DOI: 10.22034/isj.2025.521581.2330

International Studies Journal (ISJ)
Vol. 22, No. 1 (85). Summer 2025
Reseived Date: 2025/4/17
Accept Date: 2025/6/19
Article Type: Original Research
PP: 415-442

فصلنامه مطالعات بین‌المللی
سال ۲۲، شماره ۱ (۸۵)، تابستان ۱٤۰٤
تاریخ دریافت: ۱٤۰٤/۱/۲۸
تاریخ پذیرش: ۱٤۰٤/۳/۲۹
نوع مقاله: علمی- پژوهشی
صفحات: ٤٤۲-٤۱۵

Feasibility Assessment of the Capacity of Criminal Justice to Mitigate Climate Change through the Suppression of Objectives Arising from Terrorist Crimes Committed on Digital Platforms

Peyman Namamian Ph.D.*- Sobhan Tayebi Ph.D.**

Abstract

Criminal Justice serves as the cornerstone for countering the most destructive acts contrary to human rights and dignity. The engagement of this pivotal institution with actions and conducts violating legal frameworks—such as terrorism, digital (cyber) crimes and climate change—is generally evaluated through national and regional approaches. Legal structures, such as United Nations programs, and operational frameworks, such as Interpol, exist at the international level to address these issues. In contemporary times, terrorist offenses leverage digital tools and technologies to advance their goals, utilizing digital platforms in order to pursue recruitment, financing, and weapons development schemes. This deleterious process inflicts irreparable harm on the biosphere, giving rise to climate-related crimes. Although the interaction between terrorism and climate change is bidirectional, encompassing both direct and indirect effects, the present study, conducted through library-based scientific research employs a descriptive-analytical method and an innovative approach, seeks to elucidate the suppression of digital (cyber) terrorism impacting climate

* Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. / Corresponding Author/ Email: p-namamian@araku.ac.ir

** G Postdoctoral Researcher in International Criminal Environmental Law, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran.

Article Link: https://www.isjq.ir/article_229038.html?lang=en
Online ISSN: 2676-5136 Print ISSN: 2045-1735

change within the framework of criminal justice. To this end, the research aims to address the question: How can the examination of countering digital terrorism affecting climate change be effectively managed within the criminal justice framework? The findings of this study are premised on the hypothesis that criminal justice, as a potent instrument, can effectively mitigate terrorism and digital-climate eco-terrorism through the application of criminalization frameworks, treaties and oversight mechanisms.

Keywords
Criminal Justice, Digital Terrorism, Climate-Related Crimes, Roadmap.

Introduction

Terrorism, in its various dimensions and manifestations, interacts with all environmental factors—encompassing ecological, social, cultural, technological, political, security, economic, and other domains—resulting in profoundly detrimental and erroneous impacts. In fact, terrorism, similar to other environmental factors, develops systematically and leverages all available developmental tools to advance its objectives. This implies that terrorism operates in a dynamic and rapid manner. Among the tools and environmental factors at the disposal of terrorists are technological spaces, such as digital platforms, social media, new media and smart applications, which they exploit for their purposes. The purposes may include propaganda, disseminating information of their actions to instill fear, recruiting and training individuals for destructive acts, facilitating terrorist operations, securing financial resources, or creating myriad innovative avenues for terrorist activities. These actions stem from inadequate technical infrastructure, insufficient regional cooperation and deficient regulatory frameworks. This critical issue poses a serious threat to national, regional, international and citizen security. Although challenges persist due to the inadequacy of laws addressing crimes that promote terrorist activities via digital platforms, their associated risks, and existing legal gaps, solutions are imperative to establish a foundation for countering this issue. (Fathi Al-Rai et al., 2024: 453–467)

Undoubtedly, establishing criminal liability with due regard to criminal justice can obstruct the perpetration of terrorist crimes, a process contingent upon the concerted efforts of the international community. To ensure these efforts and foster international commitments, competent national authorities must establish robust legal frameworks to rigorously address this issue. In this context, the involvement of civil society[1] can also be effective in achieving social control over this matter. Generally, terrorist activities result in the exploitation of the environment, to the detriment of both living and non-living entities on the inhabited planet. In this regard, the convergence of green warfare and terrorism has given rise to a destructive phenomenon, manifesting as environmental crimes. Accordingly, any act or omission that causes severe harm or damage to the environment, thereby precipitating significant human risks—such as economic, social, health, and sanitary consequences—is deemed an environmental crime. Thus, the nature of these crimes encompasses offenses committed against living entities in the environment, such as humans, plants, and animals, as well as offenses against non-living environmental elements, including water, air, soil, sound, and noise pollution. (Poorhashemi et al., 2015: 167–182) Perpetrators, under the guise of terrorism, exploit cyberspace to excessively encroach upon the environment, leaving adverse impacts. Among these impacts are climate change, which interacts bidirectionally with terrorism facilitated through digital (cyber) spaces, yielding deleterious outcomes such as the destruction of natural resources, infringement upon biodiversity, and various forms of pollution. In this context, a pressing concern arises: What strategies can effectively mitigate these risks? The present study proceeds on the premise that criminal justice, bolstered by addressing legal gaps and advancing the objectives of international treaties, offers a viable solution to mitigate this challenge.

1- Background

Famil Zavarjalali and Kadkhodaei (2024) in their article titled Bitcoin: A

[1]. Civil Society Empowerment Programme (CSEP), https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/civil-society-empowerment-programme

Revolution in Terrorism Financing, assert that terrorism financing constitutes one of the most critical strategies for the development and proliferation of terrorism, pursued through various methods, including digital platforms such as cryptocurrencies. The authors note that terrorists have transitioned from traditional to modern methods and given that tracking digital financing offers multiple avenues for evasion, terrorists exploit this approach. Consequently, governments and relevant institutions have, thus far, been largely unsuccessful in mitigating this phenomenon.

Sliedregt (2025) in their study titled The Future of International Criminal Justice Contingent on State Cooperation and Participation asserts that individual criminal liability has evolved and progressed toward collective responsibility. They argue that violations of international obligations and human rights are, in part, attributable to the collaboration of multinational corporations with subversive groups and their financial support. Slidergt contends that international crimes stem from the actions of these corporations, and states must collaborate in the administration of justice to pursue a rightful course.

