

Vol.1 • 2025

ISSN. 1307 - 9190



# Defence Against Terrorism Review

Terrorism and Combating Terrorism Methods; Military Operations and Strategic Communication Models  
**Halil Sıddık AYHAN**

Strengthening Public Health Responses to Terrorism: Early Warning Systems and Health Care Preparedness  
**Dr. Verda TUNALIGİL- Ercan ÇİTLİOĞLU**

New Era New Challenges: Web3-Based Social Media and Terrorism  
**Dr. Onur CERAN**

Türkiye's Security Assistance to Somalia and Its Implications for Somalian Counterterrorism Efforts  
**Nebahat TANRIVERDİ YAŞAR**

D  
A  
T  
R

**COE-DAT**

Centre of Excellence Defence Against Terrorism



**Owner**

Halil Siddik Ayhan, COEDAT Director

**Coordinator**

Ahmet Erol, Chief of Staff, COEDAT

**Editor-in-Chief**

Prof. Dr. Oktay Tanrısever, Middle East Technical University

**Editor of COE-DAT**

Müge Memişoğlu Akar, Terrorism Subject Matter Expert,  
COEDAT

**Copy Editor**

Stephen Harley, Freelance Researcher

**Editorial Board**

Prof. Dr. Gökhan Ögünç, Gendarmerie and Coast Guard  
Academy

Prof. Dr. Mitat Çelikpala, Kadir Has University

Prof. Dr. Mustafa Kibaroğlu, MEF University

Prof. Dr. Sarah Leonard, South Wales University

Doç. Dr. Efe Tokdemir, Bilkent University

Doç. Dr. Osman Şen, National Defence University

**Advisory Committee**

Prof. Dr. Genker Korhan Demir, Hasan Kalyoncu University

Prof. Dr. Birgül Demirtaş, Turkish – German University

Doç. Dr. Rıza Bayrak, Middle Tennessee State University

Doç. Dr. Emrah Özdemir, National Defence University

Doç. Dr. Serkan Yenal, National Defence University

Doç. Dr. Sıtkı Egeli, İzmir Economy University

*DATR is an international peer-reviewed journal*

*DATR is a product of the Centre of Excellence-Defence  
Against Terrorism (COE-DAT).*

*It is produced for NATO, NATO member countries, NATO  
partners, related private and public institutions and related  
individuals. It does not represent the opinions or policies  
of NATO or COE-DAT. The views presented in articles are  
those of the authors.*

© All rights reserved by the Centre of Excellence-Defence  
Against Terrorism

**Sahibi**

Halil Sıddık Ayhan, TMMM Komutanı

**Yazı İşleri Müdürü**

Ahmet Erol, Kurmay Başkanı, TMMM

**Editör**

Prof. Dr. Oktay Tanrısever, Orta Doğu Teknik Üniversitesi

**Editör Yardımcısı**

Müge Memişoğlu Akar, Uluslararası İlişkiler Uzmanı, TMMM

**İngilizce Editörü**

Stephen Harley, Bağımsız Araştırmacı

**Yayın Kurulu**

Prof. Dr. Gökhan Ögünç, Jandarma Sahil Güvenlik Akademisi

Prof. Dr. Mitat Çelikpala, Kadir Has Üniversitesi

Prof. Dr. Mustafa Kibaroğlu, MEF Üniversitesi

Prof. Dr. Sarah Leonard, South Wales Üniversitesi

Doç. Dr. Efe Tokdemir, Bilkent Üniversitesi

Doç. Dr. Osman Şen, Milli Savunma Üniversitesi

**Danışma Kurulu**

Prof. Dr. Cenker Korhan Demir, Hasan Kalyoncu Üniversitesi

Prof. Dr. Birgül Demirtaş, Türk Alman Üniversitesi

Doç. Dr. Rıza Bayrak, Middle Tennessee Devlet Üniversitesi

Doç. Dr. Emrah Özdemir, Milli Savunma Üniversitesi

Doç. Dr. Serkan Yenal, Milli Savunma Üniversitesi

Doç. Dr. Sıtkı Egeli, İzmir Ekonomi Üniversitesi

*DATR dergisi uluslararası hakemli bir dergidir.*

*DATR dergisi Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)'ne ait bir yayındır. NATO, NATO Üye Ülkeleri, NATO Ortaklık Ülkeleri, ilgili özel kuruluşlar ile kamu kurumları ve ilgili kişilerin kullanımı için hazırlanmaktadır.*

*DATR dergisinde yayınlanan yazılarda belirtilen fikirler yalnızca yazarına/yazarlarına aittir; TMMM'yi, NATO'yu ve NATO'nun fikir ve politikalarını temsil etmez, bağlamaz.*

© Tüm hakları saklıdır.

Yayın Sahibi: Halil Sıddık Ayhan

Sorumlu Yazı İşleri Müdürü: Ahmet Erol

Yayın Türü: Yerel Süreli Yayın

Yayın Şekli: Yıllık İngilizce

Defence Against Terrorism Review – DATR

Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)

Devlet Mahallesi İnönü Bulvarı

Kıralıdere Caddesi No:65 06582

Çankaya/ANKARA

Tel: 0 (312) 425 8215

Faks: 0 (312) 425 6489

E-posta: datr@coedat.nato.int

Baskı: Başkent Klşe Matbaacılık

Bayındır Sokak No: 30/E

Kızılay/ANKARA

Basım Tarihi: Mart 2025

# Defence Against Terrorism Review DATR

Vol. 1, 2025

ISSN. 1307-9190

## CONTENT

Editor's Note .....	5
Terrorism and Combating Terrorism Methods; Military Operations and Strategic Communication Models .....	7
<i>Halil Siddık AYHAN</i>	
Strengthening Public Health Responses to Terrorism: Early Warning Systems and Health Care Preparedness .....	21
<i>Dr. Verda TUNALIGİL - Ercan ÇİTLİOĞLU</i>	
New Era New Challenges: Web3-Based Social Media and Terrorism .....	51
<i>Dr. Onur CERAN</i>	
Türkiye's Security Assistance to Somalia and Its Implications for Somalian Counterterrorism Efforts .....	79
<i>Nebahat TANRIVERDİ YAŞAR</i>	
Publishing Principles .....	97

*The Defence Against Terrorism Review (DATR) is calling for papers for coming issues. The DATR focuses on terrorism and counterterrorism. All of the articles sent to DATR undergo a peer-review process before publication. For further information please contact [datr@coedat.nato.int](mailto:datr@coedat.nato.int)*

*Editor's Note*

Dear Defence Against Terrorism Review (DATR) Readers,

As one of the key publications of the Centre of Excellence-Defence Against Terrorism (COE-DAT), Defence Against Terrorism Review (DATR) publishes well-researched articles with reliable information and practical recommendations. As part of its mission to make contribution to the counter-terrorism efforts of NATO as well as its members and partner nations, the COE-DAT is proud to present the first Volume of DATR 2025. This volume includes four insightful articles exploring various aspects of terrorism and effective ways of countering terrorism.

The first article of this volume is entitled as "Terrorism and Combating Terrorism Methods; Military Operations and Strategic Communication Models". It is authored by Halil Sıddık AYHAN, Director of COEDAT. In his noteworthy article, Halil Sıddık AYHAN explores Military Operations and Strategic Communication as important methods of countering terrorism. After providing a comprehensive conceptual framework for studying terrorism, he identifies several methods of combatting terrorism. The author evaluates the nature and effectiveness of military operations and strategic communication methods in the context of post-9/11 world. Halil Sıddık AYHAN concludes his noteworthy article by suggesting that counterterrorism strategies could be more effective when the "Military Force" and "Strategic Communication" models are employed as complementary methods.

The following article, is entitled "Strengthening Public Health Responses to Terrorism "Early Warning Systems and Health Care Preparedness". Its authors, Dr.Verda TUNALIGİL from Presidency of Disaster Health and Emergency Medical Services, Ministry of Health Directorate of İstanbul, Türkiye and Ercan ÇİTLİOĞLU, a prominent expert on terrorism from Başkent University, explore the emerging terrorist risks to public health systems as well as effective ways of enhancing the resilience of public health systems against terrorist threats. The article identifies emergency preparedness, epidemiological surveillance, and targeted training for health care providers and community leaders as key aspects of making public health systems more resilient against potential terrorist threats. In the concluding part of this article, Dr. Verda TUNALIGİL and Ercan ÇİTLİOĞLU make several practical and proactive recommendations for identifying and countering emerging terrorist threats to public health systems.

The next article is "Türkiye's Security Assistance to Somalia and Its Implications for Somalian Counterterrorism Efforts". In this article, Nebahat TANRIVERDİ YAŞAR, who is a researcher and a policy analyst, emphasizes Türkiye's contribution to enhancing the security capabilities of Somalia by providing training, supplying weapons, and fostering collaborations. The article also highlights the significance of Türkiye's Security Assistance to Somalia in combating the terrorist threats posed by Al-Shabaab and other terrorist

organizations. The study analyzes Türkiye's strategy of providing security assistance to Somalia in terms of the achievements, obstacles, and consequences of Türkiye's security cooperation with Somalia. In the article, Nebahat TANRIVERDİ YAŞAR proposes that NATO and other entities could benefit from Türkiye's security assistance framework, especially in harmonizing military support with capacity enhancement in vulnerable nations.

Final article of this volume "New Era New Challenges: Web3-Based Social Media and Terrorism" is authored by Dr.Onur CERAN from the IT Department of Gazi University. This article examines social media platforms by focusing on two aspects: first, the risks that they could be used by terrorist organizations, second, the effective ways of countering such risks in the rapidly developing digital world. The author explores the initiatives taken by social media platforms and governmental bodies in order to cope with various challenges including the use of social media platforms by terrorist organizations for disseminating terrorist propaganda. These measures include using algorithms, reporting mechanisms, strengthening legal structures, and developing partnerships. Nonetheless, as Dr.Onur CERAN claims, the advent of Web3 technologies, including blockchain-based decentralized platforms, creates new obstacles in the form of facilitating pseudonymous behaviour and complicating the process of content moderation. Thus, Dr.Onur CERAN concludes his article by highlighting the importance of developing creative approaches to counter-terrorism in order to tackle with the emerging cyber threats of the digital era.

We sincerely hope you enjoy the content of this volume, and we look forward to our next meeting in the next issue.

We wish to express our thanks to all authors and reviewers for their significant roles in this issue and encourage our readers to reach out with their insights and suggestions. DATR is committed to welcoming and fostering contributions from both military and civilian backgrounds.

