World Research of Political Science Journal
An International Journal

http://dx.doi.org/10.18576 /WRPSJ/070202

Cyberterrorism: a New Form of Terror, a Misunderstood Crime or a Free-Pass for Privacy Invasion? Morocco as a Case of Study

Nada Naji *

Department. of Humanities and Social Sciences, Sidi Mohamed Ben Abdellah University, Fez - Kingdom of Morocco.

Received: 1 Jul. 2024; Revised: 12 Aug. 2024; Accepted: 25 Sep. 2024.
Published online: 1 Dec. 2024.

Abstract : The phenomenon of cyberterrorism remains a contentious topic among scholars, with ongoing debates regarding its very existence. Questions arise as to whether cyberterrorism constitutes a distinct crime or if it is merely an exaggerated and politically manipulated form of cybercrime. This discourse introduces several critical issues, the first being the challenge of defining terrorism itself, a concern that has persisted since the inception of the term. Additionally, there exists a significant distinction between cyberterrorism and cybercrime, necessitating a clear understanding of the boundaries that separate the two. Another pressing inquiry involves evaluating the potential threats posed by cyberterrorism and the ramifications of cyber attacks. Furthermore, the discourse extends to the realm of human rights in the digital landscape, particularly in light of governmental initiatives aimed at enhancing cybersecurity. Numerous scholars have explored these complex questions, including Michael Stohl, who has examined the definitional ambiguities between cyberterrorism and cybercrime , and Gabriel Weimann, who has focused on assessing the threats associated with cyberterrorism . This paper will conduct a case study of the Kingdom of Morocco, analyzing the definitions it employs for terms such as "Terrorism", "cyberterrorism", "cybercrime", and "cybersecurity ". The analysis will delve into the limitations inherent in each definition before evaluating the counter-cyberterrorism measures implemented, assessing their significance, effectiveness, and the potential for unintended consequences stemming from the adopted policies.

Keywords: Cyberterrorism, Cybercrime, Cybersecurity, Morocco, Counter-terrorism.

Introduction

The concept of terrorism has been the subject of numerous attempts over the years to establish a universally accepted definition; however, these endeavors have largely proven unsuccessful. Different nations, organizations, and treaties adopt their own interpretations of terrorism. For example, U.S. law delineates between "international terrorism", which occurs beyond the borders of the United States, and "domestic terrorism", which transpires within its borders. Additionally, it distinguishes "acts of war", which may include declared wars, where terrorism is characterized as a violent act that endangers human life and aims to intimidate or coerce civilian populations, influence governmental policy through fear, or disrupt governmental operations via mass destruction, assassination, or kidnapping. Furthermore, it differentiates between armed conflicts, regardless of whether a formal declaration of war has been made, and engagements involving military forces.[1]The Moroccan law in the other hand, is not very different than the French one[2] in definition nor in the punishments.

Following the terrorist attack in Casablanca, Morocco, on May 16, 2003, the nation initiated a comprehensive approach to counter-terrorism. This strategy encompasses the enhancement of security forces, the establishment of legislative frameworks, educational and religious reforms, and initiatives aimed at human development.

1 U.S code, 18 USC 2331 : Definitions, January 17,2023

2 Code pénal, livre IV : Des crimes et délits contre la nation, l'Etat et la paix publique, Titre II : Du terrorisme, 421-1,421-2, 421-2-1.

* Corresponding author E-mail:

© 2024 AAU.

The legislative aspect of this strategy commenced with the introduction of "law 03-03"3 on May 28, 2003. Subsequently, adjustments were made through "law 86.14" in 20154, which not only clarified the definition of terrorist acts and established mechanisms for the prosecution of terrorists but also addressed the financing of terrorism, hate speech, and the preemptive prosecution of individuals based on gathered evidence.

Within Moroccan legislation, there is an absence of a precise definition of terrorism; instead, various scenarios are identified as acts of terror. Article 218-1 outlines these instances, providing a framework for understanding what constitutes terrorism in the legal context. we read:

"The following crimes are considered terrorism acts if they are intentionally related to an individual or group project intending to put the public order in danger through fear, intimidation or violence:

"1-Intentional assault on a person's life, safety or freedoms, or their abduction or detention.

