are inhumane acts under Art 7 of the Rome Statute. Obviously, the examination of these pillars proves their applicability in the context of cyber-terrorism. By targeting national infrastructure, cyber-terrorists affect civilians. Besides, the widespread attack is required to achieve the perpetrators' aims of terrorizing societies, which is the distinctive theme of their activity. Then, the conduct of cyber-terrorists against civilians, regardless of its sort. Finally, the perpetrators should intend to terrorize innocents to achieve their goals. Perloff-Giles's analysis of cyber offenses elements (Perloff-Giles, 2018) accords with the jus cogens that international courts establish, particularly the ECHR illustration of inhumane acts as violations of human rights. Indeed, cyber-terrorism manifests human dignity degrading deeds under this illustration.

---

33 The International Law Commission, "Report of the International Law Commission", Seventy-first session (29 April–7 June and 8 July–9 August 2019) A/74/10, p12. https://clck.ru/36ktFT

34 The UN Special Tribunal of Lebanon Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, 16 February 2011, Case No. STL-11-01/1 (STL Decision).

To conclude, scholars and jurists enhance the doctrine of counting cyber-terrorism as a crime against humanity under the Rome Statute. They target victims systematically and generate serious unlimited impacts. Their transnational consequences provide grounds for international concern. Regardless of its method, the state of terror the perpetrators tend to impose suffices to consider cyber-terrorism a crime against humanity. Also, the extension of the ICC's jurisdiction to prosecute cyber-terrorists profiles their conduct as crimes against humanity. The inhumane acts category entailed in Art 7 (1) (k) of the Rome Statute can include cyber-terrorism. This conclusion implies utilizing universal legal mechanisms under the jurisdiction of the ICC to prosecute cyber-terrorists. Consequently, ruthless cyber-terrorists are subject to the ICC jurisdiction as in the case of other crimes against humanity perpetrators.

3. Universal Jurisdiction in Prosecuting CAH

The evolution of international judicial cooperation innovated the universal principle of jurisdiction. It means the ability to prosecute and try criminals regardless of their location or nationality. It seeks to achieve international justice that requires transcending the traditional jurisdiction determinants to cut-off severe acts of crime. Jovana Blesic constrains the application of universal jurisdiction to international crimes as they impose an erga omnes obligation to prosecute the perpetrators (Blešić, 2022).

Universal jurisdiction presents a significant progression of international criminal justice since it enables states and the concerned bodies to prosecute international criminals globally, regardless of their nationality (Mung'omba, 2022). Thus, universal jurisdiction restricts their impunity which enhances international criminal justice. It constitutes a right of the international community to intervene wherever CAH are committed to prosecuting the perpetrators (Mung'omba, 2022). Notably, Mung'omba mentions that universal jurisdiction does not require a direct link between the prosecuting judicial body and the crime (Mung'omba, 2022). Universal jurisdiction, in his view, "stands out" of the basic jurisdictional norms, which suits its mission in enforcing international criminal justice (Mung'omba, 2022)[35]. It is based on the need to enforce justice and deterrents regarding CAH (Mung'omba, 2022). Thus, universal jurisdiction is crystalized in international law as a unique set of CAH prosecution and trying. On the UN level, states delegations at the 73rd Legal Session decided that universal

[35] See (Mung'omba, 2022). He, however, decides that the perpetrator should be present in persona before the court under the Princeton Principles, ibid 96, see also Global Policy Forum. (2021, June 2). Princeton Principles on Universal Jurisdiction: Princeton Project on Universal Jurisdiction. https://clck.ru/36ktLY

jurisdiction represents an effective toolkit to prosecute core crimes. Among them, they enlisted CAH[36].