Sincerely yours,

Prof. Dr Oktay F. Tanrısever

Editor-in-Chief



# Defence Against Terrorism Review DATR Magazine



DATR, 2025; 1 : 7-20

Electronic Online ISSN 1307 - 9190

## Terrorism and Combating Terrorism Methods; Military Operations and Strategic Communication Models

Halil Siddık AYHAN<sup>1</sup>

**Abstract:** *It can be argued that terrorism is a resort to violent and lethal acts by state or non-state actors in an organized, systematic and continuous manner in order to achieve political/economic/military superiority and to maximize their interests; against individuals/groups/communities and governments/states that do not agree with them or that do not belong to them, with the aim of creating fear and intimidation. Due to the different interpretations of terrorism, a common attitude towards terrorism, was not exhibited and the necessary importance was not given in international relations. However, particularly since the September 11 attacks, terrorism has expanded its area of interest and influence due to developing technology and international developments, With the spread of terrorism, which was previously perceived as a regional or national threat, to a global scale, the methods of combating terrorism have also changed significantly and transformations have occurred in various areas. In this study, after examining the concepts of terror and terrorism and mentioning the various methods of combating terrorism, military operations and strategic communication among those methods will be examined. .*

**Key Words:** *Terror, Terrorism, Combating Terrorism Methods, Use of Force, Military Operations, Strategic Communication*

---

<sup>1</sup> Colonel (TUR A), PhD Student in National Defense University, Alparslan Defense Sciences and National Security Institute and Director in NATO Centre of Excellence-Defence Against Terrorism, halil.ayhan@coedat.nato.int

## 1. Introduction

Terrorism, which aims to create an atmosphere of fear and terror in societies and has become a survival issue for states, is not a new phenomenon. Just as wars that started with sticks and stones evolved with technological and doctrinal developments, terrorism, which disregards human life due to its unchanging nature, has also expanded its area of interest and influence due to developing technology and the structure of international relations. Arguably, a transformation has emerged from the profile of low-intensity attacks and less educated terrorists who carry them out, to a profile of more educated, highly technologically equipped terrorists. Thanks to the economic structure and dissemination of information brought about by globalization, terrorist organizations have emerged on the world stage as an asymmetric power. These can more easily access all kinds of technological opportunities, organize more easily with means of communication, and are capable of carrying out sudden attacks on a variety of targets anywhere and at any time

Just as the phenomenon of terrorism has changed over time, the nature, dimension and scope of combating terrorism methods have also changed. The pre-9/11 counter-terrorism (CT) conjuncture of international cooperation, information (intelligence) sharing and joint counter-terrorism operations was limited, and the use of military force was at the forefront. This has evolved into the character of a global struggle within the framework of adapting to changing threats, particularly following the September 11 attacks.

In this study consisting of four sections, following the examination of the concept of terrorism, the second section will examine the comprehensive methods of combating terrorism with military, intelligence, political, economic and sociological dimensions put forward. The use of force, which includes the execution of military operations in order to neutralize terrorist organizations and eliminate their threats and ensure national security, is examined in the third section and strategic communication, which is carried out in order to provide public support, neutralize the propaganda of terrorist organizations and keep the morale of society high, is examined in the last section.

## 2. Terrorism

The word terror, originates from the Latin word “terrere” meaning to frighten, intimidate, or terrify (Başeren, 2008) and has entered all the world languages with its pronunciation as “terreur” in French and “terror” in English. Although the words terror and terrorism are often used in the same sense in the media and colloquially,

the term of terror is used in a very general approach to refer to a prolonged state of fear and horror, while the term of terrorism is used to refer to the strategy aimed at creating this terror environment (Caşın, 2008). In this respect, while terror means a state of violence, intimidation, fear and tyranny, we can define terrorism as the use of all forms of violence with the predominance of oppression and intimidation methods for political, economic, religious or ideological purposes, regardless of whether the person is a civilian or an official (Reçber, 2014, as cited in Nuhoğlu, 2022). In summary, we define terrorism as a conscious (not involuntary), planned, systematic, organized and politically motivated use of terror as a tool.

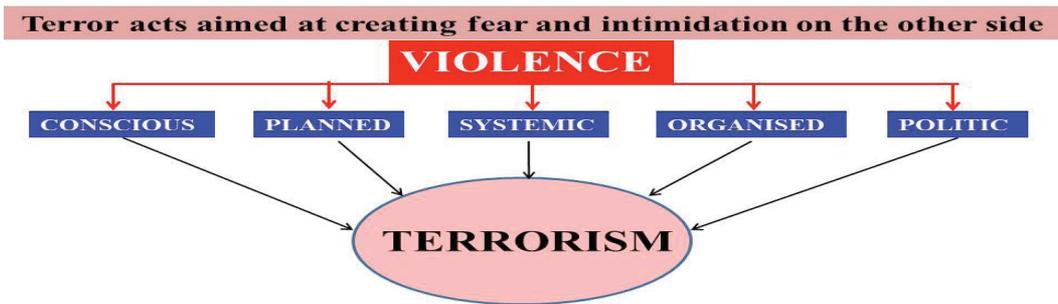


Figure 1. Conceptual Framework of Terrorism (Drawn by Author)

The definition of violence, the most important element of terrorism, includes verbal, emotional or sexual attacks beyond physical force (Özkan, 2017), and the element of violence is also used in individual crimes (deliberate murder, deprivation of liberty, intentional injury, looting and rape, etc.) and organized crime (extortion, money laundering, migrant smuggling, narcotics, arson, manslaughter, theft, fraud, loan sharking, prostitution, gambling, etc) (Gökbunar, 2014). However, terrorist organizations aim to instill fear in society through their acts of violence, create a sense of weariness and discouragement among the public, and undermine the trust of citizens in the state (Esentur, 2007). In this context, we can say that terrorism is designed to create an environment of extreme fear and chaos in society in which the victims are insignificant. Targeting diffuse broader targets that can be random or symbolic objects, including civilians, violates the norms/rules that regulate disputes, protests, and dissents, and influence the political behavior of governments, societies, or certain social groups for political purposes (Wilkinson, 2006).

When we look at the history of terrorism, the French Revolution, in which terrorism was used as a conscious (involuntary), planned, systematic, organized and politically motivated tool by the state against its citizens, whom it is obliged to

protect, can arguably be considered as the turning point of modern terrorism.

In classifying the historical evolution and development of modern terrorism following the French Revolution until today, the four waves (four distinct periods) theory (as seen in the Figure 2) developed by David C. Rapoport has been one of the most significant concepts in terrorism studies although it does not fully reflect the complexity and diversity of terrorism. In accordance with this model, within the framework of the first wave of terrorism (1880-1920), called the anarchist wave, terrorist acts were generally carried out by anarchist terrorists to achieve political goals. In the second period, called anti-colonialist terrorism, from the 1920s to the 1960s, terrorism was used in the form of independence movements and guerrilla wars. In the third wave, called the New Left or Marxist Wave, from the late 1960s to the 1980s, terrorist organizations generally carried out their actions in line with anti-state, anti-capitalist, and social transformation demands. Unlike these three waves dominated by anarchism, communism, self-determination and nationalism, the fourth wave of terrorism, which was influenced by religious factors that rose after the 1979 Iranian Revolution, is called Religious Radical Terrorism.

## Four Waves of Terrorism



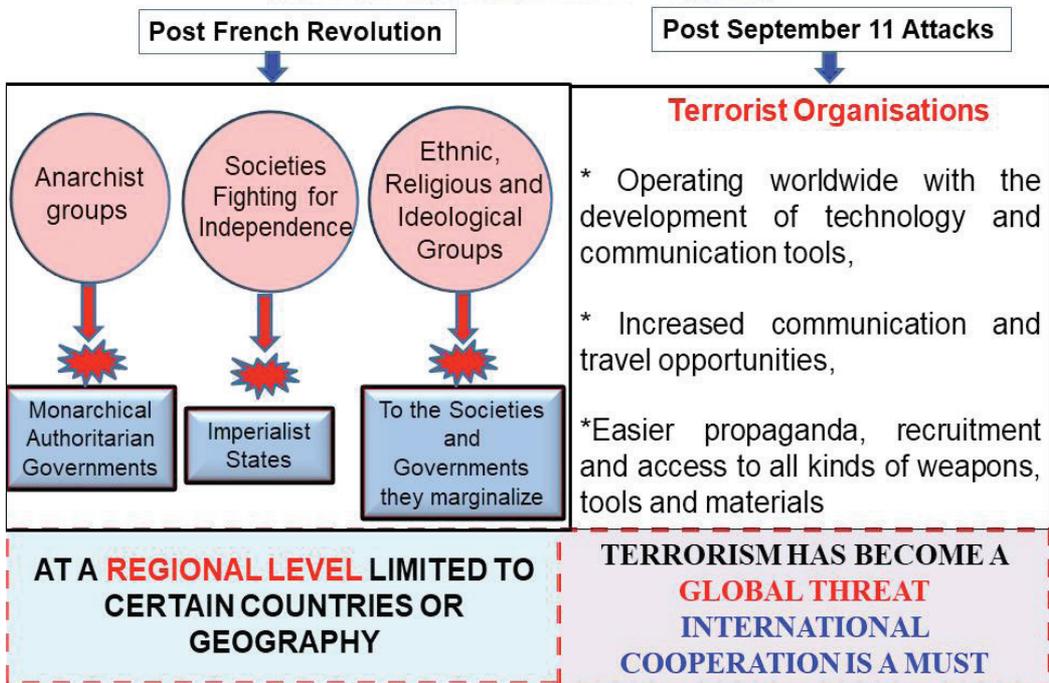
Figure 2. Four Waves of Modern Terrorism (Drawn by Author)

Although terrorism is a historical phenomenon as described above, the September 11 attacks on the twin towers in New York, representing the economic power of the United States, and the Pentagon, representing its military power, which resulted in the deaths of approximately 3,000 people, revealed the frightening level

of the lethal impact of terrorism, and for this reason, the September 11 attacks have been considered as a milestone of global terrorism.

In the post-Cold War era, and especially after the September 11 attacks, we have faced the fact that terrorism has become a movement which affects the entire world instead of having limited effects. A transformation has emerged from low-intensity attacks, the resulting panic and destruction, and the previously low-educated terrorist profile that carried it out, to a more educated and highly technologically equipped terrorist profile (Aydın, 2005). Criminal and terrorist organizations have shifted their areas of action from the national to the international level, using technological and informational opportunities to the maximum extent, and global terrorism presenting more of a threat than before has spread throughout the world, with terrorism becoming an asymmetric threat through globalization (Bal, 2006 cited in Aksu and Turhan, 2012) as explained in figure 3.

### Changing Scope and Character of Terrorism before and after 9/11 Attacks



*Figure 3. Changing Scope and Character of Terrorism Before and After 9/11 Attacks (Drawn by Author)*

### 3. Counter-Terrorism (CT) Methods

The Fight Against Terrorism (FAT), with terrorism defined as the organized, systematic and continuous use of terror, which is not a new type of action, whose most important element is violence and which indicates atrocity and fear, includes a wide range of measures with military, intelligence, political, economic and sociological dimensions. FAT or CT Methods have been implemented in various ways, with the aim of reducing or ending terrorist acts and increasing the security of society in different forms depending on the causes of terrorism (economic, social, political, religious and ideological), the structures, aims, fields of activity and objectives of terrorist groups, and the structure of the society, state and international environment as illustrated in figure 4.



Figure 4. Key Objectives in CT and factors that affect CT (Drawn by Author)

It can be argued that the systematic fight against terrorism, which aims to neutralize terrorist groups and prevent terrorist acts, started in the first half of the 20th century, when states took additional measures such as intelligence gathering, introducing legal measures, and establishing special units with an inclusive perspective, instead of traditional methods, in response to terrorist acts committed by anarchist groups in Europe.

On the other hand, the September 11 attacks revealed the frightening dimensions that terrorism has reached. With the influence and leadership of the United States, the perspectives of states and international organizations towards terrorism have changed, and the need for international cooperation in the fight against terrorism, which has become a priority, has emerged. Therefore, we can arguably consider the September 11 attacks as the end of national counter-terrorism strategy and the beginning of a new dynamic process that requires global cooperation in a wide range of areas from cybersecurity to intelligence sharing, and proactive measures that require rapid, comprehensive, tough and pre-emptive actions ahead of terrorist organizations.