2- Falsification or forgery of money or public loan bonds, falsification of State seals, hallmarks,stamps, and marks, forgery or falsification provided for in chapters 360, 361 and 362 of this Act;

3- Vandalism, defacement or damage;

4- The diversion or destruction of aircraft, vessels or any other means of transport, the destruction of air, sea or land navigation installations, or the defacement, sabotage or destruction of means of communication;

5-Theft and extraction of funds;

6-Manufacture, possession, transfer, promotion or use of weapons, explosives or ammunition contrary to the law;

7-Offences relating to automated data processing systems;

8-Forgery or falsification of cheques or any other means of performance referred to respectively in articles 316 and 331 of the Trade Code;

9-The formation of a gang or agreement for the preparation or commission of an act of terrorism;

10-Concealment of items obtained from a terrorist offense with knowledge of this. "[5]

Subsequently, the legislation also identifies additional forms of terrorism related to the contamination of air, water, and land with hazardous substances that pose risks to human health and the environment. It further addresses issues such as hate speech, incitement to violence, and the financing of terrorism, including any direct or indirect assistance in criminal activities. For example, we observe:

"Two to six years' imprisonment and a fine of between 10.000 MAD and 200,000 MAD shall be imposed on anyone who commends acts that constitute a terrorist crime by means of speech, shouts or threats whether uttered at public places or meetings or by means of books and publications sold, distributed, offered for sale in public places or meetings or through displayed flyers for the public to see, in the different media forms whether audio, visual or electronic."[6]

The absence of a universally accepted definition of "terrorism" has led to heightened discourse surrounding the concept of "cyberterrorism". While some scholars continue to question the existence of cyberterrorism, others have sought to articulate a definition and categorize its different forms. A widely recognized definition goes as follows: "any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure."[7] Or as follows: "cyberterrorism can be defined as electronic attacks from cyberspace from both the internal and external networks, particularly from the Internet that emanate

3 Royal Decree 1-03-140, Rabii the first 26, 1424 Hijra, May 28th, 2003, to put into force the law 03-03 regarding counter-terrorism (Arabic)

4 Law 86.14, , Official Gazette Issue 6365, June 1st 2015,P: 5490 (Arabic): http://www.sgg.gov.ma/BO/Ar/2015/BO_6365_Ar.pdf

5 Royal Decree 1-03-140, Rabii the first 26, 1424 Hijra, May 28th, 2003, to put into force the law 03-03 regarding counter-terrorism (Arabic)

6 Article2-218 of the royal Decree 1-03-140, May 28th 2003. Arabic

7 Robert Sheldon and Katie Terrell Hanna, Cyberterrorism, TechTarget, Security.
https://www.techtarget.com/searchsecurity/definition/cyberterrorism

© 2024 AAU.

from various terrorist sources with different set of motivations and are directed at a particular target"[8]

Terrorist attacks are put in five types: Incursion, destruction, disinformation, denial of service and defacement of websites. And just like all acts of terrorism, the motivations for cyberterrorism can be summarized as follows:

1-To destroy the enemy's operational capabilities.

2-To demonstrate their capabilities of causing harm to their followers.

3- To cause intimidation, destruction or disruption.

4-To harm the reputation of the enemy be it a nation, an organization or other.

Morocco and cyberterrorism:

The Moroccan legal framework explicitly identifies "automated data processing systems" and "electronic" devices, indicating that the Moroccan government has been vigilant regarding the digital landscape, cybernetics, and the potential criminal activities associated with these domains since 2003. Furthermore, it has categorized such activities within the realm of terrorism, despite the existence of a dedicated department focused on cybercrimes in Morocco.

To elaborate on this matter further and to ensure the prohibition of hate speech in compliance with legal standards while safeguarding press freedom and freedom of expression, the Moroccan legislation enacted in 2016, specifically law 88.13 regarding press and publications, has denounced any incitement to discrimination, hatred, violence, or criminal acts in any form of publication, whether printed or digital[9]. Additionally, this law delineates a comprehensive list of offenses applicable to both printed and online media.