Kittichaisaree argues that states impose national jurisdiction on both a subjective and objective basis (Kittichaisaree, 2017). International jurisprudence limits national jurisdiction to traditional factors[37], especially as there is no convention adopting universal jurisdiction. Furthermore, domestic courts should impose their "presumptive jurisdiction" regarding crimes against humanity. Maguir claims that the victims' interests justify the priority of the national prosecution of those crimes (Maguir, 2022). However, Soler criticizes this jurisdiction because it would reflect a power abuse of certain states that deprives a defendant of their right to a fair trial (Soler, 2019). Hence, practicing universal jurisdiction regarding CAH should be equitable and proportionate to guarantee effective justice (Soler, 2019). These conditions maintain the balance between confronting CAH and respecting national sovereignty. Also, he calls for drafting a unified international understanding of aut dedare aut judicare refusal reasons to restrict the impunity of CAH perpetrators, which is considered the major reason for core crimes continuation (Maguir, 2022). This appropriate application of universal jurisdiction, therefore, enhances international criminal justice since it stretches jurisdictional tools to prosecute and extradite CAH perpetrators. Moreover, it supports states to fulfill their obligations concerning prosecuting core crimes, which protects victims' human rights and enhances the traditional understanding of the rule of law (Maguir, 2022). Remarkably, he advocates the right of a third state to prosecute CAH perpetrators as he argues that universal jurisdiction fills up the vacuum caused by the absence of territorial jurisdiction and nationality jurisdiction (Maguir, 2022). Universal jurisdiction, hence, falls under state obligations to prosecute core crimes (Maguir, 2022).

Notwithstanding that universal jurisdiction limits the perpetrators' impunity, it was considered, in certain cases, aggression on national sovereignty and stability[38]. The African Union refused a Spanish arrest warrant against Lieutenant-General Emmanuel Karenzi Karake, considering it a violation of international law and an abuse of the principle of universal jurisdiction. It, also, condemned the European judicial attempts to subordinate the African judiciaries via the

[36] The 6th Committee of the UN General Assembly - Legal (73rd Session), 'The scope and application of the principle of universal jurisdiction (Agenda item 87)', see resolution 72/120. https://clck.ru/36ktQV

[37] See the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

[38] African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

misuse of universal jurisdiction[39]. This statement reflects the controversial theme of universal jurisdiction. Although it is a mechanism to prosecute core crimes, ending their impunity, its application suffers shortages. Nyawo justifies this fact by the absence of an international treaty or instrument that defines universal jurisdiction and explains its applications (Nyawo, 2023). He argues that universal jurisdiction is indispensable to confront CAH since all states have major interests in this (Nyawo, 2023). Furthermore, he justifies universal jurisdiction by the moral global duty that the natural theory includes (Nyawo, 2023, p. 225). This duty obliges the international community to cooperate against the evil deeds that threaten world peace and security. The UNSC mentioned the obligation to prosecute universal crimes and punish the perpetrators universally[40]. This resolution reflects the international interpretation of CAH severity that endorses a universal scheme to prosecute the perpetrators.

Human Rights Watch representative Lotte Leicht argues that the UN developed a mechanism to prosecute CAH perpetrators. It includes a standing prosecutor who initiates the investigations of CAH without establishing an ad hoc court. His jurisdiction extends universally to overcome judicial or political odds[41].

3.1. Aut Dedere Aut Judicare Cyber-terrorism

International jurisprudence affirms that terrorism accusations imply the application of universal jurisdiction due to their severity (Soler, 2019). Since aut dedare aut judicare composes a general principle in international law, the international community should utilize it to confront cyber-terrorism. Its qualitative severity, the deficiency of international human rights protection, and the threat to world peace that cyber-terrorists' impunity support the application of universal jurisdiction by both international and domestic courts to prosecute and extradite them. Then, the international deterrent is guaranteed regarding cyber-terrorism.