In this context, the approaches and practices that were prevalent before September 11 in the FAT were;

- **The Criminal Justice Model:** A model that covers the process from the apprehension of terrorists to their prosecution and punishment, and from the execution of sentences to their reintegration into society after their release from prison, while preserving the democratic state and the rule of law (Kurum, 2023)
- **Non-Force Suppression Approach:** An approach that includes non-violent covert operations, depriving the organization of its financial resources, and economic sanctions against countries that support terrorism (Kurum)
- **Strategic Communication:** Gaining public support and raising public awareness by conveying the right messages, at the right time and through the right channels, creating social resistance by reducing the impact of terrorist propaganda, demonstrating the determination and power of the country in the fight against terrorism to the public and terrorist organizations
- **Conciliatory Approach:** Establishing relations with terrorists or terrorist organizations through dialogue, negotiation and diplomacy in order to prevent or resolve terrorist attacks

FAT models becoming widespread after September 11 included:

- **The use of Military Force Model:** Use of military force to eliminate the physical threat posed by terrorist organizations
- **International Cooperation Against Terrorism:** An approach built on basic parameters such as close inter-state cooperation and the active involvement of international organizations in FAT, implementation of effective international sanctions against actors supporting terrorism, establishment of legal infrastructure, ensuring tolerance among civilizations and combating radicalism (Semercioğlu, 2016)

- **Protective and Preventive Approach Against Terrorism:** The “pre-emptive strike” doctrine, which envisages carrying out an attack in advance in order to eliminate or neutralize a potential threat, as in the example of the operation carried out by the USA and the UK in 2003 upon the allegations that Iraq possessed weapons of mass destruction and supported terrorist groups. Or the “preventive strike” within the framework of a threat that has reached a certain stage (the threat element has started/completed preparations for the attack), as in the example of the air strikes carried out by the USA against the Taliban and Al Qaeda in Afghanistan.

Of course, although these approaches aim to generalize the methodology of counter-terrorism, it would be appropriate to proceed from the fact that the terrorist threat is not standardized in every geography and society. Therefore, CT should be handled within the framework of the unique conditions of the country/society exposed to the threat. In this study, the “Use of Military Force” and “Strategic Communication” models from the approaches mentioned will be analysed together with several case studies.

#### 4. Use of Force (Military Operations)

The use of the military force model, which involves domestic or international operations/actions by law enforcement forces, military units, and special units to neutralize targets such as terrorist groups’ leaders, members, operational and sheltering bases, training camps, logistics (weapons, ammunition, food, health supplies, etc.) centers, and supply points, is an effective method of restricting or destroying the operational/action capabilities of terrorist organizations. Within the framework of this model, military operations against the Liberation Tigers of Tamil Eelam (LTTE) organization and the Taliban are examined in the following sections.

In countering the Liberation Tigers of Tamil Eelam (LTTE)<sup>2</sup> organization, which was waging a violent struggle against the government to establish an independent state of Tamil Eelam in northwestern Sri Lanka, the Sri Lankan government adopted the use of the military force model and conducted extensive military operations to neutralize the organization. When the benefits of the approach within the framework of the military power model are analyzed at the most recent stage of this struggle, it can be seen that after the leader, headquarters and senior executives of the organization were killed in operations, the organization’s capacity for action was destroyed, civilian casualties were prevented and stability was achieved by ending

<sup>2</sup> LTTE terrorist organization officially declared its establishment in 1976. In 1983, it began its armed actions with an attack on a Sri Lankan army convoy in Jaffna, which resulted in the killing of 13 Sri Lankan army members.

the chaos that had been going on in the country for 26 years.

As a result of the external support it received, the LTTE became the first terrorist organization to possess aircraft, although not yet sufficient in capacity, in addition to specially trained land forces equipped with all kinds of modern equipment that can be found in advanced armies, including tanks, mortars, artillery, and anti-aircraft guns, and naval forces with sea vehicles and torpedoes that enabled it to conduct maritime and amphibious operations (Fontanellaz, 2025). Although the phenomenon of suicide bombing emerged elsewhere, the LTTE invented the suicide vest, used suicide bombers extensively, and killed former Indian Prime Minister Rajiv Gandhi and Sri Lankan Prime Minister Premadasa with suicide attacks. The LTTE carried out more than two hundred such suicide attacks.

The failure to achieve results in negotiations with the terrorist organization, which has claimed more than seventy thousand lives in its actions, had between 7,000 and 15,000 members and possessed the capabilities mentioned above, made the use of military force an inevitable course of action. Although this approach was successful in the case of Sri Lanka, with the neutralization of the LTTE after a long struggle of 26 years, it has been criticized for the number of civilian casualties and human rights violations. However, it can be argued that in the conjuncture where everything was legitimized under the war on terrorism following the September 11 attacks, criticisms regarding the model of using military force against terrorist acts and violent attacks of the LTTE remained weak.

As another example of the usage of military force in CT; in retaliation for the September 11<sup>th</sup> 2001 terrorist attacks that killed approximately 3,000 people, the US-led "Operation Enduring Freedom" (OEF), along with attacks of existing Afghan anti-Taliban forces -primarily comprising the loose coalition of Afghan groups called the Northern Alliance- (Background: "Operation Enduring Freedom, 2004"), against Al Qaeda and Taliban forces in Afghanistan. Control of the capital Kabul was achieved on November 13<sup>th</sup> 2001, with the final toppling of the regime in December effectively ending the Taliban era in Afghanistan. When we look at the results of the operation, which was carried out in a very short period of three months within the scope of the military force model; the Taliban regime was overthrown, the administration in Afghanistan was seized, the presence of the Al-Qaeda organization in Afghanistan was weakened, many of its leaders were captured or killed, the influence of the organization on the global terrorism network was reduced, and an interim government was established in Afghanistan.

In the first phase of its fight against terrorism in Afghanistan, the US stopped terrorist attacks with its rapid and effective use of military force, inflicted great damage on, and neutralized, the organization's leadership, manpower, logistics and

communications infrastructure, sent a deterrent message to terrorist organizations and the entire world by showing its overwhelming power, encouraged international cooperation with the successful operation it carried out, and also consolidated its hegemony.

However, the US, which responded harshly by using the war model (that is, military force), in the fight against terrorism, had to face the disadvantages as well as the advantages mentioned above. These drawbacks can be summarized as follows:

In accordance with Mary Kaldor's<sup>3</sup> thesis; that new wars differ from old wars in terms of actors, sphere of influence (local-global), purpose and methods, and that the logic of new wars, which have become complex, should be understood from a new perspective, and new methods should be developed, the successful operation carried out by the US in Afghanistan in a short period of time with its lethal air capabilities in the old war conjuncture, is almost completely different from the operation carried out by the US in the region after taking control of Afghanistan. This can be seen in the new war conjuncture, which includes many different dimensions such as training local forces, strengthening the administration, preventing external support and border control, economic support and international cooperation.

As Kaldor states, the US, which succeeded in Iraq and Afghanistan with military operations in a short period of time, did not succeed in building legitimate political authority in the subsequent phase, as it did in Japan and Germany after WW2, which is seen as the most important strategy in the new type of war (Kaldor, 2023, trans. Türközü). The increasing poverty, malnutrition, poor hygiene conditions and lack of access to health services due to the war also negatively affected the lives of Afghans and these casualties/injuries and the negative conditions brought about by the war caused anger in Afghan society and increased sympathy for the Taliban. All these adversities, along with the influence of the Taliban's propaganda, strengthened the resistance and facilitated the recruitment of new fighters to the organization. These fighters, consisting of civilian militias, terrorist organizations, religious or ethnic groups, united on the basis of ethnic or religious affiliation arguably fighting for the preservation of ethnic or religious identities, rather than traditional goals, such as gaining land or power, regained control in Afghanistan. Consequently, it has become clear that military intervention alone will not be enough to end terrorism, and that terrorism must be fought with a holistic perspective that includes diplomatic, economic, intelligence and social measures.

---

<sup>3</sup> The writer of "New and Old Wars: Organized Violence in a Global Era- New and Old Wars: Organized Violence in a Global Era (1999)" and who brought the term "new war" to academic literature.

## **5. Strategic Communication**

“Strategic Communication” in the fight against terrorism is the conveying of the necessary messages to the public and members of the organization by using print and visual media, social media, internet and other communication channels. These are utilised within the scope of breaking the motivation of terrorist organizations, preventing recruitment and ensuring the dissolution of the organization, isolating and delegitimizing the organization by neutralizing the propaganda of the terrorist organization, preventing the exploitation of terrorist propaganda by raising the awareness of the society and gaining its support, displaying a collective common stance of individuals against terrorism, and showing the determination and power of the state in the fight against terrorism to both the public and terrorist organizations.

The experience and success of the United States in influencing the states and societies in the Eastern Bloc as the defender of democracy and freedoms against totalitarian dictatorships within the framework of the containment strategy against the Soviet Union and communism during the Cold War, and in securing political support through the active use of the media in the First Gulf War, was also reflected in gaining the support of its own public opinion and the international community in the immediate aftermath of the September 11<sup>th</sup> attacks. Constantly prioritizing the attack on the twin towers and civilian casualties, the US carried out the operation in Afghanistan with the broad participation of the international community within the framework of terrorism, which it defined as its new enemy. In the aftermath of the operation, the US-led NATO coalition, in line with the principle of focusing on the hearts and minds of the people within the framework of strategic communication, made efforts to restructure the country and increase the legitimacy and dominance of the new government on the basis of a democratic regime and a free market economy. Within this scope, projects and practices were developed to establish a local civil administrative system and support development (Özdemir, 2021).

However, by carefully analyzing their target audiences, insurgent groups have outperformed the Government of Afghanistan and Coalition Forces in strategic communication through violent intimidation, taking advantage of their Pashtun identity and physical proximity to the population. In addition, the Afghan government’s inability to fight corruption, smuggling and poverty has strengthened the Taliban’s disinformation campaign. The insurgents waged a “silent war” of fear, intimidation and persuasion throughout the year, not just during the hot weather “fighting season” to gain control over the population, resulting in a Taliban “shadow government” that neutralized the government and traditional power structures and controlled the population. In addition, the Taliban, through its violent actions in support of its

strategic communications, not only demonstrated the central government's inability and weakness in providing security but also provoked the reaction of ISAF (International Security Assistance Force) troops, further alienating these forces from the population and weakening popular support (COMISAF Initial Assessment, 2009).

As a result, after a successful military operation, the United States and its allies, with an enormous armed power, had to leave the country in 2021 after a 20-year struggle, realizing that, as a result of faulty strategic communication, it was necessary to adopt approaches aimed at winning the people instead of policies disconnected from the people, that it was not possible to build a new state for the people of another country with technological means alone, and that law and order could not be established in the short term by relying on corrupt and unjust local forces (Güneş, 2021).

Following the terrorist attack in Paris in November 2015, the government's declaration of its determination to fight against terrorism in order to prevent fear and panic in society, and the message to French society that they are not alone in the fight against terrorism, with the unity march against terrorism in Paris by the heads of state and government from nearly fifty states within the framework of public diplomacy, have been successful examples of strategic communication. These have increased the capacity of the French people to cope with the threat of terrorism, support for the security forces and social solidarity.