"-Direct incitement to commit crimes related to murder, infringement of a person's physical integrity, terrorism, theft or subversion;

- Commending war crimes, crimes against humanity, genocide or terrorist crimes;
- Direct incitement to hatred or discrimination."[10]

The body of laws in Morocco indicates that there is no differentiation made between offenses perpetrated in the physical realm and those executed in the digital sphere. The legislation focuses on the nature of the crime itself rather than the medium through which it is committed, thereby applying a generalized approach. Actions deemed criminal in the physical world are equally classified as such in the online environment, subject to the same legal frameworks and repercussions, irrespective of whether the Moroccan Kingdom is the victim or another nation. Additionally, in the context of terrorism, Moroccan law extends its scope beyond merely penalizing the act itself to encompass the criminalization of the intent to engage in terrorist activities, as elaborated in the provisions concerning terrorism-related offenses.

"Receiving or attempting to receive a coaching or training, whatever its form, type or duration, within or outside the Kingdom of Morocco, for the purpose of committing a terrorist act within or outside the Kingdom, whether or not the said act occurred."[11]

The existence of various legal frameworks can complicate the determination of sentences in specific cases, as the penalties differ significantly from one set of laws to another. For example, in the context of hate speech offenses, the terrorism legislation prescribes a prison term ranging from two to six years, along with fines that vary between 10,000 MAD and 200,000 MAD. In contrast, the Press and Media Law imposes fines that range from 100,000 MAD to 500,000 MAD but does not mandate any imprisonment for the same offense.

8 Shamsuddin Abdul Jalil, Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, GIAC Security Essentials Certification (GSEC), June 2003, p: 4 (pdf)

https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154#:~:text=There%20are%20five%20main%20types,others%20and%20have%20different%20objectives.

9 "General Texts", Part Three – Penalties – On the Special Protection of Certain Rights, the Jurisdiction of Courts, and the Procedures Followed Before Them – Title One – On the Special Protection of Certain Rights – Section One – Protection of Public Order – Official Gazette, Issue 6491, 11th of Dhu al-Qi'dah 1437, August 15, 2016, p. 5977

Ibid, P :5978. Arabic10

11 218-1-1, Official Gazette, Issue 6365, p. 5490

© 2024 AAU.

The process by which judges navigate these legal frameworks involves assessing the individual's status as a journalist and determining whether the hate speech in question has resulted in actual violence. However, the complexities increase significantly within the realm of human rights, particularly concerning issues related to the internet.

Morocco from counter-terrorism to counter- cyberterrorism:

In the realm of counter-terrorism, Morocco has implemented a multifaceted approach since 2003, which encompasses not only legislative measures but also the establishment of a proficient investigative bureau and specialized counter-terrorism units within its security and military frameworks. A significant aspect of this strategy has been the rehabilitation of the religious sector, achieved through the creation of a structured environment for various religious institutions and authorities, including mosques and imams. This initiative involves the training of religious leaders and guides, the empowerment of women to participate in religious guidance roles, the prohibition of hate speech within mosques, and the banning of unauthorized home mosques[12]. Such measures have not only institutionalized the religious sector but have also enhanced the ability to monitor and regulate religious discourse, thereby mitigating the potential for extremist ideologies to proliferate.

Given that Islam is the predominant religion in Morocco, it is taught in both public schools and specialized religious institutions. Fortunately, the authorities quickly recognized that the instruction provided was not consistently moderate and did not always align with the national interpretation of Islam. As a result, the country initiated a gradual reform of its educational system, developing a new curriculum for schools and establishing a structured framework for traditional religious schools. Significant revisions to the curriculum occurred in 2017, during which numerous chapters containing violent verses were removed.

Furthermore, Morocco noticed that the social and economic situation had a role in extremism and therefore started the “national initiative for human development” in three stages (from 2005 to 2010, from 2011 to 2018, and from 2019 to 2023), aiming to improve the social and economic status of the people, with an emphasis on rural areas, youth, women and people with special needs[13].

This extensive approach was formulated to confront "terrorism" as a global threat and has reliably proven its efficacy since its establishment. In the context of cyberterrorism, Morocco perceives it as a dual phenomenon, categorizing it as both a form of cybercrime and a type of terrorism. It is regarded as terrorism in terms of its underlying motivations and legal frameworks, while simultaneously being classified as cybercrime concerning the strategies implemented to combat it.