According to her profiling of cyber offenders as an enemy to mankind (Perloff-Giles, 2018), Perloff-Giles supports imposing universal jurisdiction to prosecute and extradite cyber-terrorists. Besides, she argues that states can prosecute pirates

39 Ibid para 6.

40 UNSC/S/RES/138, 23 June 1960, para 4. https://clck.ru/36ktdL

41 The European Parliament. (2018, June 28). Workshop: Universal jurisdiction and international crimes: Constraints and best practices. Brussels, EP/EXPO/B/COMMITTEE/FWC/2013-08/Lot8/21.

wherever they are active on the "high seas" under the UNCLOS[42]. Then, she stretches the "high seas" term to include cyberspace as she considers it a transnational sphere of interactions (Perloff-Giles, 2018). She establishes her view on a US court judgment deciding that being on the "high seas" is not a condition to apply universal jurisdiction against piracy[43]. Her comparison shows that both piracy and cybercrime endanger international commerce as cyberattacks can disrupt commercial and financial services websites. So, universal jurisdiction is an effective approach to suppress transnational cybercrimes.

Kittichaisaree claims that technical issues complicate universal jurisdiction support, such as cloud computing as in cyberspace, several states may claim their extraterritorial jurisdiction over cloud-based activities (Kittichaisaree, 2017). As he reviews international legal instruments, he mentions that the permission to extraterritorially prosecute an "unauthorized broadcast" from a vessel located on high seas[44] extends to cyber-facilitated broadcast (Kittichaisaree, 2017). So, he applies the broadcasting term to internet broadcasting websites like Facebook[45] and Twitter[46]. These online platforms are used by terrorists to broadcast their ideologies and recruit their personnel, which provides a reason for states to impose their jurisdictions. Besides, the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, establish universal jurisdiction regarding criminal acts, which applies to cyber-terrorism, if they target the personnel included in Article 1[47]. It demands the Party States utilize their legal tools to suppress these activities, achieving the Convention's aims. Due to the accelerated development in internet access meanings, cyberterrorism is cheap if compared to its impacts (Kittichaisaree, 2017). Thus, the Budapest Convention on Cybercrime should be universalized to establish a global network, facilitating the prosecution of cyber-terrorists.

As Maguir argues, prosecuting cyber-terrorism by a national court proves efficient as it is motivated by the victims' trust in their courts[48]. Besides, the presumptive jurisdiction reflects, at its core, imposing universal jurisdiction over these crimes; it

---

42 Article 101 c of the United Nations Convention on the Law of the Sea, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).

43 United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013).

44 Art 109, the UNCLOS.

45 The organization is recognized as extremist, its activity is prohibited in the territory of the Russian Federation.

46 A social network blocked in the territory of the Russian Federation for disseminating illegal information.

47 Art 3 of the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, entered into force on 20 February 1977.

48 See the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

prevents the victims from jurisdictional vulnerabilities related to cyber-terrorism prosecution (Kittichaisaree, 2017). Hence, this attitude complies with the extraterritorial punishment of cyber perpetrators, regardless of their location or nationality. Nonetheless, the transnational impacts of cyber-terrorism may involve several jurisdictions that lead to their conflict. So, the complementarity principle of the ICC retains its significance to cure state authorities' deficiency in cyber-terrorism prosecution. Yet, this system of fallback complementarity expresses the vertical order between the ICC and its Members to prosecute core crimes (Burens, 2016). So, Laura Burens argues that a horizontal inter-state mechanism of complementarity enhances universal jurisdiction to prosecute these crimes under the Statute. Besides, she introduces the state where the perpetrator is located as the obliged member to utilize universal jurisdiction in the prosecution process (Burens, 2016). This integration of vertical and horizontal complementarity eliminates the odds before universal jurisdiction due to the transparency of the subsidiarity principle (Burens, 2016, p. 89)[49]. Also, Resolution 72/120 mentions that the utilization of universal jurisdiction should fall under international law and the subsidiarity principle to prevent its abuse or inefficiency[50]. Soler, for his part, claims that this integration is required for the adequate application of universal jurisdiction to overcome the deficiency of the subsidiarity principle (Soler, 2019).