However, in the aftermath of the Paris attack and other attacks in Europe, similar to the 9/11 attack, associating terrorism together with Islam and introducing the concept of the "other" has been a mistake in strategic communication. It is argued that as a result of this mistake, Muslim youth, who felt excluded, discriminated against and treated unfairly, and who held the governments of these countries and the discrimination they were subjected to responsible for their failures, tried to avenge themselves by joining the ranks of DAESH. As a result, the organization's violent acts in Europe and the recruitment to the organization from there turned into a mutually reinforcing cycle, and in parallel, discrimination and hatred against Muslims in Europe increased exponentially (Aktaş, 2017).

## **6. Conclusion**

Counter-terrorism methods carried out with the aim of achieving basic objectives such as reducing terrorist acts, preventing the activities of terrorists, increasing the security of society against terrorism, which is a multifaceted threat; are shaped within the framework of factors such as the structure of the terrorist

threat (international terrorism, domestic terrorism, foreign-supported terrorism, ethnic, religious, radical terrorism, etc.), principles of struggle (respect for human rights, protection of democratic values, compliance with legal restrictions, unlimited use of force, etc.), capabilities (military power, intelligence capabilities, financial resources, trained personnel, technology, etc.), principles of struggle (respect for human rights, protection of democratic values, respect for legal restrictions, unlimited use of force, etc.), capabilities (military power, intelligence capabilities, financial resources, trained personnel, technology, etc.), the state of society (unity and solidarity in society, spirit of solidarity, resistance of society, etc.), the legal infrastructure and framework, and the need or necessity for international coordination and cooperation.

In the fight against terrorism, which has evolved in line with the developments in the international political and security environment and changing technologies, the methods mentioned above- Criminal Justice Model, Suppression Approach without the Use of Force, Strategic Communication, Reconciliatory Approach, Use of Military Force Model, International Cooperation Against Terrorism, Protective and Preventive Approach Against Terrorism, have been used together or separately in interaction with the above-mentioned factors.

As seen in the “Use of Military Force” and “Strategic Communication” models examined with case studies, there is no standard recipe for success in the fight against terrorism, which has a complex and dynamic structure. However, if an evaluation is made on the basis of these two models, specific to the cases examined in this study; it is considered that the complementary and balanced use of the “Use of Military Force” model, which limits the activities of terrorists, and “Strategic Communication” model, which aims to reduce support for the terrorist organization and increase the spirit of resistance and solidarity of the society, will be the right approach.

As explained in this article, although terrorism is a historical phenomenon, for the first time in the 21st century, it has begun to carry the characteristics of an instrument of influence reaching extraordinary dimensions. Although the 20th century is referred to as an age of terrorism, the claim that the 21st century will be an age of super terrorism seems to have become reality. The fact that there is no consensus on the definition of terrorism, that states cannot unite in the fight against organized terrorism (which has elements of personnel, organizational structure, ideological infrastructure and violence), and that some states even support terrorist organizations because of their own interests, mean that sadly it will not be difficult for this claim to come true.

## Bibliography

- Aksu, Muharrem ve Faruk Turhan.(2012). Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik. *Uluslararası Alanya İşletme Fakültesi Dergisi*, 4 (2), 69-80.
- Aktaş, Murat. (2017). AB Ülkelerinde İslamofobi ve Terörizm, *Ombudsman Akademik*, 4 (7), 127-155.
- Aydın, Nurullah. (2005). Bilgi ve Teknoloji Çağında Küresel Terör ve Terörizm, Ankara:Kocacık Yayıncılık İletişim.
- Bal, İhsan. (2006b). Alacakaranlıkta Terörle Mücadele ve Komplo Teorileri, Ankara: USAK Publications.
- Başeren, Sertaç H. (2008). Terrorism with Its Differentiating Aspects. *Defence Against Terrorism Review*, 1(1), 1-11.
- Çaşın, Mesut Hakkı. (2008). *Uluslararası Terörizm*. Ankara:Nobel Publications.
- COMISAF Initial Assessment, 30 August 2009, [https://nsarchive2.gwu.edu/NSAEBB/NSAEBB292/Assessment\\_Redacted\\_092109.pdf](https://nsarchive2.gwu.edu/NSAEBB/NSAEBB292/Assessment_Redacted_092109.pdf)
- Esentur, Uğur. "Devlet Aleyhine Suç İşleyen Teröristlerin Sosyo-Ekonomik Özellikleri". MA Thesis, Ankara University, 2007.
- Fontanellaz, Adrien. The LTTE's Black Tigers; a military perspective, [https://www.academia.edu/42929759/The\\_LTTEs\\_Black\\_Tigers\\_a\\_military\\_perspective](https://www.academia.edu/42929759/The_LTTEs_Black_Tigers_a_military_perspective)
- Gökbunar, Ali Rıza. (2014). Organize Suç ve Terör Örgütleri ile Mücadelede Sivil Silah: Sosyal Destekler. *CBÜ Sosyal Bilimler Dergisi*, 12 (2), 230-242.
- Güneş, Mehmet. (2021). ABD'nin Afganistan'daki Başarısızlığında Terörle Mücadele Stratejisinin Etkisi, 20. Uluslararası Kamu Yönetimi Forumu, Conference Paper, 23 October 2021, Ankara:Ufuk Üniversitesi.
- Kaldor, M. (2023). *New and Old Wars: Organized Violence in a Global Era* (S. Erdem Türközü, Trans.). Ankara: Fol Publications.
- Kamuran, Reçber. (2014). Uluslararası Hukuk. Bursa:Dora Publications.
- Kurum, Mehmet. (2023). *Teori ve Pratikte Siyasal Şiddet ve Terörizm*. Ankara:Nobel Akademik Publications.
- Nuhoğlu, Özlem. (2022). "Uluslararası Terör ve Terörizm: Kavramsal Bir Tartışma". MA Thesis, Tekirdağ Namık Kemal University.
- Özdemir, Emrah. (2021). 11 Eylül Terör Saldırıları Sonrası ABD Gayrinizami Harp Anlayışının Değişimi. *The Journal of Security Studies*, 17 (39), 563-601.
- Özkan, Gizem. (2017). Kadına Yönelik Şiddet - Aile İçi Şiddet ve Konuya İlişkin Uluslararası Metinler Üzerine Bir İnceleme. *Hacettepe Hukuk Fakültesi Dergisi*, 1 (7), 533-564.
- Semericioğlu, Harun. (2016). Uluslararası Terörizmde Küresel İşbirliği: Bir Ütopya. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 34 (2), 112.
- Wilkinson, Paul. (2006). Terrorism versus democracy the liberal state response, Routledge. <https://www.hrw.org/reports/2004/afghanistan0304/2.htm>.



# Defence Against Terrorism Review DATR Magazine



DATR, 2025; 1 : 21-50

Electronic Online ISSN 1307 - 9190

## Strengthening Public Health Responses to Terrorism: Early Warning Systems and Health Care Preparedness

Tunalıgil V.\*<sup>1</sup> Cıtlıođlu E<sup>2</sup>

### Abstract

*The rise of terrorism presents significant challenges to public health systems. Understanding terrorism requires examining its root causes, such as socioeconomic disparities and political oppression, rather than focusing solely on security measures. This study explores the role of public health in countering terrorism and enhancing community resilience. The analysis synthesizes existing literature on public health responses to terrorism. Key strategies were identified, including emergency preparedness, epidemiological surveillance, and targeted training for health care providers and community leaders. Ethical considerations regarding civil liberties and threat identification were also examined. Findings indicate that effective public health interventions can significantly mitigate the psychological and physical impacts of terrorism. Training programs for health care professionals and community leaders improve the identification of radicalization signs and promote resilience. A multidisciplinary approach fosters alliance between public health, law enforcement, and community organizations, improving early warning systems and emergency response capabilities. The unpredictable nature of terrorism necessitates a shift in public health strategies to include mental health services and community engagement. Despite a decrease*

\* Corresponding Author: Verda Tunalıgil, MD, MPH, PhD verda@post.harvard.edu ORCID ID 0000-0002-4965-9231

<sup>1</sup> Presidency of Disaster Health and Emergency Medical Services, Health Directorate of İstanbul, Republic of Türkiye Ministry of Health, İstanbul, Türkiye

<sup>2</sup> Strategic Studies Implementation and Research Centre, Başkent University, Ankara, Türkiye

*in the number of attacks, casualty rates remain high, highlighting the need for ongoing preparedness. Ethical frameworks are essential for balancing threat assessment and civil liberties, while innovative technologies offer new avenues for improving response efforts. Strengthening public health responses to terrorism is vital for fostering community resilience and safety. This article presents novel public health strategies for enhancing preparedness and responses to terrorism, including eight actionable recommendations. Public health professionals can effectively address the complexities of terrorism by integrating a range of tactical initiatives. Enhancing training for health care providers and advocating for human rights policies are crucial steps in raising awareness and establishing a strong foundation for lasting community strength and peace. Incorporating risk assessment tools, ensuring robust referrals to support services, and bolstering health care response capacities are essential components of this comprehensive approach. Joint efforts with community partners, along with diligent monitoring, evaluation, and data collection, ensures ongoing effectiveness. A proactive approach that prioritizes collaboration and continuous evaluation will help mitigate the impacts of terrorism and promote societal well-being.*

**Keywords:** *disaster health management, emergency medical services (EMS), mass violence incident, strategic research, extremism, radicalization, human rights, community well-being, resilience*

## **1. Introduction**

Terrorism is a complex phenomenon influenced by various historical, social, and political factors. Understanding the context in which terrorism arises is crucial for addressing its impacts, emphasizing the importance of examining root causes and misconceptions, as well as the role of public health and community resilience. Security measures and global anxieties are direct consequences, precipitated by terrorism. The resilience of citizens is vital for assessing long-term effects (Roy, N., Kapil, V., Subbarao, I., & Ashkenazi, I., 2011). Definitions vary, but understanding the human element is important for grasping motivations and justifications. Individuals' insights and perspectives are essential for a comprehensive understanding of terrorism (Çitlioğlu, 2012b). Terrorism can be characterized as a method of coercion using violence or threats to instill fear for political or ideological purposes. Contemporary terrorist violence is characterized by the terrorist "triangle," in which A attacks B to persuade and coerce C into changing its stance. This differs from

“ordinary” violence, which typically targets innocent victims to generate fear and pressure governments (United Nations Office on Drugs and Crime, 2018).

Internationally, terrorism is defined as the unlawful use of violence to achieve political or ideological goals, often targeting civilians. Key treaties, like the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism, guide cooperation on counter-terrorism, emphasizing the need to respect human rights (Çitlioğlu, 2005). The complexities of accountability in terrorism-related situations, especially regarding attacks on hospitals, stem from the ambiguous legal status of non-state actors and the challenges in enforcing International Humanitarian Law (Tunalıgil, 2024). To effectively mitigate these threats, public health strategies must integrate comprehensive emergency response plans, community resilience initiatives, protection of health care infrastructure, and readily available mental health resources to address the psychological impact of terrorism on affected communities, ensuring continuity of care during crises and supporting resilience and recovery.

### **1.1. Historical context and misconceptions**

Terrorism has deep, longstanding societal roots, often arising from feelings of injustice and alienation. Mischaracterizing terrorism as solely religiously motivated can lead to discrimination and oversimplification. Its motivations are complex, influenced by psychological, social, and political factors, rather than being solely linked to mental illness (Çitlioğlu, 2024). Contemporary terrorism evolved from state conflict tactics, transitioning from targeted violence to indiscriminate acts, particularly during the industrialized warfare of the World Wars. David Rapoport’s “waves” theory describes distinct periods of terrorism, while Parker and Sitter identify four concurrent motivators such as socialism, nationalism, religious extremism, and exclusionism (United Nations Office on Drugs and Crime, 2018).