Fakhoury (2024) in their article titled The Role of Digital Technology in Countering Terrorism asserts that digital technology, in the global era, exerts an undeniable influence on numerous facets of society. The author contends that the complex role played by digital technology in mitigating and preventing terrorist activities delineates a critical domain in the fight against terrorism. Fakhoury further emphasizes the need for a comprehensive understanding of how digital tools, platforms, and methodologies support ongoing efforts to combat terrorism at both national and international levels.

Shackelford (2016) in their article titled On Climate Change and Cyberattacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems, asserts that, given the distinct nature of cyberspace, similar issues arise from its overuse and the myriad challenges it presents. With shifting weather patterns, rising sea levels, and increasing global temperatures, climate change constitutes a problem that affects the entire world. Nevertheless, it is equally true that actions undertaken by multiple actors on a smaller scale can

influence both the global climate change crisis and the promotion of a global culture of cybersecurity.

2- Theoretical Framework: Foundations and Conceptualization

2-1- The Rationale for Criminal Justice

The criminal justice system fulfills a multifaceted role in society, with its ultimate objective being the preservation of public order, the assurance of justice, and the safeguarding of the rule of law. Also, its primary aim centers on the prevention and punishment of criminal behavior, which is vital for the stability and safety of communities. Furthermore, this system is responsible for the rehabilitation of offenders and the provision of opportunities for their reform and reintegration into society. By balancing these objectives, the criminal justice system strives to protect citizens, ensure a fair and lawful judicial process, and foster a safer environment for all. This fundamental perspective, aimed at realizing the criminal justice system, significantly contributes to a profound understanding of its rationale and is wholly essential. For the criminal justice system, by ensuring the enforcement of laws and the administration of justice to the greatest extent possible, plays a pivotal role in safeguarding society and maintaining order. Consequently, the principle of guaranteeing justice and fair treatment within the criminal justice system revolves around the foundational belief that all individuals are entitled to equal treatment under the law. (Berk et al., 2018: 3–44) This underscores that the evolution of criminal justice is oriented toward transitioning from individual criminal liability to collective legal responsibility, thereby facilitating the equitable distribution of justice. (Sliedregt, 2025: 1–10)

Although the state and implications of criminal justice vary across societies, influenced by the diversity of cultures, social behaviors, and human ecological contexts, (Liu, 2024: 1–25) the existence of criminal justice fundamentally responds to severe breaches of public order, protection of the rights of victims and society, promotes general prevention, and combats crime-enabling tools such as terrorism, digital spaces, and climate-related exploitation. Nevertheless,

its efficacy requires a balance between ethics, law, and social realities. Criminal justice pursues objectives such as just retribution, deterrence, rehabilitation and societal reintegration, compensation for harm, and the maintenance of public order. These objectives collectively justify the existence of the criminal justice system, enabling it to both protect society and uphold fairness and ethics in dealing with offenders.

2-2- The Nature of Terrorist Crimes

Terrorism can no longer be regarded merely as a phenomenon, as it manifests as an organized crime with violent dimensions, occurring within a specific framework. Modern terrorism, indeed as an evolved form of terrorism, employs diverse methods to pursue and influence political objectives, typically utilizing intimidation as a strategic tool for impact. Terrorists target densely populated public areas—such as transportation hubs, airports, shopping centers, tourist sites, and nightlife districts—to foment widespread insecurity, prioritizing the disruption of safety and the instillation of fear and terror. (Onat, 2021: 891–914) According to paragraph 3 of UN Security Council Resolution 1566 (2004), terrorist acts are described as criminal actions in which individuals attempt to cause death or severe suffering to others or take hostages, to intimidate a broader society, a specific group of citizens or particular individuals. Such crimes may involve threatening large populations to coerce authorities into specific actions or inaction. From the perspective of international terrorism documents, these acts violate their provisions. The description articulated by the UN Security Council appears to carry profound implications and understanding its motives and methods enables a comprehensive grasp of its essence. This underscores the gravity of terrorism and the necessity of global cooperation for its effective management. (Fakhoury, 2024: 609–618)

Although the approach of universal jurisdiction toward terrorism is robust, this issue must be addressed in a more decisive and effective manner within the framework of the complementary jurisdiction of the International Criminal Court. Terrorism does not operate in isolation today, but sustains its destructive trajectory by exploiting various domains, including economic terrorism,

environmental terrorism, digital terrorism, cultural terrorism and similar manifestations. While terrorism may lack logical coherence in its operations, it consistently functions with an internally developed structure. Accordingly, it is imperative to examine how terrorism leverages technological tools to advance its inappropriate and destructive approach.

2-3- Digital Platforms and Terrorist Crimes

Digital (cyber) terrorism is a form of terrorism that can be succinctly described as terrorism occurring in cyberspace. In its purest form, digital terrorism refers to cyberattacks motivated by political or ideological objectives aimed at coercing or intimidating governments or societies, resulting in violence, severe economic harm, or significant fear among the public. In a broader sense, it may encompass the terrorist use of cyberspace, including online information and communication technologies, to advance terrorist goals. (Bastug and Ismail, 2024: 1–20) Accordingly, digital terrorism constitutes a distinct category within cybercrimes, involving the use of digital technologies to support or execute ideologically motivated attacks. In this context, terrorist groups increasingly utilize the internet for exchanging ideas, planning operations, and communicating with members globally. It has been established that digital platforms, including social media and encrypted messaging services, provide terrorist organizations with an environment conducive to recruiting individuals and disseminating propaganda with relative ease (Harrison, 2018: 28–33).

The digital communications facilitate the scope of reach and impact of terrorism, enabling groups to bypass geographical constraints and propagate their ideologies globally. (Corliss, 2023: 58–112) In this regard, the approach of international authorities has been clarified. For instance, UN Security Council Resolutions 2178 (2014) and 2396 (2017) call on member states to cooperate in adopting national measures to prevent terrorists from exploiting technology and communications to commit digital crimes with a terrorist intent[1]. Resolution 2396 (2017) further encourages member states to enhance cooperation with the private sector, particularly information and communication technology

[1]. https://main.un.org/securitycouncil/en/s/res/2178-%282014%29

companies, in collecting digital data and evidence in cases related to terrorist crimes[1]. The UN Security Council, in Resolutions 2419 (2018), 2462 (2019), and 2490 (2019), acknowledges that activities by non-state individuals and entities in the digital domain may pose a threat to international peace and security, including through digital attacks on critical infrastructure, disruption of online payment systems, internet access blockages, and interference with Twitter and Instagram accounts. The "Global Counter Terrorism Programme on Cybersecurity and New Technologies[2]", adopted in April 2020, aims to enhance the capacities of member states, international and regional organizations, and UN entities to raise awareness of threats posed by digital crimes with terrorist intent and to bolster technical capacities needed for prevention, mitigation, and response to terrorist and violent extremist groups exploiting new technologies, such as the internet (Zaidy, 2024: 1–12).