Regarding national laws, the UK Legislation extends its jurisdiction over terrorism crimes, regardless of their actus reus, according to the purposes entitled in article 63B[51]. This extraterritorial jurisdiction enhances protection against cyber-terrorism; the Crown Prosecution Service can utilize its legal tools to prosecute the perpetrators extraterritorially[52] if their mens rea was included in the mentioned article. Furthermore, the UK judiciary in R v. Kumar Lama[53], outlined that a domestic court should utilize universal jurisdiction to prosecute grave crimes. Though, Hovell criticizes this trial because of shortages of abroad evidence gathering that led the court to consider Colonel Lama not guilty[54]. Likewise, Combating Information Technology

49 L. Burens claims that this principle maintains the balance between states sovereignty and the international interest to prosecute core crimes.

50 Resolution 72/120, Supra 17.

51 Terrorism Act 2000, the UK, 63A- 63D.

52 The Crown Prosecution Service (2021), 'Jurisdiction', (CPS: Legal Guidance on 26 July 2021). https://clck.ru/36ktjD

53 Case no. 2013/05698 (Central Criminal Court, London, 2016).

54 Hovell, D. (2017, April 6). The 'Mistrial' of Kumar Lama: Problematizing Universal Jurisdiction. EJIL Talk – Blog of the European Journal of International Law. https://clck.ru/36ktkR

Crimes Law[55] extended the Egyptian jurisdiction largely over cybercrimes to include offenses committed by non-nationals provided that[56]:

– the crime was committed on board any naval or aerial or land transportation registered in Egypt or raising its flag;

– the victim is Egyptian;

– the crime was planned or surveilled or funded in Egypt;

– the criminal is an organized group working in several countries among them Egypt;

– the crime might harm any of Egypt's interests or security or any citizen's or residents' interests or security;

– the criminal was found in Egypt after committing the crime and was not yet extradited.

This broad approach by the Egyptian Legislator is a result of the legal vacuum that the Egyptian judges suffered regarding cyber-terrorism. Indeed, it manifests a comprehensive view of the application of universal jurisdiction in cyberspace to enhance the legal protection against cyber-terrorism.

To conclude, the transnational nature of cyber-terrorism, along with its severity on international peace and security, pushes the international community to adopt universal jurisdiction to prosecute and punish the perpetrators. It is a suitable mechanism to confront them because it aligns with the obligations of the state to prosecute core crimes, as recognized in international customary law. Indeed, the ongoing impunity of cyber-terrorists leads to an increase in their crimes. So, the international community should unify its legal efforts to develop a unified global understanding of universal jurisdiction to avoid the legal vacuum.

4. Bridging the Gap

It is recognized that cyber-terrorism is a major sort of illegal activity in cyberspace due to the capabilities provided by the latter; its ambiguous nature, which extends through the real world, allows them to roam and work effectively for their objectives. This manner crystallizes the international theme of cyber-terrorism which requires the utilization of international legal mechanisms to confront. However, the international character of these tools might introduce them as intervention schemes in the internal affairs of independent states. Put simply, states might oppose them justifying that on a sovereignty basis. This fact creates a dilemma concerning prosecuting and trying cyber-terrorists and, also, enhances their impunity in the actual international legal practice. Thus, world peace and security become more fragile against their threats. So, these international mechanisms require

[55] Law No 175/2018.

[56] Ibid pt 1 Art 3.

a firm legal basis to overcome states' opposition and persuade them to cooperate against cyber-terrorism as an international danger.

4.1. Explaining the Dilemma

The application of international legal norms, regardless of their stability, is yet to be palatable. Interests of states and their interpretation of international law concepts complicate creating a unified manner of the application of international jus cogens. Regarding the research question, international legal practice discloses that both international law norms, the R2P and universal jurisdiction, are continuously refuted. Skeptics are either jurists or diplomatic statements. They reflect the absence of a unified international understanding of these theories. Thus, trying to establish universal jurisdiction on the R2P theory is unfruitful unless the research contains its critiques and contextualizes them within its trajectory.