The World Health Organization (WHO) plays a vital role in countering terrorism by addressing public health emergencies related to chemical, biological, and radiological threats. The WHO strengthens national health systems and collaborates with expert organizations worldwide to manage health risks linked to terrorism, emphasizing the critical role of health in both national and international security (International Peace Institute, 2012). Research indicates that terrorism has become a tactical tool for state security, often manifesting through proxy wars and asymmetric threats. This shift in peace and warfare poses risks, as it may provide states with a means to address security concerns without tackling the underlying motivations of paramilitary activities classified as terrorism (Çitlioğlu, 2012a).

The impact of terrorism on public health includes immediate physical injuries and lasting psychological effects. An article highlights the challenges of treating blast-related injuries from terrorism, stressing the importance of learning from countries experienced in such attacks. Insights from experts in eight countries aimed to improve strategies for managing civilian casualties, focusing on both immediate medical care and long-term mental health impacts on survivors (Lerner, 2007). Emergency medical services (EMS) are crucial in responding to these incidents, significantly influencing community resilience, which is defined as the ability to withstand, adapt to, and recover from traumatic events, including terrorism.

### **1.2. Addressing root causes and the role of organized crime**

Effectively combating terrorism necessitates addressing root causes such as socioeconomic disparities, political oppression, and marginalization. Current global strategies often focus on short-term military responses, overlooking the socio-political and economic factors that contribute to terrorism. A multidisciplinary approach that targets systemic injustices is essential for preventing radicalization (Çitlioğlu, 2024). The complex roots of terrorism often stem from exclusion and exploitation, rather than cultural factors. The historical evolution of terrorism shows similarities to warfare, where major powers have employed terror-like tactics while mischaracterizing other groups. Global challenges, including resource depletion and environmental crises, exacerbate tensions, making it crucial to address the socio-economic and political grievances that lead individuals toward terrorism. A comprehensive approach prioritizing structural solutions and fostering inclusion, rather than relying solely on military measures, is vital for effectively eradicating terrorism (Çitlioğlu, 2009).

These root causes can create environments where extremism flourishes, negatively impacting public health by increasing stress, anxiety, and social fragmentation. The evolving nature of terrorism is increasingly linked with organized crime, complicating enforcement efforts. Criminal organizations often exploit social grievances and economic inequalities, further destabilizing communities and undermining their resilience. Cross-disciplinary strategies that integrate public health initiatives are essential. Community health programs can address the psychological impacts of terrorism and enhance resilience by fostering social cohesion and providing mental health resources. Engaging community members in developing solutions can empower them and improve their capacity to respond to and recover from crises.

### **1.3. Effective counterterrorism strategies and public engagement**

Effective counterterrorism requires adaptable strategies that consider the nature and characteristics of terrorist organizations, as well as how the public perceives them. A balanced approach is necessary, incorporating clear operational goals and effective communication to maintain public trust (Çitlioğlu, 2024). Integrating public health considerations into counterterrorism strategies enhances preparedness for potential terrorist attacks, ensuring that EMS can effectively handle mass casualties and psychological trauma. Preventing terrorism involves addressing core issues, dismantling organizations, and fostering social support against extremist ideologies.

Engaging with communities through inclusive dialogue can create an environment where individuals feel valued, contributing to a reduction in extremist sentiments. Public health initiatives focusing on mental health, social cohesion, and education are critical for building resilience against terrorism. By strengthening community capacity to cope with trauma and fostering a culture of support, public health efforts can mitigate terrorism's impacts, leading to a safer and more resilient society. The importance of immediate responders is emphasized in a pioneering study that accentuates the role of "bystanders." This transformative research, which draws on extensive field leadership experience in responding to mass casualty events, advocates for communities to recognize the potential of those present during emergencies to prevent harm before professional help arrives. Strategies to encourage public interventions are needed, especially in cultures where public involvement is not prioritized (Ashkenazi, I., & Hunt, R. C., 2019).

### **1.4. Terrorism**

Terrorism is characterized by its unpredictability and high casualty rates, leading to profound social and geopolitical repercussions. While not the deadliest form of violence globally, this intentional use of coercion to instill fear for political objectives led to 8,352 deaths in 2023, marking a 22% increase from the previous year, despite a decrease in the number of attacks to 3,350. The Sahel region has witnessed a troubling connection between terrorism and organized crime, which, along with the psychological impacts of terrorism, significantly affects social dynamics and undermines geopolitical stability (Institute for Economics & Peace, 2024). Acts of terror that transcend borders involve the use of violence and intimidation by non-state actors to achieve political, ideological, or religious goals, often targeting civilians to instill fear (Çitlioğlu, 2004). The transformation of international relations

has led to an increase in regional conflicts and feelings of victimization among communities, with future tensions expected due to population growth, climate change, and resource shortages. Terrorist groups are likely to focus on identity-based ideologies, but “global terrorism” is not fundamentally different from earlier forms of terrorism (Çitlioğlu, 2008).

Global public health measures are essential in mitigating these detrimental effects and supporting affected communities. A study on the health impacts of terrorist attacks in Turkic states from 1970 to 2019 identified 4,629 incidents that resulted in 7,496 fatalities and 10,928 injuries, highlighting Türkiye as the most affected country in terms of medical outcomes (Çalışkan, 2023). Addressing these challenges is fundamental for improving population health and quality of life, as well as ensuring the well-being of communities at both local and global levels.

## **1.5. Study aim and research design**

### **1.5.1. Research objectives**

This article argues that strengthening public health responses to terrorism through early warning systems and health care preparedness is essential for improving global resilience to terrorism’s multifaceted impacts. By focusing on both immediate physical harm and long-term psychological effects, effective preparedness enhances community recovery and fosters resilience. Integrating public health initiatives with security strategies is key to reducing the harm caused by terrorism. The primary objective of the article is to explore how public health frameworks can be optimized to enhance the response to the effects of terrorism, cultivate a culture of prevention, and ultimately contribute to more sustainably resilient communities.

### **1.5.2. Key inquiries**

Several critical questions drive the article’s inquiry: How can early warning systems be effectively integrated into public health frameworks to improve terrorism preparedness and response? What public health strategies are essential to enhance health care preparedness for terrorism-related events? How can addressing the root causes of terrorism, such as political oppression and socioeconomic disparities, contribute to more effective public health interventions? The article, consequently, considers the role of public health professionals in combating terrorism and violent extremism while addressing the consequences for vulnerable populations.

### **1.5.3. Theoretical frameworks**

To analyze the relationship between public health and terrorism, the article draws on several theoretical frameworks. The **social determinants** framework addresses how factors such as socioeconomic inequality, political exclusion, and community dislocation contribute to terrorism and its health impacts. **Public health laws** are examined through the lens of legislative reforms that support bioterrorism preparedness while safeguarding individual rights. The concept of **community resilience** is explored to understand how social cohesion, mental health support, and community engagement can mitigate the long-term consequences of terrorism. An **interdisciplinary collaboration** approach emphasizes the need for integrated strategies combining public health, law enforcement, and social services to address terrorism and violent extremism effectively. A **public health preparedness** framework is termed, focusing on the development of proactive strategies, resources, and systems for responding to potential terrorist threats and ensuring rapid, coordinated responses to minimize health impacts in the aftermath of such events.

### **1.5.4. Thematic synthesis of evidence**

The thematic synthesis of evidence systematically reviews empirical findings from relevant research, focusing on key themes such as health care preparedness, emergency response strategies, and community engagement in the face of terrorism. To maintain consistency in the screening and evaluation of the literature, a structured approach was employed. This thematic approach provides an integrative and comprehensive understanding of how public health can contribute to mitigating the impacts of terrorism and strengthening preparedness for future threats.

### **1.5.5. Structure of the review**

The review is structured to offer a comprehensive analysis of the intersection between public health and terrorism. It begins by outlining the theoretical frameworks that guide the analysis, followed by a synthesis of evidence on public health's role in terrorism preparedness. The article concludes by proposing strategies for improving health care systems and fostering community resilience, with key recommendations for public health practice, policy development, and interdisciplinary collaboration.

## **2. Critical roles of public health professionals in the context of terrorism**

### **2.1 Terrorism and public health**

Terrorism poses a significant threat to public health worldwide, impacting health care systems and increasing mortality and morbidity. The interplay between terrorism and public health requires a multifaceted response, emphasizing the need for public health professionals to address the psychological and physical impacts on vulnerable populations while enhancing preparedness and resilience. In 2016, terrorism caused approximately 25,500 deaths globally, with the highest fatalities in Iraq, Afghanistan, and Pakistan, while Europe and North America experienced relatively few successful attacks. Understanding the causes of terrorism, such as exclusion and desensitization to violence, is essential, as discriminatory policies can exacerbate societal alienation (Lindert, J., Bilsen, J., & McKee, M., 2018). Terrorism disrupts health care services, leading to an increased demand for emergency care, a rise in mental health issues, and heightened rates of mortality and disability. Chronic exposure to terrorism can exacerbate fear and anxiety within affected communities. Fortifying emergency response coordination, improving epidemiological surveillance, advancing public health laboratories, expanding mental health care, effectively planning health services, and fostering better public communication were six key areas recommended for adaptation by public health systems in a Spanish study (Arcos González, P., Castro Delgado, R., Cuartas Alvarez, T., & Pérez-Berrocal Alonso, J., 2009). Strengthening public health infrastructure is critical, especially following events like the September 11 attacks, which revealed vulnerabilities in health systems. Addressing root causes of terrorism, including poverty and alienation, is necessary to bolster overall resilience in public health practices (Beaglehole, 2004). Public perceptions of fairness in health responses to bioterrorism is fundamental, as demonstrated by a study revealing disparities among racial and ethnic groups in Los Angeles County. While 72.7% believed the public health system would respond fairly, African Americans reported the lowest perceived fairness at 63.0%. This indicates a need for focused improvements in public health communication and equity (Eisenman, D. P., Wold, C., Setodji, C., Hickey, S., Lee, B., Stein, B. D., & Long, A., 2004). The 2003 Istanbul bombings were a series of deadly terrorist attacks in Türkiye. Two studies indicated the widespread impact of terrorist bombings on health care systems and stressed the importance of trauma centers in disaster response. The first attack on November 15 targeted two synagogues Beth Israel and Neve Shalom, killing 30 people and injuring approximately 300. Secondary blast injuries occurred in 86% of cases, and a significant proportion of victims did not require hospitalization, with only 13% being admitted. On November 20, a subsequent attack occurred, in which

truck bombs targeted the British Consulate and the HSBC Hongkong and Shanghai Banking Corporation head office, resulting in 33 deaths and approximately 450 injuries. These bombings collectively resulted in 63 deaths and approximately 750 injuries, making them among the deadliest terrorist attacks in recent Turkish history (Rodoplu, Arnold, Tokyay, Ersoy, Cetiner, & Yücel, 2004). A study examining the health care response to these attacks provided valuable insights. The November 15 bombing affected 24 hospitals, where 330 patients were treated, 85 of whom required hospitalization. Ten of these hospitalized patients needed intensive care unit (ICU) care, with an average stay of 4 days. Tragically, 26 individuals died. Transportation varied, with 43% of patients arriving by ambulance and 57% by other means. In the November 20 bombing, 495 patients were treated across 34 hospitals. Of these, 59 required hospitalization, and 10 needed ICU care. A total of 370 days were spent in the hospital by these patients, with an average of 6.2 days per patient. Only 33% arrived by ambulance, and 34 deaths resulted from the attack. The study assessed the prevalence of head and neck injuries and brought the critical importance of disaster preparedness in healthcare facilities to light (Taviloglu, Yanar, Kavuncu, Ertekin, & Güloğlu, 2005). Both studies revealed the far-reaching consequences of terrorist bombings on health care, drawing attention to the vital role of trauma centers in responding to mass casualty incidents. The findings also pointed to the challenges in coordinating EMS due to factors such as hospital location and personal preferences.