The international community has thus far adopted specific international legal instruments to address the exploitation of the internet by terrorist groups, led by the United Nations, the Council of Europe, and the European Union. However, the development of legal regulations faces challenges due to the novel characteristics of the internet. Nevertheless, in 2021, the UN General Assembly held its first organizational session to draft a comprehensive international convention on countering the use of information and communication technologies for criminal purposes. The objective of this draft was to "strengthen international cooperation to combat certain crimes committed through information and communication technology systems and to share evidence of serious crimes electronically," with the ultimate goal of preparing a "draft UN Convention Against Cybercrime[3]." However, due to technical and legal reasons, the document has not yet been finalized or adopted.

---

[1]. https://main.un.org/securitycouncil/en/content/sres23962017

[2]. Global Counter Terrorism Programme on Cybersecurity and New Technologies; https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/mya_project_itemid_27.pdf

[3] "Draft United Nations Convention against Cybercrime", UN General Assembly, A/AC.291/L.16, New York, 29 July–9 August 2024, 7 August 2024, https://documents.un.org/doc/undoc/gen/v24/055/48/pdf/v2405548.pdf

3- Digital Terrorism and Climate Change

3-1- Immediate Effects of Digital Terrorism on Climate Change

Terrorism and climate change exert bidirectional, direct effects on one another. Beyond the threats to human safety and security posed by floods and droughts, climate change generates risks to human life and well-being, including public health crises, shortages of fuel and energy, food insecurity, disruptions to national security, organized crime, vulnerable populations, forced migration accompanied by "climate refugees" fleeing environmental and social degradation in search of safety and stability, and the destruction of critical infrastructure. (Lydon et al., 2024: 16–30) The process of the direct effects of digital terrorism and climate change is cascading, wholly pervasive, and entails the most severe consequences.

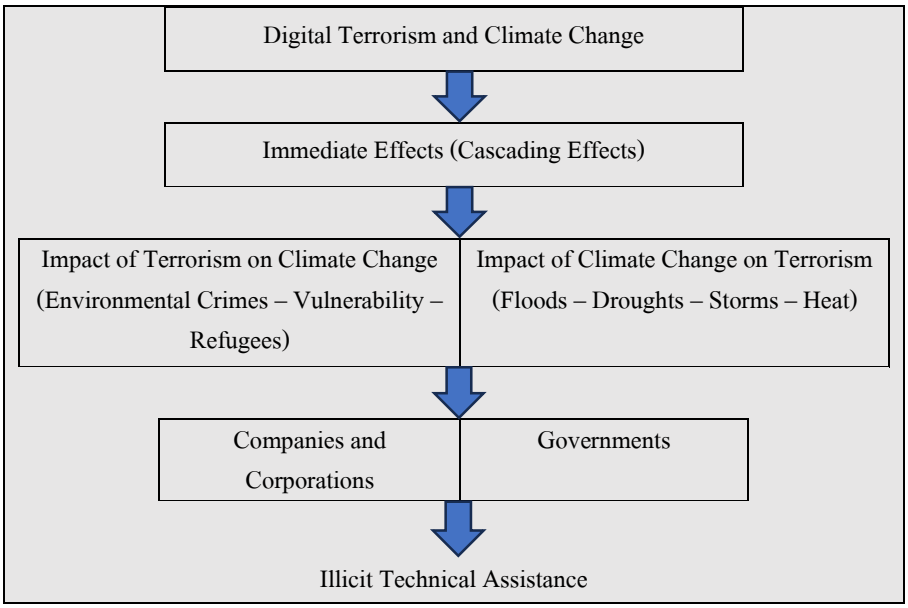

Figure 1: Immediate Effects (Researcher-Driven)

Although terrorism has posed a serious threat to life in the biosphere, climate change is the primary driver of terrorism in the future. It is currently recognized by many countries as a strategic security threat, though its potential role in igniting, facilitating, or exacerbating terrorist conflicts remains relatively

unexplored. Nevertheless, there are increasing indications that climate change—whether through direct or indirect effects—must be regarded as a significant driver of terrorism at the macro level. It is arguably well-established that the causes of terrorism can encompass large-scale geopolitical processes while simultaneously involving far more personal factors at the individual level. In this context, the key factors influencing the impact of climate change on terrorism can be observed in aspects such as population growth, social polarization, migration patterns and technological development. (Silke, 2022: 883–893) Digital terrorism spans a vast domain, which will be subject to more detailed analysis in the forthcoming discussions.

3-2- Mediated Effects of Digital Terrorism on Climate Change

Some policymakers worldwide recognize climate change as an escalating security threat, increasingly pointing to climate change, particularly climate-related terrorism. Mediated effects between climate change and factors such as resource scarcity, loss of economic opportunities, and instability contribute to this phenomenon. Consequently, climate change is indirectly considered through its impact on conditions often regarded as drivers of terrorism, which lead to terrorism. (Mavrakou et al., 2022: 894–913) The process of the indirect effects of terrorism and climate change is cyclical, disrupting the natural life cycle and placing the rights of future generations at risk of violation.