International legal practice reveals that the application of universal jurisdiction to confront cyber-terrorism is yet to be palatable. States, and even international organizations, might oppose it and frustrate foreign legal measures adopting universal jurisdiction as a basis. This opposition appears apparently in the statement of the African Union when the organization claimed that universal jurisdiction violated the stability of the whole continent[57]. Although the judicial measures were taken by a European court to prosecute CAH in Rwanda, they were reviewed in a merely political context relevant to the European colonization of Africa memories. Such attitudes enhance the perpetrators' impunity and hinder the enforcement of justice.

Furthermore, at the 12th Meeting of the Sixth Committee of the UN General Assembly, the representatives' discussions reveal a considerable gap regarding universal jurisdiction. While Germany presented the judicial experience of a domestic court in prosecuting CAH committed by Syrian officials[58], Columbia stipulated that the application of universal jurisdiction should be under a bilateral or international treaty[59]. The majority of the representatives pointed out that the effectiveness of universal jurisdiction requires its incorporation within national legal systems[60]. This report crystalizes the diversion of states' attitudes towards universal jurisdiction that deepens the gap in its conceptualization and application. Besides, states might oppose universal jurisdiction since they might neither permit a foreign jurisdiction to prosecute a cyber-terrorist within their territory nor extradite a national terrorist to a foreign

57 African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

58 Speakers Disagree on How, When, Where Universal Jurisdiction Should Be Engaged, as Sixth Committee Takes up Report on Principle. (2022, October 12). UN Press. https://clck.ru/36ktp8

59 Ibid para 7.

60 Ibid paras 3, 4, 5 & 8.

jurisdiction. In addition, Blešić claims that political will is the determinant factor of universal jurisdiction application (Blešić, 2022). It depends on the existence of bilateral treaties between states.

Moreover, the decentralization of international criminal justice enforcement leaves universal jurisdiction relying merely on states' will and actions (Nyawo, 2023). This presents a crucial deficiency in it as it might lead to political conflicts between states, particularly under the absence of international guiding rules about universal jurisdiction. Thus, drafting an international legal instrument is a must to stabilize the judicial status regarding CAH prosecution. So, to overcome this barrier, universal jurisdiction requires a universal justification that accords with its purposes and nature.

International doctrine points out that the R2P theory has several critiques. Royer notes that international law practice reveals that states might profile the R2P principle as a reflection of Western imperialism (Royer, 2021). He argues that the utilization of the R2P theory to justify military interventions against CAH promoted this picturization of that humanitarian theory (Royer, 2021). Also, the R2P would threaten the balance between justice and order (Royer, 2021), which leads to chaos within the targeted state. This dichotomy is the basis of the R2P critiques (Royer, 2021). Therefore, he suggests that jurists should focus on that aspect of the R2P to guarantee the impartiality of its utilization (Royer, 2021). Furthermore, he argues that doctrine should judge the intervention under the R2P according to each case separately (Royer, 2021) as the selective application might trigger injustice in international legal practice (Royer, 2021). The generalization of judging the R2P endangers the reliability of this humanitarian concept; its misuse should never permit its abandonment. So, to overcome this obstacle, the circumstances of each case per se are the determinant of the R2P utilization. This mechanism liberates this principle from the states' political will and enhances its impartial application. Lastly, Royer considers the critiques of the R2P a failure to estimate the consequences of evil that this theory confronts.

Hence, the need to adopt universal jurisdiction against cyber-terrorism exceeds the states' limited opposition. This international criminal act requires the utilization of international toolkits that transcend domestic legal borders and prosecute cyber-terrorists regardless of their location. The R2P theory is the appropriate justification to impose universal jurisdiction regarding cyber-terrorism.

4.2. The Solution: The Validity of the R2P to Impose Universal Jurisdiction Against Cyber-Terrorism

Doctrine considers cyber-terrorism an international evil because of its impacts (Margariti, 2017). Its severity on world peace and security matches the ordinary CAH. The international community is the victim of both crimes (Margariti, 2017). However, its cyber theme distinguishes it as a modern enemy to humanity (Perloff-Giles, 2018). It is an evolved sort

of CAH that falls under the category: other inhumane acts. The congruence of cyber-terrorism elements with the contextual elements of CAH, as jurisprudence concludes[61], solids this categorization. Hence, it requires universal jurisdiction as a global mechanism to prosecute and extradite terrorists. Still, due to the opposition to universal jurisdiction[62], it requires a firm pillar to justify its application that overcomes these obstacles. This pillar is the R2P theory.