Recognizing the threats posed by cybercrime, Morocco has implemented a national cybersecurity and information systems, and aside several regulations such as Law 53-05 regarding electronic exchange of legal data and Law 09-08 regarding automated processing of personal data as well as the ratification of many international conventions on fighting cybercrime and terrorism via technological means of communications, such as the Budapest Convention on Cybercrime[14] as well as the followed protocols regarding the matter on 2022[15].In its legal framework, Morocco distinguishes between two categories of cybercrimes: those that are directly associated with computer systems and data protection, and those that, while occurring in cyberspace, pertain to traditional offenses such as forgery, falsification, sexual harassment, and intimidation.

The Kingdom of Morocco has also chosen to establish a variety of organizations that specialize in this area, among which are:

- Regional laboratories dedicated to digital and anti-cybercrime trace analysis operate under the auspices of the Moroccan Directorate General for National Security (DGSN).
- The General Directorate for Information Systems’ security (DGSSI): Attached to the national defense administration of the kingdom of Morocco, the General Directorate for Information Systems’ security was created in

12 Royal Decree No. 1.03.193, December 4, 2003, concerning the Competencies and Organization of the Ministry of Endowments and Islamic Affairs, Official Gazette Issue 5172, December 25, 2003

http://www.indh.ma/ : 13 The official web site of the national initiative for human development

14 Youssef BENTALEB, Fighting Cybercrime in Morocco: Achievements and Some Challenges, CYBERCRIME, January 9th, 2017. https://incyber.org/en/fighting-cybercrime-in-morocco-achievements-and-some-challenges-by-prof-youssef-bentaleb-moroccan-centre-for-polytechnic-research-and-innovation/

15 الجريمة إلكترونية.. المغرب يوقع على بروتوكول دولي لمحاربتها، تيل كيل عربي، 13 مايو 2022م https://ar.telquel.ma/الجريمة-إلكترونية-المغرب-يوقع-على-برو

© 2024 AAU.

2011, by Decree number 2-11-509. The DGSSI has many responsibilities, among which we can cite: the coordination between inter-ministries works related to the elaboration and execution of the state's information systems' security strategies and for the organization of trainings and awareness campaigns for the benefit of the

personnel of public administrations and organisms. In addition, the DGSSI makes sure that all the directives of the strategic committee are followed and ensures the certification of electronic signatures. It also makes sure that the technologies used are up to date, and develops the necessary security systems for the public administrations and organisms[16]. The DGSSI has four centers/directorates: Directorate of strategies and regulation (DSR), Directorate of Assistance, training, monitoring and expertise (DAFCE), Directorate of secured information systems (DSIS), and Directorate of management of the monitoring center, detection and response to computer attacks (maCERT). Each directorate has many specialized divisions.

Protection of individual's privacy and of personal data while fighting cybercrime:

Similar to other nations engaged in the battle against cybercrime, the Moroccan government encounters significant scrutiny and criticism from its civil society, which expresses concerns that the strategies implemented to combat cybercrime may precipitate human rights violations, particularly regarding online freedom of expression and data privacy. To alleviate these apprehensions, Morocco has initiated the formation of a national commission dedicated to safeguarding personal data. Additionally, the government has prioritized educational initiatives, training programs, and awareness campaigns aimed at cultivating a populace that is not only well-versed in media and cyber issues but also capable of recognizing and mitigating cyber threats. This approach is intended to empower current and future generations, fostering a culture of knowledge dissemination and expertise in the domain. Among the various initiatives undertaken, one can identify:

- The National Commission for the Monitoring of Personal Data Protection (CNDP) was established under law No. 09-08, enacted on February 18, 2009, which addresses the safeguarding of individuals in relation to the processing of personal data. The primary function of the CNDP is to ensure that the processing of personal data adheres to legal standards and does not violate privacy, individual freedoms, or fundamental human rights. The Commission is comprised of a president and six members, all of whom are appointed for a term of five years, with the possibility of a single renewal. Its members are distinguished individuals recognized for their impartiality, ethical standards, and expertise in legal, judicial, and information technology domains. The president is appointed by His Majesty the King of Morocco, while the six members are also selected by His Majesty based on a proposal[17].
- Morocco Cyber confidence space : Serves as a digital platform where individuals in Morocco can access a wide array of documents related to cybercrime, alongside various initiatives aimed at combating issues such as violence, hate speech, and sexual harassment online. This portal equips users with essential tools and guidance to safeguard themselves, their children, and others they may encounter on the internet. Additionally, it allows citizens to report cybercrime incidents anonymously and request the removal of harmful content. By utilizing this platform, users can acquire valuable information to educate themselves and others, thereby actively participating in the fight against cybercrime through the principle of "see something, say something". The active engagement of citizens in this endeavor transforms them into defenders of the internet, fostering a sense of accountability in their online activities and promoting a spirit of civic duty in their efforts to prevent cybercrime.[18]
- Several training opportunities in cybersecurity out of which we can cite:

    - School 1337: A well-equipped coding school. It represents a unique educational model characterized by its comprehensive resources, devoid of traditional educators, tuition fees, formal classes, and rigid schedules. This institution allows students to access its facilities at any time, day or night, throughout the week, fostering an environment of self-directed learning. Students are encouraged to engage in peer-to-peer learning and participate in professional training sessions to enhance their skills and expertise. Established in Khouribga in 2018, School 1337 has since expanded to include campuses in Ben Guerir and Tetouan, with plans for further expansion as it continues to attract a growing number of students annually. These individuals are seen as having the potential to become future leaders in the digital realm and essential contributors to national cybersecurity, as coding is increasingly recognized as a vital tool in the modern internet landscape.[19]

16 For more information about the DGSSI: https://www.dgssi.gov.ma/fr/presentation/dgssi/presentation-missions.html

17 For more information visit the official website of the CNDP at: https://www.cndp.ma/fr/

18 To learn more about Morocco's Cyberconfidence space please see the official website: https://cyberconfiance.ma/ar/

19 For more information visit the official website of 1337 school: https://1337.ma/en/

© 2024 AAU.

- The National Agency for Telecommunications Regulation (ANRT) Awareness programs: "the Moroccan Centre for Polytechnic Research and Innovation (CMRPI), under the aegis of the Moroccan Ministry of Industry, Commerce, Investment and Digital Economy, has implemented a broad four-year awareness-raising campaign: the Moroccan National Campaign to Fight Cybercrime (CNLCC 2014-2017). This campaign is the first such experiment of its scale in Africa. Its objective is to establish a culture of secure use and good cybersecurity practice in Moroccan society. It targets the public and private sectors as well as citizens belonging to different age groups."[20] These campaigns collaborate with experts in the field as well as universities in order to raise the public awareness through workshops and trainings aiming to fight cybercrime. This will lead to a more media-educated public, cybersecurity literacy, and potentially to future cybercrime fighters[21].

Conclusion: is it enough?

Despite the extensive measures implemented, the Kingdom of Morocco continues to experience a persistent increase in the rate of cybercrime, correlating with the growing utilization of cyberspace. The official annual report from the Presidency of the Public Prosecution for the year 2021, released on January 2, 2023, indicates that Morocco recorded a total of 26 cases in appeal courts, resulting in the sentencing of 72 individuals, alongside 167 cases in trial courts, where 310 individuals were sentenced for offenses related to automated information processing systems in 2021 alone. This data reflects an approximate 43 percent rise in the number of cybercrime cases compared to 2020, which had 117 cases, and a 30 percent increase in the number of individuals sentenced. The majority of the cases in 2021 can be attributed to:
-Access or trying to access to automated processing systems (92 cases/150 person)
-Access or Staying in an automated processing system causing deletion or manipulation in the data or harm to the system (17 cases/41 person)
-Input, deletion or destruction of data in an automated processing system (20 cases/ 26 person).
- Access or Staying in an automated processing system supposed to contain information about security (4 cases/ 23 person).

As for the public order crimes committed through informatics, there has been in 2021 alone 623 cases in which 739 person have been sentenced, and thus a 42 per cent of raise in number or cases compared to 2020 (438 case), and of 48 per cent raise in number of people sentenced (498 in 2020). Most of the cases relate to these crimes in 2021 were about:
-Obtaining an amount of money through threat to divulge secrets or spread outrageous matters (286 case, 331 person).
-Sexual harassment through the phone or electronic texts, or recordings or photos (190 case/204 person).
-Fraud through the internet (103 case/135 person).