Building on the broader implications of health care responses to terrorism, it is just as crucial to focus on the unique needs of pediatric populations during such crises. Preparing hospitals for pediatric terrorism victims necessitates specialized training and protocols tailored to address children's unique medical and psychological needs. A review categorizes mass casualty terrorism into biological, chemical, nuclear, and thermomechanical threats, emphasizing the need for child-specific emergency protocols (Chung, S., & Shanno, M., 2005). Addressing gaps in medical countermeasures for children is urgent, with continued advocacy needed to protect pediatric populations from biological or chemical threats. Despite progress, significant gaps remain in pediatric formulations and safety information (Disaster Preparedness Advisory Council, 2016). The psychological impact of terrorism on children necessitates effective coping strategies for families. A study revealed that children exposed to terrorism-related news experienced increased anxiety, but those whose parents were trained in coping techniques reported lower fear levels, emphasizing the importance of public health initiatives addressing these psychological effects (Comer, J., Furr, J., Beidas, R. S., & Weiner, C. L., 2008).

Bioterrorism preparedness involves enhancing public health infrastructure and rapid response capabilities. The anthrax events brought attention to gaps in preparedness, prompting the Centers for Disease Control and Prevention (CDC) to issue guidelines for improving response capabilities at all levels of government. Integrating mental health strategies into national health plans is crucial to address the psychological consequences of terrorism (US Institute of Medicine, 2003). Reevaluating public health laws to better address bioterrorism challenges while protecting individual rights is essential, ultimately ensuring a balanced approach. Modern public health law reforms are needed to strengthen infrastructure against evolving health threats (Gostin, 2002).

## 2.2. Public health professionals as key players in combating terrorism and violent extremism

Public health professionals can play several important roles in the fight against terrorism and countering violent extremism [Table 1].

**Table 1.** An outline of the critical roles of public health professionals along with their key components.

Critical Role	Description	Key Components
<b>Prevention and intervention programs</b>	Developing and implementing programs to prevent diseases	Vaccination, screening, health promotion initiatives
<b>Community engagement and education</b>	Fostering community involvement and awareness about health	Workshops, outreach programs, educational materials
<b>Early warning systems</b>	Monitoring and detecting potential public health threats	Surveillance systems, data analysis, rapid response protocols
<b>Mental health and trauma support</b>	Addressing mental health needs, especially post-crisis	Counseling services, crisis intervention, community support
<b>Research and data collection</b>	Gathering and analyzing data to inform public health decisions	Epidemiological studies, health assessments, surveys
<b>Capacity building and training</b>	Enhancing skills and knowledge of health professionals	Workshops, certifications, mentorship programs
<b>Policy advocacy and collaboration</b>	Advocating for health policies and work with stakeholders	Lobbying, coalition building, public health legislation
<b>International collaboration</b>	Partnering with global entities to address health issues	Joint initiatives, sharing best practices, research partnerships
<b>Advanced technologies</b>	Utilizing technology to improve public health outcomes	Telehealth, data analytics, mobile health applications

### **2.2.1. Prevention and intervention programs**

Public health professionals play a crucial role in implementing intervention programs aimed at preventing radicalization and violent extremism. These interventions focus on addressing root causes such as social exclusion, socioeconomic disparities, and mental health needs of vulnerable populations.

A proceedings paper on countering violent extremism (CVE) highlights the importance of understanding societal factors rather than just individual behaviors and advocates for community engagement. Health professionals face ethical dilemmas in identifying potential threats while respecting civil liberties. The CDC offers guidelines for violence prevention that include a tiered model, addressing broader determinants of extremism and supporting rehabilitation efforts. The need for community-centric strategies, rigorous evaluations of CVE programs, and evidence-based practices to promote resilience and effectively reduce violence was also emphasized at the workshop (National Academies of Sciences, Engineering, and Medicine, 2017).

### **2.2.2. Community engagement and education**

Public health professionals can engage with communities to raise awareness about the risks of radicalization and extremism. They can collaborate with community leaders, educators, and religious figures to promote tolerance, resilience, and non-violent conflict resolution strategies.

A review explored police programs designed to enhance community connectedness as a means to combat violent extremism by reducing social isolation and fostering belonging. It discussed the potential for police to disrupt terrorist activities and collaborate with communities to identify individuals at risk of radicalization. After analyzing studies from 2002 to 2018, the review found only one eligible study. It concluded that there is insufficient evidence to assess the effectiveness of police-led initiatives in reducing violent extremism, emphasizing the need for more rigorous evaluations (Mazerolle, L., Eggins, E., Cherney, A., Hine, L., Higginson, A., & Belton, E., 2020). Building partnerships with community stakeholders, including educators, social workers, and law enforcement, is imperative to foster trust and build resilience. A multidisciplinary approach enables public health initiatives to be both evidence-based and culturally sensitive, promoting long-term social cohesion and well-being. Medical professionals can collaborate with experts in fields such as sociology, psychology, and criminology to engage communities effectively. By integrating diverse perspectives, they can

address the complex social determinants contributing to violence and extremism. These efforts ultimately empower public health professionals to create supportive environments conducive to health and safety.

### **2.2.3. Early warning systems**

Developing and implementing early warning systems serves as a pragmatic instrument to identify individuals at risk of radicalization or involvement in extremist activities. This process can involve training health care providers to recognize the signs of radicalization and refer those individuals to appropriate support services. By adopting this approach, we can foster a proactive strategy for prevention and enhance community safety.

Public alert and warning systems are crucial for managing the impacts of emergencies, particularly those stemming from natural disasters and terrorism. A systematic review of 1,737 studies narrowed down to 156 relevant studies identified key themes for enhancing these systems, such as message clarity, protective action guidance, and community engagement. Recommendations for improvement include regular training, increasing accessibility, and refining protocols as emergencies become more frequent and severe (Sadiq, A. A., Okhai, R., Tyler, J., & Entress, R., 2023). Another aspect of early warning systems is their role in detecting bioterrorism and communicable disease outbreaks. A study utilizing syndromic surveillance demonstrated that while current detection capabilities are limited under certain conditions, the potential to identify broader health trends exists. This validates the need for improved systems to monitor public health threats effectively (Cooper, D. L., Verlander, N. Q., Smith, G. E., Charlett, A., Gerard, E., Willocks, L., & O'Brien, S., 2006). The urgency for enhanced early warning systems in public health is further echoed in a commentary advocating for better digital communication channels to ensure timely sharing of critical medical information, particularly during bioterrorism events. The piece calls attention to the challenges posed by inadequate coordination and access to vital research (Kassirer, 2002). The critical need for early warning systems for detecting hazardous biological agents in drinking water has been emphasized, particularly regarding potential terrorist threats. This report advocates for advanced detection technologies and community involvement in emergency response planning (Foran, J. A., & Brosnan, T. M., 2000). The effectiveness of early warning systems is also highlighted in a study analyzing the fear of terrorism's impact on hospital emergency department usage. During a terror alert in Istanbul, researchers found a significant reduction in emergency visits, particularly among females. This emphasizes the indirect health

consequences of terrorism fear and accentuates the importance of maintaining access to health care during crises, showcasing how public health systems must adapt to threats (Hurşitoğlu, M., Erdal, G. S., Akdeniz, E., Koçoğlu, H., Kocamaz, N., Tevetoğlu, I. O., Yücel, H., Harmankaya, O., Güven, A., Akarsu, M., Tükek, T., Öztürk, G., Doğan, H., Yılmaz, B. K., Güneş, M. E., & Kumbasar, A. B., 2019).

Innovative techniques are being explored to detect terrorist activities more effectively. A recent study proposed new methodologies for analyzing sparse data, which could enhance understanding and prevention of terrorism (Prieto-Curiel, R., Walther, O., & Davies, E., 2023). A political violence early-warning system, ViEWS illustrates the intersection of “political violence and public health” by forecasting organized violence and considering its implications for community health. This system employs methodologies integrating conflict research and machine learning to identify emerging threats, especially in regions with histories of violence (Hegre, H., Allansson, M., Basedau, M., Colaresi, M., Croicu, M., Fjelde, H., Hoyles, F., Hultman, L., Höglbladh, S., Jansen, R., Mouhleb, N., Muhammad, S. A., Nilsson, D., Nygård, H. M., Olafsdottir, G., Petrova, K., Randahl, D., Rød, E. G., Schneider, G., & Vestby, J., 2019). Another research study aimed at quantifying the future lethality of terrorist organizations highlights the development of an early-warning signal based on early attack data. This model enhances predictive capabilities regarding potential threats, reinforcing the importance of advanced statistical techniques in counter-terrorism efforts (Yang, Y., Pah, A. R., & Uzzi, B., 2019).

These studies emphasize the integral role of early warning systems in protecting public health and safety in the face of terrorism and other emergencies in aggregate.

#### **2.2.4. Mental health and trauma support**

Providing mental health services and trauma support to individuals affected by terrorism, including victims, families, and communities, helps prevent further radicalization and retaliatory violence. Effective strategies for addressing global mental health in the context of violent extremism require collaboration among mental health professionals, community organizations, and policymakers. Such partnerships promote integrated models within civil society, prioritizing mental health and psychosocial support over securitized approaches. This focus aims to prevent extremism and rehabilitate affected individuals, fostering safer and more resilient communities. It also necessitates reassessing current practices to align with core values and evidence-based methods. Prioritizing broader prevention frameworks ultimately supports those at risk of radicalization and strengthens global mental

health efforts (Weine, S., & Kansal, S., 2019). Psychological Operations (PSYOP) seek to influence perceptions and behaviors through strategic messaging, essential for effective counterterrorism strategies. By incorporating public health principles alongside PSYOP, communities can be educated about radicalization and extremist narratives. A trauma-informed approach that addresses the psychological needs of affected populations promotes trust and social cohesion. Engaging local leaders and grassroots organizations enhances community credibility and ownership of safety, supporting both counterterrorism efforts and overall societal well-being (Çitlioğlu, 2006).

The necessity for a public health response to the psychological impacts of terrorism is highlighted, as this area is often overlooked. Preparedness for all forms of violence, including terrorism, is especially crucial for vulnerable populations such as children and individuals with mental illness. A workshop report by the Institute of Medicine emphasizes the importance of integrating mental health services into public health strategies, emphasizing that psychological well-being is critical for overall health. It calls for coordinated efforts among public health, medical care, and emergency services to address the mental health needs resulting from terrorism and improve resilience and outcomes following violent events (US Institute of Medicine, 2003). Trauma support is essential for providing mental health services to individuals affected by terrorism, including survivors, loved ones, and the society, to mitigate the effects of terrorist attacks.

### **2.2.5. Research and data collection**

Conducting research to better understand the social, psychological, and health-related factors that contribute to radicalization and extremism. This research can inform evidence-based interventions and policies aimed at preventing and countering terrorism.