The previous review of doctrine points out the prominence of the R2P theory in international law. It was developed into a tool to defend humanity. The R2P's fundamental purpose is protecting humanity against atrocities. Thus, its employment to confront CAH proves its worth in international doctrine and jurisprudence. The R2P, as Royer introduces, is a humanitarian tool to prevent evil since it justifies legal intervention to haunt CAH perpetrators (Royer, 2021). It prioritizes protecting individual human beings rather than maintaining sovereignty under the Westphalian understanding[63].

Royer praises the flexible theme of the R2P as it harmonizes its application with the humanitarian needs to prevent CAH (Royer, 2021). He presents a moral reframing of the R2P as he constructs it based on confronting evil (Royer, 2021). As a consequence, political will cannot oppose norms that are built on it. Instead, the R2P combines states' political interests and humanity's morals in a shield against evil (Royer, 2021). De facto, it is a political moral R2P that defends individuals against evil deeds (Royer, 2021). This reframing of the R2P proves its validity to utilize other international law norms to suppress CAH. Remarkably, Royer's vision of the R2P harmonizes it with state sovereignty; the latter, at its core, is a shield against evil as it organizes the autonomous administration of internal affairs. Hence, it limits national disorder that evil could exploit to spread (Royer, 2021). So, sovereignty reflects the state's responsibility to protect individuals against evil.

As the ICC practice discloses, the collective obligation on states exhorts them to adopt universal toolkits to eradicate CAH to secure world peace[64]. The nature of universal jurisdiction is compatible with this purpose; prosecuting CAH internationally limits their occurrence and enhances justice. Since the R2P justifies military intervention against CAH, it rather justifies judicial intervention, i.e., imposing universal jurisdiction. As the research concludes that cyber-terrorism is a CAH, the R2P should justify prosecuting cyber-terrorists universally. This conclusion implies that a court or a sole prosecutor can prosecute a

---

61 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522; Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494; IT-97-25-T.

62 Discussed in the previous section.

63 Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

64 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

cyber-terrorist located within another jurisdiction if the territorial jurisdiction is lax in that. The horizontal complementarity applies in this case according to Burens's explanation (Burens, 2016). The R2P justifies this judicial intervention because of the international community's duty to prevent CAH as established in international customary law. Judicial intervention to confront CAH is better than military intervention since it enhances global trustworthiness in international criminal justice and eliminates cyber-terrorists' threats to humanity.

Conclusion

The research studies the R2P norm and analyzes its pillars to create a comprehensive image of it in international law. It is a preventive instrument that protects humanity against atrocities. Its firmness could be concluded from its continuous adoption by the UNSC and the international community to intervene to suppress CAH. It is a general principle in international law. Furthermore, legal analysis proves the flexible feature of the R2P since its employment should be on a case-by-case basis. Being utilized to justify military operations permits the R2P to justify legal intervention to prosecute CAH. These facts prove the suitability of the R2P for this mission.

Also, the research analyzes cyber-terrorism. It is a modern criminal activity that inflicts damage on states. Doctrine considers it a mutual enemy to humanity as it threatens world peace and security. By analyzing its elements, the research compares them to the contextual elements of CAH. It concludes the congruence between them. This means that cyber-terrorism is a CAH under the Rome Statute. The category of other inhumane acts extends to include cyber-terrorism. Hence, the international community should act to prosecute and punish cyber-terrorists to eradicate their impunity.

External judicial intervention is achieved in international private law through universal jurisdiction. It includes utilizing domestic judicial tools within other jurisdictions. So, it faces several obstacles from states and even regional organizations. These obstacles frustrate international legal efforts to suppress cyber-terrorism. This fact implies finding a suitable legal justification for universal jurisdiction. A justification that paves the way for the international community to prosecute cyber-terrorists.