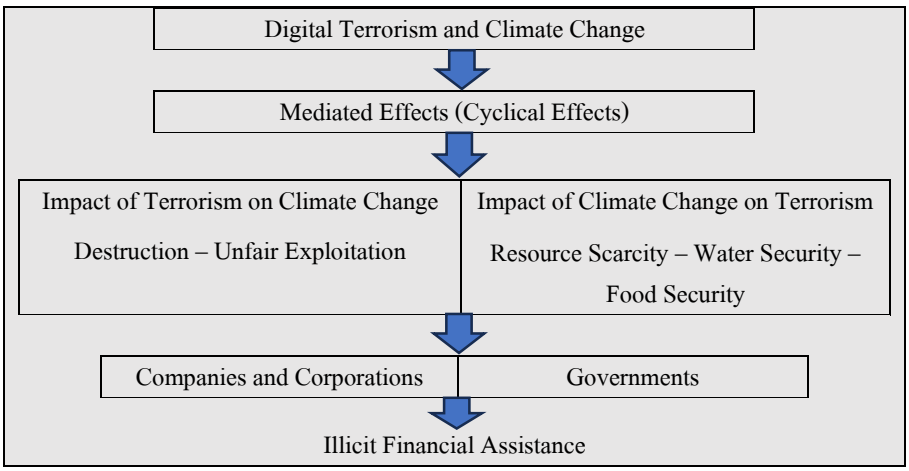

Figure 2: Mediated Effects (Researcher-Driven)

This trend indicates that terrorism and climate change threaten the resources essential for human needs, and irrational exploitation disrupts global equilibrium in terms of economic and social security. Although climate change is not a direct driver of conflict or violent extremism, it can exacerbate the drivers of both, acting as a "risk multiplier." These factors involve a complex interplay of historical, social, economic, and political elements, which are intensified by climate change through frequent and severe extreme weather events, such as drought and famine. Severe security responses to suppress conflicts and the emergence of illicit economies may contain further hardships and suffering in such climate- and security-sensitive hotspots, which, in turn, may drive recruitment, whether out of livelihood necessity or growing grievances. For instance, in Sudan's Darfur region, conflict over natural resources has evolved into a decade-long crisis in an area that forms part of a primary route for tracking and trafficking humans and weapons (with a technological approach) to Libya; where the United Nations Development Programme consistently monitors the destruction of natural resources in this region in which all dammed water reservoirs have dried up over the past decade, rendering it impossible to exclude climate change considerations from efforts to stabilize the situation. (UNDP, 2020: 1–12)

3-3- The Role of Digital Platforms in Exacerbating the Impacts of Climate-Related Terrorism

Climate change, through its mediated impacts, may be amplified when interacting with digital platforms such as systems, applications and similar technologies, with cryptocurrency production being a notable example. The varied impacts of digital media platforms on the intent to share information about the risks of climate change also constitute a concern. Indeed, differing types of information and data can cast doubt on the verification of the negative effects of climate change. (Lu, 2024: 495–515) Furthermore, the growing threats to digital security pose serious challenges to population health, endangering public health, which is considered a form of human rights violation (Namamian, A., 2024: 1–11).

Although countries are striving to strengthen cyber sovereignty, such developments highlight the extent to which technological progress is intertwined with internet governance, even in the absence of immediate threats. In this context, cyberspace and technological advancements have played a significant role in global climate change, particularly in terms of greenhouse gas emissions (Shackelford, 2016: 653–711).

This role is dual, capable of both reducing and increasing impacts. For instance, cryptocurrency mining, energy consumption by data centers, increased electronic waste, and polluting industrial activities contribute to higher carbon emissions. Conversely, leveraging artificial intelligence, promoting environmental campaigns by cyberspace and smart energy optimization structures, which are able to reduce greenhouse gas emissions. However, the most severe impacts of climate change may pertain to human migration, as millions are displaced due to coastal erosion, coastal flooding, and severe droughts. It has been predicted that by 2050, forced climate refugees will emerge. According to current forecasts, the "carrying capacity" of large parts of the world will be jeopardized by climate change, leading to forced migration that triggers violence and conflict. (Macklin, 2022: 979–996) Additionally, concerns arise from radical environmental movements, which, based on their ideological approaches and the reinforcement of ecofascism or green extremism, may lead to violent acts, manifesting as militant terrorism in this form. Conversely, an opposing perspective exists that views climate change as a distraction for humanity, thereby justifying violent acts. For example, Anders Behring Breivik, the Norwegian terrorist who killed seventy-seven people in a bombing in Oslo and a shooting in Utøya on July 11, 2011, believed that global warming caused by human activities was a hoax. He displayed overt hostility toward environmental activists, asserting that "enviro-communism" was part of a broader conspiracy to draw humanity into a "global government" under UN supervision. (Darwish, 2024: 443–463) Another example is Brenton Tarrant, the Australian terrorist who killed fifty-one people in two mosque attacks in Christchurch, New Zealand, on March 15, 2019. He believed that "invaders"

(migrants) were those increasing the world's population. "Kill the invaders, kill the overpopulation and by doing so, save the environment," he argued, referring to both migrants and those contributing to higher birth rates. (Christensen, 2024: 174–196) Thus, the connection between digital terrorism and climate change becomes increasingly evident.

4- Criminal Justice in Addressing Digital Climate-Related Terrorist Crimes

4-1- Legal and Treaty Approaches

Standardizing responses to digital terrorist crimes has not been an easy process, with its origins dating back to the 1960s. However, its framework and development gained momentum from the 1990s onward. Key milestones include the 2001 Convention on Cybercrime, strengthened in 2004, UN Security Council Resolution 2341 of 2017 on global counterterrorism strategies, the Global Programme on Countering Terrorism in Cybersecurity and New Technologies of 2020 (Nemamian and Shahbazi, 2024: 73–91), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law of 2024 (CETS 225), alongside national-level laws. (Behadori Jahromi et al., 2024: 1–31) Significant efforts have been made within the United Nations Counter-Terrorism Committee Executive Directorate (CTED), alongside other global reform initiatives stemming from governmental and regional initiatives presented as agreements. Each of these initiatives is at a different stage of development and addresses a critical need. However, each also introduces a new layer of complexity to the management of cross-border data.

Multilateral Initiatives	
United Nations Convention against Cybercrime: Strengthening International Cooperation to Combat Certain Crimes Committed through Information and Communication Technology Systems and Sharing Electronic Evidence for Serious Crimes	The United Nations Convention against Cybercrime was adopted by the United Nations General Assembly on 24 December 2024 in New York through Resolution 79/243.