Counterterrorism efforts rely on integrating diverse information sources to effectively prevent and respond to threats. A strategic research agenda should prioritize information security, IT needs for emergency responders, and data fusion. The report identifies seven key challenges, including systems analysis and sensor networks, highlighting the importance of effective data collection and analysis for threat assessment. It recommends establishing a Homeland Security Institute to support comprehensive vulnerability analysis and standards development, emphasizing collaboration with state and local governments, industry, and academia. Balancing security with civil liberties and promoting international cooperation are also crucial for enhancing global security against terrorism. (National Research

Council, 2002). A systematic review of public mental health approaches to online radicalization examined the interplay of individual, familial, communal, and structural factors. It emphasized the urgent need for further research, particularly in light of the increasing influence of social media on radicalized beliefs (Mughal, R., DeMarinis, V., Nordendahl, M., Lone, H., Phillips, V., & Boyd-MacMillan, E., 2023). While the North Atlantic Treaty Organization Readiness Initiative primarily focuses on military readiness and rapid deployment, it also recognizes the importance of research operations in developing evidence-based interventions and policies aimed at preventing terrorism. This comprehensive approach draws attention to the necessity of a multifaceted response to security challenges, blending military readiness with insights especially from social research (North Atlantic Treaty Organization, 2024). A study evaluated hospital disaster plans for mass casualty incidents following terrorist explosions through a live exercise using real patient data. Researchers developed a comprehensive database of 420 patients injured in terrorist attacks and 100 from motor vehicle accidents. This robust data informed victim profiles used in live exercises across eight hospitals. The findings highlighted that traditional exercises often fell short in effectively assessing the quality of clinical decision-making. By leveraging real patient data, the study provided a more accurate evaluation of hospital preparedness, pinpointing specific areas for improvement in clinical decision-making and resource management during mass casualty incidents. This best practice example reinforces the essential role of research and data collection in managing such crises (Ashkenazi, I., Ohana, A., Azaria, B., Gelfer, A., Nave, C., Deutch, Z., Gens, I., Fadlon, M., Dahan, Y., Rapaport, L., Kishkinov, D., Bar, A., Tal-Or, E., Vaknin, N., Blumenfeld, A., Kessel, B., Alfici, R., Olsha, O., & Michaelson, M., 2012).

### **2.2.6. Capacity building and training**

Building the capacity of health care providers, social workers, educators, and community leaders to address the complex challenges posed by terrorism and violent extremism. This can include training on recognizing signs of radicalization, promoting resilience, and responding effectively to crises.

The rise in terrorist attacks in Europe highlights the urgent need for capacity building and training among health care providers, social workers, educators, and community leaders to effectively address the complex challenges posed by terrorism and violent extremism. A crucial aspect of this effort is enhancing hospital preparedness through comprehensive education and training strategies. A systematic review of the Global Terrorism Database 2000-2017 identified 203

relevant articles and 47 key recommendations, emphasizing the necessity of regular, realistic training scenarios that engage all staff and community stakeholders. The integration of military expertise for managing severe injuries is essential, as significant gaps in current surgical education have been identified by medical leaders. This emphasizes the importance of a multi-disciplinary approach to foster resilience and effective community responses to these threats (Schorscher, N., Kippnich, M., Meybohm, P., & Wurmb, T., 2022). In Pakistan, a study focused on the preparedness of medical staff for terrorism-related disasters revealed similar gaps in training and capacity building. Qualitative interviews with 15 medical professionals highlighted critical themes such as professional and psychological readiness, direct disaster experiences, and various barriers to effective response, including insufficient space, lack of disaster-related curricula, and absent protocols. Although medical staff understood the necessary skills to manage such disasters, addressing these gaps through enhanced training is vital for fostering collaboration among various stakeholders in the community (Khilji, F. U. R., Raziq, A., Shoaib, M., Baloch, N. S., Raza, S., Iqbal, Z., Ishaq, R., Haider, S., Iqbal, Q., Ahmad, N., & Saleem, F., 2021). A study evaluating the terrorism preparedness of occupational health professionals found that brief training improved participants' confidence in clinical skills and minimizing exposure while caring for victims of terrorist attacks. Only 32%, however, felt their employers were prepared for a bioterrorism event, and 75% felt unprepared to provide mental health counseling after an attack. These findings suggest that while short training sessions can boost confidence, more comprehensive training is necessary to ensure adequate preparedness for various potential terrorist events (Gershon, R. R. M., Gemson, D. H., & Qureshi, K., 2004).

The field of terror medicine, which addresses the medical implications of terrorism, remains inconsistently integrated into medical school curricula, despite the increased demand for its inclusion following the 2001 attacks. A proposed structured 4-year curriculum, culminating in a short course for fourth-year students, aims to help medical schools effectively incorporate terror medicine into their training programs. This framework not only prepares future health care providers to respond to terrorist events but also ensures that the medical community is better equipped to handle the psychological and physical impacts of such crises (Cole, L. A., Wagner, K., Scott, S., Connell, N. D., Cooper, A., Kennedy, C. A., Natal, B., & Lamba, S., 2014).

These studies collectively illustrate a critical need for comprehensive training and collaborative efforts among various sectors to effectively address the challenges posed by terrorism and violent extremism.

### **2.2.7. Policy advocacy and collaboration**

Public health professionals can collaborate with policymakers, law enforcement, and civil society organizations to develop integrated approaches to counter extremism and advocate for legal measures that promote community resilience, social cohesion, and human rights. A paper emphasizes the critical issues of terrorism and extremism, focusing on the effectiveness of counter-radicalization policies in educational settings. It advocates for policy advocacy that promotes collaboration among stakeholders to develop more effective strategies. The discussion highlights the importance of advocating for policies and initiatives that prioritize human security and the rights of individuals, aiming to create a safer and more inclusive educational environment while addressing the root causes of radicalization (Adebayo, 2021).

### **2.2.8. International collaboration**

Engaging in international collaboration and knowledge sharing with public health professionals from other countries and regions affected by terrorism. This can facilitate the exchange of best practices, lessons learned, and innovative strategies for prevention and response.

A study analyzing 119,803 terrorist attacks from 2001 to 2018, using the Global Terrorism Database and the UN sanctions list, found that, on average, 13 new organizations join the global cooperation network each year, with a survival rate of about 34.66%. The network's core shows stability, indicating strong connections among key organizations, while peripheral ones are more variable (Cui, D., Ou, C., & Lu, X., 2024). These findings highlight the complexities of counter-terrorism efforts amid evolving threats. Fostering international knowledge sharing can enhance understanding of these dynamics, leading to more effective prevention and response strategies. Collaborative efforts can identify emerging threats and share best practices, ultimately strengthening community resilience and improving global counter-terrorism initiatives. The CDC and its partners have initiated efforts to enhance medical preparedness for terrorist bombings, despite the absence of mass-casualty attacks in the United States since 9/11. Acknowledging bombings as a "predictable surprise," they address challenges in motivation and prioritization for preparedness. Key outcomes include a course on clinical care for bombing victims, guidance on surge capacity, and a bomb injury surveillance tool. These initiatives have both United States and international relevance and emphasize the need for further collaboration (Hunt, R., Ashkenazi, I., Deitchman, S., Dorn, B. C., Enders, J., Falk, H., Garbarino, L., Kapil, V., Madden, J., Marcus, L., Sarmiento, K., & Sasser, S., 2010).

Highlighted are the interconnected challenges of understanding terrorist organizational dynamics and enhancing preparedness for terrorist acts, emphasizing the necessity of coordinated efforts across various sectors. Integrating public health approaches into counter-terrorism efforts enhances effectiveness, promotes community resilience, and upholds human rights and social justice. Engaging in international collaboration and knowledge sharing with public health professionals from affected regions can facilitate the exchange of best practices and innovative strategies for prevention and response. Studies emphasize the interconnected challenges of understanding terrorist networks overall, enhancing preparedness, and promoting global cooperation to effectively combat terrorism.

### **2.2.9. Advanced technologies**

Modern technologies in public health play a crucial role in mitigating the risks and harms associated with terrorism through various innovative methods. Advanced surveillance systems, including drones and satellite imagery, improve monitoring capabilities. Data analytics and artificial intelligence help identify patterns that predict potential threats, facilitating early detection of health crises. Telehealth technologies enable rapid health care delivery, allowing for remote medical support during emergencies, while mobile health applications offer real-time information and alerts to the public.

Geographic Information Systems (GIS) aid in mapping health impacts and optimizing resource allocation, and biodefense technologies provide rapid diagnostic tools for biological agents. Social media monitoring helps analyze public sentiment and emerging threats, while wearable technology tracks health metrics of first responders and civilians. Integrated emergency response systems enhance coordination among health care providers and emergency services, and training simulations using virtual reality improve preparedness for managing health impacts from terrorist events. These technologies significantly bolster public health's capacity to address terrorism-related challenges. The effectiveness of public health digital surveillance systems for prevention and control can be significantly enhanced by integrating GIS, social media, and internet-based data within global public health surveillance frameworks to better serve at-risk populations (Croner, 2003; Maddah, N., Verma, A., Almashmoum, M., & Ainsworth, J., 2023; Velasco, E., Agheneza, T., Denecke, K., Kirchner, G., & Eckmanns, T., 2014). Integrating diverse datasets like demographics and infrastructure vulnerabilities with GIS technology is crucial in disaster management and terrorism response. It supports impact assessments and improves communication, enhancing response efforts and recovery. Public health can use GIS to analyze data, estimate damage, and identify

at-risk populations, bolstering community resilience against terrorism. Enterprise GIS plays a key role in emergency management by ensuring accurate data sharing across agencies throughout all stages of response (Eichelberger, 2018; Johnson, 2000; Tunalgil, 2024). Analysis of social media data following consecutive terrorist attacks in London revealed clusters of negative emotions, particularly in socially deprived areas, indicating that terrorism broadly affects public sentiment (Dai, 2020). A study simulating an anthrax attack in Seattle further projected a potential median sales price drop of \$280,000 in the central business district, leading to an overall residential property value decrease of over \$50 billion and an estimated 70,000 foreclosures (Dormady, N., Szelazek, T., & Rose, A., 2014).

In exploring the intersection of machine learning and terrorism, the implications of big data collection and analysis on the privacy-security dilemma are examined. Rapid advancements in surveillance technologies raise concerns about their effectiveness, especially regarding the identification of terrorists, including lone-wolf attackers. The irregular nature of terrorist digital footprints complicates data analysis, leading to issues such as class imbalance and spurious correlations. The distinction between data and metadata is also often misrepresented, with proponents of mass surveillance downplaying privacy invasions associated with metadata collection. The potential for machine learning to infer personal data from metadata further complicates privacy concerns. Given the sparse datasets and privacy risks in bulk data collection, the article urges a critical reassessment of these surveillance strategies and the algorithms that depend on them, especially concerning national security (Verhelst, H. M., Stannat, A. W., & Mecacci, G., 2020).

The advantages of advanced technologies in public health encompass increased operational capacities in crisis management and improved data analysis for informed decision-making. These tools help public health officials anticipate threats and effectively communicate with the public, ultimately saving lives and fostering trust in health systems.

### **3. Eight public health strategy suggestions to counter terrorism**

Bolstering health care response capacities is crucial for enhancing the overall effectiveness of public health strategies in countering terrorism. Public health preparation for escalating terrorism involves the implementation of early warning systems and an effective health care response. Public health preparedness for terrorism involves addressing immediate health impacts such as injuries and trauma, as well as long-term effects like psychological distress and disease outbreaks. Using a world map is crucial for identifying vulnerable regions, allocating resources

effectively, coordinating response efforts, assessing risks comprehensively, prioritizing training and capacity building, and fostering international collaboration. This visual tool enhances strategic planning and strengthens resilience against the health consequences of terrorism. Strengthening public health responses to escalating terrorism involves the implementation of early warning systems and enhanced health care preparedness **[Image]**.