The significant increase in cybercrime statistics may initially appear concerning; however, when these figures are juxtaposed with analogous incidents occurring outside the digital realm, they become more palatable. Furthermore, when analyzed in relation to the overall escalation of similar offenses, it becomes evident that cybercrime merely mirrors the broader crime trends within the nation. This uptick in criminal activity is not solely a domestic issue but has also emerged as a global challenge, exacerbated by the economic downturn and psychological stressors stemming from the COVID-19 pandemic, as well as the rapid transformations within economic and social landscapes. Although the prevalence and severity of both general and cybercrime in Morocco remain relatively low compared to other nations—thanks in part to legislative and security measures—the increase in criminal activities necessitates a comprehensive examination from various angles, including psychological, political, economic, and social perspectives. Each sector must actively engage in efforts to mitigate the emergence of new criminal behaviors.

Declaration of interest statement:
No conflict of interest to declare.

References

[1] Code pénal, livre IV : Des crimes et délits contre la nation, l'Etat et la paix publique, Titre II : Du terrorisme, 421-1,421-2, 421-2-1.
[2] Gabriel Weimann, Cyberterrorism: how real is the threat?, United states institute of peace, special report 119, December 2004.

20 Youssef BENTALEB, Fighting Cybercrime in Morocco: Achievements and Some Challenges.

21 In order to learn more about the initiative see:CYBER SECURITY: NATIONAL CAMPAIGN TO FIGHT CYBERCRIME, Moroccan Ministry for industry and trade :https://www.mcinet.gov.ma/en/content/cyber-security-national-campaign-fight-cybercrime

© 2024 AAU.

[3] General Texts", Part Three – Penalties – On the Special Protection of Certain Rights, the Jurisdiction of Courts, and the Procedures Followed Before Them – Title One – On the Special Protection of Certain Rights – Section One – Protection of Public Order – Official Gazette, Issue 6491, 11th of Dhu al-Qi'dah 1437, August 15, 2016, p. 5977
[4] Law 86.14, Official Gazette Issue 6365, June 1st 2015 (Arabic)
[5] Michael Stohl, Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?, Crime, Law and Social Change Volume: 46 Issue: 4-5, 2006
[6] Robert Sheldon and Katie Terrell Hanna, Cyberterrorism, TechTarget, Security.
https://www.techtarget.com/searchsecurity/definition/cyberterrorism
[7] Royal Decree No. 1.03.193, December 4, 2003, concerning the Competencies and Organization of the Ministry of Endowments and Islamic Affairs, Official Gazette Issue 5172, December 25, 2003
[7] Royal Decree No. 1.03.140, Rabii the first 26, 1424 Hijra, May 28th, 2003, to put into force the law 03-03 regarding counter-terrorism (Arabic)
[8] Shamsuddin Abdul Jalil, Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, GIAC Security Essentials Certification (GSEC), June 2003(pdf) :
https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154#:~:text=There%20are%20five%20main%20types,others%20and%20have%20different%20objectives.
[9] The official web site of the national initiative for human development :
http://www.indh.ma/
[10] U.S code, 18 USC 2331 : Definitions, January 17,2023
[11] Youssef BENTALEB, Fighting Cybercrime in Morocco: Achievements and Some Challenges, CYBERCRIME, January 9th, 2017.
https://incyber.org/en/fighting-cybercrime-in-morocco-achievements-and-some-challenges-by-prof-youssef-bentaleb-moroccan-centre-for-polytechnic-research-and-innovation/D9%8A%D9%88%D9%82%D8%B9-%D8%B9%D9%84%D9%89-%D8%A8%D8%B1%D9%88/
[12] الجريمة إلكترونية.. المغرب يوقع على بروتوكول دولي لمحاربتها، تيل كيل عربي، 13 مايو 2022م
https://ar.telquel.ma/بروتوكول-على-يوقع-المغرب-إلكترونية-الجريمة

© 2024 AAU.