Council of Europe: Second Additional Protocol to the "Budapest Convention"	The Budapest Convention was adopted in 2001, and the Second Additional Protocol was adopted in 2022.
Regional and Governmental Initiatives	
European Union: e-Evidence Regulation	Adopted in 2019.
Brazilian Civil Rights Framework for the Internet	Adopted in 2014, and Data Protection Law, implemented in 2021.
China: Data Security Law and Personal Information Protection Law	Adopted in 2017 and updated in 2021.
India: Personal Data Protection Bill	Adopted in 2021.
Russian Federation: Data Localization Law	Adopted in 2015.
United States of America: Clarifying Lawful Overseas Use of Data Act (CLOUD Act)	Adopted in 2018.
United Nations Initiatives	
Global Initiative of the Counter-Terrorism Committee Executive Directorate (CTED), United Nations Office on Drugs and Crime (UNODC), and International Association of Prosecutors (IAP)	Pursuant to UN Security Council Resolutions 2322 (2016) and 2396 (2017), encourages cooperation between governments and the private sector regarding access to and security of digital data.
United Nations Office on Drugs and Crime (UNODC)	Electronic Evidence Center, established in 2007
Secretary-General's Roadmap for Digital Cooperation	Initiated in 2018 with the formation of a High-Level Panel on Digital Cooperation in the era of digital interdependence, ongoing to date, addressing a wide range of issues including digital human rights, digital identity, privacy, and data protection.
United Nations Counter-Terrorism Centre (UNCCT), of United Nations Office of Counter-Terrorism (UNOCT), and International Criminal Police Organization (INTERPOL)	Publication of a handbook titled Use of the Internet and social media for Counter-Terrorism Investigations in 2021.

Significant Initiatives	
Joint EU-Europol Project on Criminal Justice and Law Enforcement Cooperation[1]	Focused on leveraging data expertise, adopted in 2021.
G8 Cybercrime Network	Operating since 1997, with a focus on emergency data and data preservation, ongoing to date.
E Internet and Jurisdiction Policy Network (I&JPN)	Operating since 2020, with a focus on internet and judicial policy, ongoing to date.

Table 1: Major Efforts for Reforms

Source: (CTED, 2022: 16–22)

These efforts demonstrate the significant measures undertaken, the approaches considered and the undoubtedly positive outcomes achieved globally to seriously combat cyberterrorism. Among these outcomes are the standardization of various methods to counter the diverse and numerous forms of terrorism and the multilateral cooperation of international organizations in achieving a unified approach to confronting cyberterrorism. Nevertheless, numerous challenges persist in the shadow of these global cooperative efforts.

Legal Fragmentation	The development of legal frameworks introduces complexities, and the coexistence of multiple shared legal regimes leads to regulatory fragmentation and diplomatic efforts.
Reduced Interoperability	Conflicts in implementing regulations due to states' domestic approaches driven by national interests.
Localization	The expansion of internet access and data availability within the framework of domestic regulations and local structures.
International Human Rights Concerns	Concerns over the lack of guarantees for human rights in the processes of data retention and counterterrorism.
Private Sector Procedures	The approach to information and data security and their preservation depends on the capacity and influence of large and small companies.

Table 2: Procedures and Challenges, Source: (CTED, 2022: 23–28)

[1]. The European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Union Agency for Law Enforcement Cooperation (Europol)

[2]. The G7 24/7 Cybercrime Network began under the auspices of the Group of Eight (G8).

The focus of technical assistance providers in advancing and addressing challenges should be on ensuring interoperability and expanding the capacity of law enforcement authorities developing across various legal regimes. It is also clear that guaranteeing respect for and compliance with international human rights laws and fundamental freedoms is an essential component of reforms and capacity-building efforts.

Ensuring Interoperability	Establishing a global framework based on foundational treaties such as the United Nations International Covenant on Civil and Political Rights.
Capacity Building	Considering international treaty structures, adhering to data propriety, and enhancing measures to prevent terrorism's access to cyber structures.
Countering Terrorism Legitimation	An approach to confronting and suppressing the interaction with and recognition of terrorists and terrorist groups.
Peacebuilding and Peace Acceptance	A global perspective on positive state interactions to move away from destructive tensions and dismantle exploitative structures such as terrorism.
Digital Order	Encompassing financial, commercial, political, security, cultural, and cyber dimensions, exemplified by China's "Digital Silk Road" with its approach to cross-border initiatives including financial infrastructure, technological innovations, and health. (Ghorbani Sheikhneshin and Keshvarian Azad, 2024: 161–185)

Table 3: Looking to the Future
Source: (Researcher-Driven)

Fortunately, such efforts may serve as critical turning points in addressing cross-border cybercrimes and pave the way for enhanced cooperation in the proper utilization of digital platforms, thereby facilitating global law enforcement requests for access to electronic evidence. Consequently, with a clear vision, it is possible to advance toward the right to secure and low-risk access to information and data, while controlling improper access, which enhances interoperability. Meanwhile, ongoing efforts enable the development of a

transnational legal framework to overcome barriers in combating cyberterrorism and its adverse effects. Accordingly, it appears that by strengthening laws, both from technical and legal perspectives, the groundwork for criminalizing cybercrimes has been established, leading to more effective accountability and legal prosecution.

4-2- Countering Digital Climate-Related Terrorism in Light of International Cooperation

In today's world, terrorist criminality in the digital realm has become an international challenge, with numerous international organizations collaborating to address it. (Namamian and Ameri-Siahuei, 2024: 19–28) Strengthening international cooperation can have two distinct dimensions. The first is a national-to-international dimension, indicating that states providing or controlling online platforms must conduct accurate assessments and precise foresight regarding this issue. The second is an international-to-national dimension, highlighting the role of the United Nations, other international organizations, and states in adhering to treaty obligations. (Namamian, B., 2024: 215–233) multi-stakeholder cooperation is another form of international collaboration that can be employed within the framework of common rules, uniform codes, union norms, and self-regulatory methods, while preserving and enhancing cybersecurity, to counter cyberterrorism (Shackelford, 2016: 653–711).

Consequently, key future challenges will include ensuring interoperability among various initiatives and expanding the capacity of law enforcement agencies in the face of new transnational regulatory regimes, as discussed in the previous section. This moment thus presents an opportunity for global and regional institutions, as well as private and multilateral groups, to expand capacity-building efforts aimed at addressing these challenges. These objectives include ensuring interoperability across different regimes and enhancing capacity, while guaranteeing respect for human rights and fundamental freedoms. Law enforcement agencies will always face judicial barriers in a

global environment, but capacity building and interoperability can reduce unnecessary delays in resolving some of the most urgent investigations.