Then, the research introduces the R2P principle as the required justification for universal jurisdiction regarding cyber-terrorism. Since the latter is an international threat to world peace and security, the international community must act to eradicate its dangers via universal jurisdiction mechanisms. This intervention complies with international law because it safeguards human rights, which is its favored interest.

Finally, the research closes the gap between international public law and international private law; it employs the R2P theory from the former to justify universal jurisdiction from

the latter. This combination manifests the complementarity of international law branches, which is required to produce a strong understanding of international cyber issues.

References

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court.* Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt –July 23, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:343.3/.7:341.4:343.9
EDN: https://elibrary.ru/cmvqzx
DOI: https://doi.org/10.21202/jdtl.2023.43

Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре
г. Сохаг, Египет

Ключевые слова

кибербезопасность,
киберпространство,
кибертерроризм,
международное публичное право,
международное частное право,
права человека,
право,
преступления против человечности,
цифровые технологии,
юрисдикция

Аннотация

Цель: развитие беспроводных технологий и цифровой инфраструктуры радикальным образом изменило среду обитания человечества, порождая новый тип пространства – киберпространство. Уникальность и особенности этой среды, включая анонимность, безграничность, проблемы, связанные с определением и установлением юрисдикции, стали питательной средой для появления новой глобальной угрозы – кибертерроризма, характеризующегося высоким уровнем латентности, низким уровнем раскрываемости и несравнимо большей опасностью, нежели преступления «в реальном мире». Противодействие новым формам преступности потребовало разработки универсальных инструментов, преодолевающих ограничения традиционной юрисдикции и позволяющих государствам преследовать террористов в киберпространстве. Определение соответствующих инструментов и выявление препятствий политико-юридического характера по их реализации является целью проведенного исследования.

Методы: для достижения поставленной цели используется, прежде всего, формально-юридический метод, применяемый для анализа правовых источников, к которым относятся судебная практика, национальное законодательство и международные акты. Также был задействован доктринальный подход, позволивший на основе научных трудов и теоретических конструкций объяснить сложность новых явлений современного мира и спрогнозировать их развитие в будущем. Основное внимание при этом уделяется стороне преступника, чтобы доказать ее антагонизм с человечеством в соответствии с теоретическими взглядами. Наконец, в исследовании анализируются теории универсальной и традиционной юрисдикции, а также то, как они применяются для преследования террористов.

Результаты: в работе дается критический анализ переосмысления и адаптации концепции юрисдикции применительно к глобальной, безграничной и децентрализованной цифровой среде (киберпространство) и противодействию новым формам терроризма (кибертерроризм); приводятся различные юрисдикционные модели, применимые в киберпространстве; преодолевается разрыв между основными отраслями права: международным частным и публичным правом – путем установления взаимосвязи в отношении к кибертерроризму двух теорий: концепций «обязанности защищать» (R2P) и применения универсальной юрисдикции; выявлены тенденции развития универсальной юрисдикции.

Научная новизна: исследование развивает накопленные научные знания в части обоснования введения иностранной юрисдикции на территории государства для преследования кибертеррористов; устанавливается связь между теориями универсальной юрисдикции в международном частном праве и «обязанностью защищать» (R2P) в международном публичном праве; при этом последняя признается в качестве пригодной основы для введения универсальной юрисдикции в отношении кибертерроризма; переосмысливаются такие традиционные понятия, как суверенитет и юрисдикционная независимость. Устраняется пробел в знаниях, связанных с рассмотрением кибертерроризма как преступления против человечности в международном праве.

Практическая значимость: реализация предложенных выводов будет способствовать усилению международного преследования кибертерроризма; гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления.

Для цитирования

Абделькарим, Я. А. (2023). Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма. *Journal of Digital Technologies and Law*, *1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

Список литературы

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 23 июля 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.