4-3- Leveraging Emerging Technologies and Climate-Related Terrorism

The development of digital technologies has profoundly affected all aspects of human life. When considering the negative dimension of this development in relation to digital terrorist crimes, key issues include terrorism financing (Famil Zavarjalali and Kadkhodaei, 2024: 235–252), disruptive digital activities such as malicious attacks on infrastructure, disruption of online commerce, and cryptocurrencies. (Namamian and Shekarbeigi, 2023: 7–18) Consequently, the harms resulting from digital crimes and the misuse of technology are globally on the rise, rapidly drawing attention at both national and international levels. (Olumoye, 2013: 10–20) Indeed, cybercrimes are the fastest-growing type of crime worldwide, one that no company or nation can combat alone. Numerous cybercrime developments are highly likely to occur, and if they do, they could lead to massive financial collapse due to lost revenue, wasted resources, and reduced productivity. These developments include the rise of financial cybercrimes, espionage, deep infiltration of government and private organizations storing customer data, an increasing number of individuals worldwide engaging full-time in cybercrimes, and the growing sophistication of attack tools and methods. (Johnson, 2024: 515–534) A critical point to note here is modern terrorism, which leverages cyberspace. This implies that terrorism can access advanced weapon technologies, including nuclear weapons, through digital platforms. (Sadeghipour et al., 2024: 257–276)

Accordingly, the global cyberspace provides a unique environment for conducting cyberterrorism and pursuing other international terrorist objectives. As a result, disruptive actions occur across several domains. In the first domain, malicious attacks against computer systems conducted via the internet (cyberterrorism) can not only cause the destruction, corruption, or inaccessibility of intangible computer data, thereby disrupting production processes, banking systems, or public administration, but also damage physical property and human lives. For example, attacks on computer systems managing nuclear power plants,

dams, flight control systems, hospital computers, or military weapon systems could have such consequences. Given that many aspects of modern society heavily rely on computer systems, the risks posed by this type of criminal activity are significant. However, currently, very few instances of such attacks are known. In contrast, the terrorist use of the internet and other electronic communication systems in the second domain—public dissemination of illegal content—is widespread. Here, terrorists exploit the internet and other communication systems to threaten terrorist acts, incite, promote, and glorify terrorism, participate in fundraising and terrorism financing, provide terrorism training, recruit for terrorism, and publish racist and xenophobic materials. Consequently, the internet has become a vital tool through which terrorists broadcast their messages to a broad audience. Finally, the internet and other computer systems play a significant role in the third domain mentioned above, namely the logistical preparation of terrorist crimes, including internal communications, acquiring information (e.g., about bombings, hostage-taking, or hijackings), analyzing targets, and other forms of intelligence gathering (Sieber, 2006: 395–449).

5- Strategies for Mitigating the Impacts of Digital Terrorism on Climate Change

5-1- Prevention Through the Criminalization of Digital-Climate Terrorism

The nexus between climate change and violent extremism leading to terrorism is the central focus of the initiative "Addressing the Relationship Between Climate Change and Violent Extremism." Led by Germany and Kenya, with support from the implementing partner, the Global Community Engagement and Resilience Fund, this initiative aims to better understand how climate change exacerbates vulnerabilities in communities and amplifies known drivers of violent extremism that lead to terrorism. (GCTF, 2025: 1) Today, the primary approach of developed countries, particularly European nations, is restorative justice grounded in criminal justice and the criminalization of various and diverse dimensions of terrorism. (Nasirzadeh and Mohammadalipour, 2024: 117–140)

Criminal justice, from both legal and political perspectives, is among the effective strategies for eliminating or reducing terrorism. This is because states prioritize restoring security, and these two dimensions often intersect strategically, inevitably producing consistent effectiveness (Mirmohammadsadeghi and Ghadiri Bahramabadi, 2015: 9–41).

On one hand, climate change intensifies existing social vulnerabilities, enabling terrorism. On the other hand, climate change triggers terrorism through a complex relationship. Criminal justice, by identifying the intersection of terrorism and climate change, can be effective. (Spadaro, 2020: 58–80) This premise is established as follows: when climate change leads to issues such as drought and water scarcity, individuals, in pursuit of survival, may engage in unproductive activities, including joining subversive groups, thereby manifesting this impact. This demonstrates that when accessible resources become scarce, social processes are disrupted, and destructiveness proliferates. If these events occur through the exploitation of the digital realm, utilizing cyber platforms for such purposes, it becomes evident that security is threatened by driving factors. In this regard, it appears that criminal justice, by employing alternative tools such as restricting access to data, information dissemination platforms, and appealing digital platforms through criminalization and the imposition of severe penalties, can prevent such occurrences.

5-2- Protection of the Affected Climate

The climate change crisis is regarded as the most significant contemporary environmental crisis, resulting from the increase in greenhouse gases due to misguided industrialization practices and the reliance on fossil fuels. (Tayebi et al., 2023: 149–162) To mitigate climate change and, concurrently, curb eco-terrorism, efforts must focus on strengthening partnerships and improving frameworks. In this regard, supporting climate resilience initiatives—through enhancing the supportive roles of stakeholders and investing in resilience—can effectively deepen the understanding of how critical social and economic resilience reduces the potential impacts of climate change disasters and political violence. For instance, Boko Haram, other radical religious movements, hired

gangs of political thugs, and general criminal networks primarily draw support and recruits from impoverished young men seeking alternatives to their predetermined life paths, condemned by their historical circumstances. (Jeremiah, 2021: 81–92) Nevertheless, while climate change and terrorism are global phenomena, their intensity and frequency are unevenly distributed. Therefore, the scope of the impact of climate change and terrorism on society must address various research scales across different time horizons. (Henkin et al., 2022: 1–7)

5-3- Facilitating the Implementation of Climate Policies and Roadmap

The emergence of environmental terrorism and conflicts over natural resources is linked to the loss of water reserves and fertile agricultural lands. Short-term and long-term strategies to reduce vulnerability to climate risks and adapt to climate change are essential and can be proposed within the framework of climate policies.

Creativity in developing solutions for environmental improvement ----> Regulation and control of environmental data and information arising from all industrial and developmental activities ----> Excellence in adhering to national laws and international treaties ----> Rapid transition to replacing fossil fuels with renewable energy sources ----> Obligation to secure and facilitate funding and take swift preventive actions ----> Urgent efforts toward climate regulation and climate restoration

1st: Roadmap for Combating Climate Change

Recognizing the environment as a critical concern from a public policy perspective ----> A laboratory of democracy and activating civil society ----> Protecting the environment through scientific methods ----> Public diplomacy and environmental diplomacy ----> Sustainable political development and sustainable environmental development ----> Education and awareness-raising

2nd: Roadmap for Achieving Policy Implementation

Applicability of regulations at national and international levels ----> Framework for liability for causing damage and obligation to provide compensation ----> Transparency in implementing international criminal law ----> Criminalization tailored to current conditions and situational requirements ----> Rigorous prosecution of ecosystem destruction

3rd: Roadmap for Climate-Related Counter-Terrorism Issues

Individual and collective efforts under the umbrella of cybersecurity ----> Deeming state-sponsored terrorism and ineffective support illegitimate ----> Unified treaty-influenced infrastructure ----> Protection of networks and creation of encryption codes to prevent and counter illicit exploitation ----> Development and study of experimental models for countries' utilization

4th: Roadmap for Combating Cyberterrorism

Rational control of users via mobile phones, computers, laptops, and other cyber communication ----> devices ----> Strengthening data centers and establishing highly confidential regulations to prevent potential misuse ----> Protection of networks and data to prevent fake and unreliable data ----> Protection of the environment against electronic waste ----> Designing green energy consumption for digital tools

5th: Roadmap for Mitigating the Impact of Digital Platforms on Climate Change

This framework indicates that criminal justice, to be realized at the national level, requires policy implementation, and at the international level, necessitates a roadmap, which will be achieved through treaty-based efforts to combat cyber-climate eco-terrorism.

Conclusion

Climate change is a factor associated with increased violent conflicts and instability, which may worsen with rising temperatures. The growing scarcity of essential resources such as water, increasing desertification of agricultural

regions, and overall temperature rise have all been shown to exacerbate political instability and state fragility. The nexus between climate change and terrorism is now defined by the evolution of strategies and recruitment opportunities that leverage environmental stress as a form of control. This is a strategy likely employed by state and non-state actors alike, involving environmental damage through acts of warfare or terrorism, resulting in environmental terrorism. Environmental terrorism, traditionally encompassing actions to defend the environment and promote related policy changes, does not appear to be a new threat. However, terrorism and climate change seem to proliferate more rapidly on digital platforms, as unchecked dynamics can sometimes transform values into counter-values. For instance, climate environmental activists, occasionally under pressure from governments, may be drawn to groups promoting destructive processes. This could create a dangerous security impact in the heart of advanced regions, where water scarcity is not yet prevalent, but the loss of civic rights could foster the emergence of a new form of environmental terrorism. Thus, on one hand, climate change-related conditions provide both an opportunity for the development of environmental terrorism in resource-scarce regions and a potential platform for a new form of terrorism driven by anti-progress extremist ideologies. On the other hand, ecofascism represents another form of terrorism that far-right extremists may perpetrate. The trajectory of terrorism appears to be increasingly modernizing. Terrorism has left its mark on multiple places, notably impacting the environment and climate change, as well as cyber platforms and artificial intelligence. Digital tools, including digital platforms and devices, have been at the disposal of terrorist mechanisms, and these tools and platforms also influence climate change. In this context, viewing criminal justice as a balanced global tool offers hope that criminalization, grounded in treaty-based resources and international documents, gains valuable legitimacy, ensuring that responsibility and accountability remain robust. Accordingly, addressing digital terrorism impacting climate change within the framework of criminal justice has been narrated across various dimensions. One dimension is that treaty-based tools, state commitments, and international

cooperation can serve as a restraining factor. Another is that the tool of criminalization can act as a deterrent. Additionally, strengthening global jurisdiction, revising the list of crimes against humanity, enhancing the performance of the International Criminal Court, and developing complementary jurisdiction through transnational courts can be effective restraining factors. Within the scope of this research, the following recommendations can be promoted:

First, it appears that the international community requires a strategic treaty on cyberterrorism and climate change to make this pathway unsafe for terrorism.

Second, localization of the aforementioned treaty at the national level through the development and strengthening of policy implementation to counter cyber-climate terrorism, thereby enhancing the role of states in combating terrorism.

Third, formulation of a cybersecurity vision by relevant institutions and the establishment of a committee to counter cyber-climate terrorism, clarifying the responsibilities of relevant entities and enhancing the effectiveness of non-military defense mechanisms.

References

1. Ameri-Siyahoui, F., & Namamian, P. (2024). Confronting terrorist criminals in the digital space; a look at the legislative experience in Islamic countries. *Quarterly Journal of Comparative Studies in Islamic Countries Law, Ilam University*, *2*(3), 19–28. **(In Persian)**
2. Bahaduri Jahromi, A., Farahani, M. S., Jafarian, M. M., & Ghasemipour, R. (2014). New anti-competitive practices in cyberspace platforms. *University of Tehran Quarterly Journal of Public Law Studies*, 1–31. **(In Persian)**
3. Bastug, M. F., & Onat, I. (2024). Cyberterrorism. In *Oxford research encyclopedia of criminology*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.784
4. Berk, R., Heidari, H., Jabbari, S., Kearns, M., & Roth, A. (2018). Fairness in criminal justice risk assessments: The state of the art. *Sociological Methods & Research*, *50*(1), 3–44. https://doi.org/10.1177/0049124118782533

5. Christensen, C. B. (2024). Ecofascism and green Nazis in Denmark 1920–2020. *Scandinavian Journal of History*, *50*(2), 174–196. https://doi.org/10.1080/03468755.2024.2317812
6. Corliss, C. (2023). Digital terror crimes. *Columbia Journal of Transnational Law*, *58*, 58–112.
7. Darwish, M. (2024). Fascism, nature and communication: A discursive-affective analysis of cuteness in ecofascist propaganda. *Feminist Media Studies*, *25*(2), 443–463. https://doi.org/10.1080/14680777.2024.2317811
8. Fakhoury, A. (2024). The role of digital technology in countering terrorism. *Pakistan Journal of Criminology*, *16*(3), 609–618.
9. Famil Zavar Jalali, A., & Kadkhodaei, A. A. (2024). Bitcoin; A revolution in terrorism financing. *University of Science and Culture Quarterly Journal of Law and New Technologies*, *5*(9), 235–252. **(In Persian)**
10. Fathi Al-Rai, A., Alomran, N. M., & Al Ansari, M. A. J. (2024). The crime of digital promotion of terrorism through digital platforms and new media: A comparative study of Jordanian and Emirati laws. *International Journal of Electronic Governance*, *16*(4), 453–467.
11. Ganjbakhsh, M., Jafarpour, K., & Sadeghipour, E. (2024). Citing the doctrine of an expanded interpretation of the right to self-defense in confronting postmodern terrorism: With an emphasis on the cyberterrorism of the People's Mojahedin-e-Khalq Organization. *Quarterly Journal of International Studies*, *21*(3), 257–276. **(In Persian)**
12. Ghorbani Sheikhneshin, A., & Keshwarian Azad, M. (2024). China's digital silk road initiative: The infrastructure of the Chinese digital order. *Quarterly Journal of International Studies*, *21*(3), 161–185. **(In Persian)**
13. Global Counterterrorism Forum. (2025). *Understanding the risks of climate change's relationship with violent extremism conducive to terrorism and building solutions* (Article ID/312).
14. Harrison, S. (2018). Evolving tech, evolving terror. *Center for Strategic and International Studies*, 28–33.
15. Henkin, S., Boyd, M. A., & Romm, M. (2022). Of terror? Part I: Approaches

to the study of climate change and terrorism. University of Maryland, 1-7.

16. Jeremiah O., A. (2021). Climate change - terrorism nexus? A preliminary review/analysis of the literature. *Perspectives on Terrorism*, *15*(1), 81–92.
17. Johnson, S. D. (2024). Identifying and preventing future forms of crimes using situational crime prevention. *Security Journal, 37*, 515–534. https://doi.org/10.1057/s41284-023-00398-x
18. Liu, J. (2024). The relationism theory of criminal justice—A paradigm shift. *Asian Journal of Criminology, 19*, 1–25. https://doi.org/10.1007/s11417-023-09410-0
19. Lu, Y. (2024). The influence of cognitive and emotional factors on social media users' information-sharing behaviours during crises: The moderating role of the construal level and the mediating role of the emotional response. *Behavioral Sciences, 14*(6), 495–515. https://doi.org/10.3390/bs14060495
20. Lydon, D., Hallenberg, K., & Kapageorgiadou, V. (2024). 'This is not a drill': Police and partnership preparedness for consequences of the climate crisis. *International Journal of Police Science & Management, 27*(1), 16–30. https://doi.org/10.1177/14613557241226639
21. Macklin, G. (2022). The extreme right, climate change and terrorism. *Terrorism and Political Violence, 34*(5), 979–996. https://doi.org/10.1080/09546553.2020.1784144
22. Mavrakou, S., Chace-Donahue, E., Oluanaigh, R., & Conroy, M. (2022). The climate change–terrorism nexus: A critical literature review. *Terrorism and Political Violence, 34*(5), 894–913. https://doi.org/10.1080/09546553.2022.2091581
23. Mirmohammad Sadeghi, H., & Ghadiri Bahramabadi, R. (2015). The role and position of politics in criminal justice governing terrorism crimes. *Quarterly Journal of Criminal Law Research, 4*(13), 9–41. **(In Persian)**
24. Movahedian, H., Norouzi, N., & Tayebi, S. (2023). A legal approach to climate change with an emphasis on the technological convergence model. *Quarterly Journal of Law and New Technologies, University of*

Science and Culture, *4*(7), 149–162. **(In Persian)**

25. Namamian, P. (2024a). Responding to threats from terrorist crimes on digital platforms for violation of public health rights. *Iranian Health Law System Quarterly*, *1*(4), 1–11. **(In Persian)**
26. Namamian, P. (2024b). Countering and preventing the committing of terrorist crimes on virtual social networks. *New Technologies Law Quarterly, University of Science and Culture*, *15*(10), 215–233. **(In Persian)**
27. Namamian, P., & Shahbazi, M. (2024). Protecting the security of digital platforms against terrorist crimes; a strategy in promoting the digital security of governments. *Quarterly Journal of Internal Security Studies and Research, Sacred Defense Science and Education Research Institute*, *2*(1), 73–91. **(In Persian)**
28. Namian, P., & Shekarbeigi, A. (2023). Countering terrorist crimes in the digital age; challenges and strategies. *Sooreh University, Quarterly Journal of Strategic Communication Studies, 3*(9), 7–18. **(In Persian)**
29. Nasirzadeh, M., & Mohammadalipour, F. (2014). Restorative justice and capacity building to combat terrorism in Europe. *Quarterly Journal of International Studies, 21*(3), 117–140. **(In Persian)**
30. Olumoye, M. Y. (2013). Cyber crime and technology misuse: Overview, impacts and preventive measures. *European Journal of Computer Science and Information Technology*, *1*(3), 10–20.
31. Onat, I., Guler, A., Kula, S., & Bastug, M. F. (2021). Fear of terrorism and fear of violent crimes in the United States: A comparative analysis. *Crime & Delinquency*, *69*(5), 891–914. https://doi.org/10.1177/00111287211014152
32. Pourhashemi, A., Namamian, P., & Tayebi, S. (2015). Criminalization of environmental terrorism; challenges, norms and strategies. *Quarterly Journal of Environmental Science and Technology*, *17*(1), 167–182. **(In Persian)**
33. Shackelford, S. J. (2020). On climate change and cyber attacks: Leveraging polycentric governance to mitigate global collective action problems. *Vanderbilt Journal of Entertainment and Technology Law*, *18*(4), 653–711.

34. Sieber, U. (2006). International cooperation against terrorist use of the internet. *Revue Internationale de Droit Pénal*, *77*(3), 395–449.
35. Silke, A., & Morrison, J. (2022). Gathering storm: An introduction to the special issue on climate change and terrorism. *Terrorism and Political Violence*, *34*(5), 883–893. https://doi.org/10.1080/09546553.2022.2054820
36. Sliedregt, E. (2025). The future of international criminal justice is corporate. *Journal of International Criminal Justice*, *00*, 1–10. mqaf004. https://doi.org/10.1093/jicj/mqaf004
37. Spadaro, P. A. (2020). Climate change, environmental terrorism, eco-terrorism and emerging threats. *Journal of Strategic Security*, *13*(4), 58–80. https://doi.org/10.5038/1944-0472.13.4.1869
38. United Nations Counter-Terrorism Committee Executive Directorate (CTED). (2022, January). *The state of international cooperation for lawful access to digital evidence: Research perspectives* (CTED Trends Report). Germany.
39. United Nations Development Programme (UNDP). (2020). *The climate security nexus and the prevention of violent extremism: Working at the intersection of major development challenges* (Policy Brief).