## PUBLIC HEALTH STRATEGIES FOR COUNTERING TERRORISM



**Image.** Enhancing public health responses to terrorism through early warning systems and robust health care preparedness.

Public health preparation for countering escalating terrorism entails the establishment of effective early warning systems and robust health care responses. By integrating risk assessment tools, training health care providers, and fostering community collaboration, these systems can identify and address potential threats, ensuring swift and coordinated action during crises. This comprehensive approach not only enhances public safety but also promotes resilience and social cohesion in the face of emerging challenges. This comprehensive approach enhances governments' ability to detect, respond to, and mitigate terrorism threats while promoting public health, social cohesion, and human rights [Table 2].

**Table 2.** A summary of key points in public health preparedness and response to counter terrorism.

Focus Area	Description
<b>Training health care providers</b>	Collaborating with health care providers to train them in recognizing signs of radicalization, including behavioral changes and triggers, and preparing them for responding to terrorist incidents and psychological first aid
<b>Building awareness</b>	Raising awareness about factors contributing to radicalization, such as social exclusion, discrimination, economic disparities, and psychological trauma, enabling providers to identify vulnerable individuals.
<b>Integration of risk assessment tools</b>	Developing and integrating evidence-based, culturally sensitive risk assessment tools within health care settings to evaluate patients for signs of radicalization and extremist propaganda exposure
<b>Referral to support services</b>	Establishing protocols for health care providers to refer at-risk individuals to support services, including mental health counseling, social support, and community-based interventions
<b>Bolstering health care response capacities</b>	Enhancing readiness to respond to terrorist incidents by training staff in emergency protocols, stockpiling medical supplies, and coordinating with local authorities for crisis response
<b>Collaboration with community partners</b>	Forging partnerships with community organizations, religious leaders, educators, and law enforcement to improve early warning systems and health care responses, ensuring culturally appropriate interventions.
<b>Monitoring and evaluation</b>	Implementing mechanisms for monitoring the effectiveness of early warning systems and health care responses to identify and mitigate radicalization risks, allowing for continuous adjustments based on emerging trends
<b>Data collection and analysis</b>	Collecting and analyzing data on individuals identified through early warning systems to understand radicalization patterns, while ensuring patient confidentiality and sharing anonymized data for research and policy development

### **3.1. Training health care providers**

Public health professionals are encouraged to collaborate with health care providers to enhance the recognition of signs of radicalization. Key indicators such as behavioral changes, social isolation, expressions of extremist ideologies, and potential triggers for radicalization should be detailed. Training should also incorporate preparedness for responding to terrorist incidents, including mass casualty events and psychological first aid.

### **3.2. Building awareness**

Enhancing health care response capacities is crucial for strengthening public health strategies against terrorism. One effective approach is to raise awareness among health care providers about the factors that contribute to radicalization. These factors include social exclusion, discrimination, economic disparities, and psychological trauma. By understanding these root causes, health care providers can better identify vulnerable individuals who may be at risk and respond appropriately to their needs. This proactive engagement not only improves individual care but also contributes to broader public health efforts aimed at preventing extremist attitudes and actions while fostering community bonds.

### **3.3. Integration of risk assessment tools**

Developing and integrating risk assessment tools within health care settings is essential for systematically evaluating patients for signs of radicalization or exposure to extremist propaganda. These evidence-based tools should draw on the latest research to ensure reliability and validity in identifying at-risk individuals. It is crucial to ensure that these assessments are culturally sensitive, considering the diverse backgrounds of patients to avoid stigmatization and promote effective identification and intervention. Equipping health care providers with these tailored tools enhances their capacity to recognize potential warning signs early and implement appropriate interventions that support both individual well-being and community safety.

### **3.4. Referral to support services**

Establishing clear protocols for health care providers is necessary for effectively referring individuals at risk of radicalization to appropriate support services. These protocols should outline specific steps for identifying at-risk patients and provide guidance on available resources. Referral services may include mental health counseling to address underlying psychological issues, social support

programs to combat isolation, and religious counseling where applicable to foster understanding and connection. Additionally, community-based interventions that promote resilience and counter extremist narratives should be integrated into these protocols. By creating a comprehensive referral system, health care providers can play a critical role in addressing the needs of vulnerable individuals and contributing to community safety and cohesion.

### **3.5. Bolstering health care response capacities**

Health care facilities' level of readiness to respond to terrorist incidents is critical for effective crisis management. This can be achieved by training staff in emergency response protocols, ensuring they are well-prepared to act swiftly and effectively during a crisis. Facilities should also focus on stockpiling essential medical supplies, such as first aid kits, trauma gear, and medications, to ensure immediate availability when needed. Coordinating with local authorities, including law enforcement and emergency services, is vital for facilitating rapid deployment and collaboration during incidents. Health care facilities can significantly improve their capacity to manage the aftermath of terrorist attacks and safeguard public health by prioritizing these measures.

### **3.6. Collaboration with community partners**

A crucial aspect of public health preparedness in addressing terrorism is building partnerships with community organizations, religious leaders, educators, and law enforcement. This collaboration enhances early warning systems and health care responses. Community input is essential for creating culturally appropriate interventions and fostering trust among affected populations. Coordinating with local authorities, including law enforcement and emergency services, ensures rapid deployment and effective collaboration during incidents. Health care facilities can improve their ability to respond to terrorist attacks by adopting these strategies, ultimately protecting public health and security.

### **3.7. Monitoring and evaluation**

Implementing mechanisms for monitoring the effectiveness of early warning systems and health care responses is essential for identifying and mitigating risks associated with extremism. Continuous evaluation enables health care providers to assess how well these systems function in practice and their impact on at-risk individuals. By analyzing data on referrals, interventions, and outcomes, health care facilities can identify emerging trends and adapt their strategies accordingly.

Regular feedback loops and stakeholder engagement will ensure that protocols remain relevant and responsive to real-world scenarios. This proactive approach not only enhances the effectiveness of interventions but also strengthens overall public health strategies aimed at preventing radicalization.

### **3.8. Data collection and analysis**

Collecting and analyzing data on individuals identified through early warning systems is crucial for understanding patterns of radicalization and informing preventive strategies. Protecting patient confidentiality while sharing anonymized data for research and policy purposes is essential. Integrating robust health care response capacities into early warning systems will enable governments to enhance their ability to detect, respond to, and mitigate threats posed by terrorism effectively. This will not only safeguard public health and safety but also promotes resilience, social cohesion, and adherence to human rights principles in addressing the complex challenges of terrorism.

## **4. Conclusions**

In an era marked by escalating terrorism, strengthening public health responses is imperative. Effectively addressing terrorism requires not only robust security measures but also a commitment to public health initiatives. Focusing on the underlying social determinants of terrorism, such as socioeconomic disparities and political oppression, can lead to the development of more effective, community-oriented strategies. Training for health care professionals and community leaders is essential for identifying signs of radicalization and responding to the needs of affected populations. A multidisciplinary approach that integrates public health, law enforcement, and community organizations is vital for improving early warning systems and emergency preparedness. Policies must protect individual rights while ensuring community safety, fostering trust between the public and health authorities. Innovative technologies can enhance these efforts by providing new tools for surveillance and response. A proactive and comprehensive public health strategy is essential for mitigating the impacts of terrorism.

Prioritizing collaboration, ongoing evaluation, and community engagement significantly contributes to societal resilience in the face of terrorism-related challenges. Embracing a holistic understanding of health, safety, and human rights is key to building a safer, healthier world for all. In an increasingly interconnected world, the need for a universally accepted and dedicated approach to counter terrorism is paramount. Such a commitment would yield substantial global benefits, fostering enhanced cooperation and resilience among nations. A unified strategy,

grounded in shared principles and practices, would not only address the immediate challenges posed by terrorism but also contribute to long-term stability and security. The international community stands to gain significantly from a collaborative and comprehensive framework that prioritizes prevention, response, and recovery efforts in the face of this pervasive threat.

## **5. Acknowledgements**

The entirety of the research study, including the literature review, research idea conceptualization, methodology development, analysis, results interpretation, critical discussion, and conclusion formulation were conducted solely by the two authors. This work utilized the free OpenAI GPT-4o technology in a nearly negligible capacity. Its application was confined to minor tasks such as paragraphing, section partitioning, standardizing the reference list, finding synonyms for no more than ten words, and correcting inadvertent typographical errors.

## 6. Bibliography

- Adebayo, G. O. (2021). Counter-radicalization policies and policing in education: Making a case for human security in Europe. *Heliyon*, 7(2), e05721. <https://doi.org/10.1016/j.heliyon.2020.e05721>
- Arcos González, P., Castro Delgado, R., Cuartas Alvarez, T., & Pérez-Berrocal Alonso, J. (2009). Terrorismo, salud pública y sistemas sanitarios [Terrorism, public health and health services]. *Revista Española de Salud Pública*, 83(3), 361-370. <https://doi.org/10.1590/s1135-57272009000300002>
- Ashkenazi, I., & Hunt, R. C. (2019). You're it—You've got to save someone: Immediate responders, not bystanders. *Frontiers in Public Health*, 7, 361. <https://doi.org/10.3389/fpubh.2019.00361>
- Ashkenazi, I., Ohana, A., Azaria, B., Gelfer, A., Nave, C., Deutch, Z., Gens, I., Fadlon, M., Dahan, Y., Rapaport, L., Kishkinov, D., Bar, A., Tal-Or, E., Vaknin, N., Blumenfeld, A., Kessel, B., Alfici, R., Olsha, O., & Michaelson, M. (2012). Assessment of hospital disaster plans for conventional mass casualty incidents following terrorist explosions using a live exercise based upon the real data of actual patients. *European Journal of Trauma and Emergency Surgery*, 38(2), 113-117. <https://doi.org/10.1007/s00068-011-0154-x>
- Beaglehole, R. (2004). Terrorism and public health: A balanced approach to strengthening systems and protecting people. *Bulletin of the World Health Organization*, 82(1), 72. <https://doi.org/10.2471/BLT.04.018404>
- Chung, S., & Shanno, M. (2005). Hospital planning for acts of terrorism and other public health emergencies involving children. *Archives of Disease in Childhood*, 90(12), 1300-1307. <https://doi.org/10.1136/adc.2004.069617>
- Cole, L. A., Wagner, K., Scott, S., Connell, N. D., Cooper, A., Kennedy, C. A., Natal, B., & Lamba, S. (2014). Terror medicine as part of the medical school curriculum. *Frontiers in public health*, 2, 138. <https://doi.org/10.3389/fpubh.2014.00138>
- Comer, J., Furr, J., Beidas, R. S., & Weiner, C. L. (2008). Children and terrorism-related news: Training parents in coping and media literacy. *Journal of Consulting and Clinical Psychology*, 76(4), 568-578. <https://doi.org/10.1037/0022-006X.76.4.568>
- Cooper, D. L., Verlander, N. Q., Smith, G. E., Charlett, A., Gerard, E., Willocks, L., & O'Brien, S. (2006). Can syndromic surveillance data detect local outbreaks of communicable disease? A model using a historical cryptosporidiosis outbreak. *Epidemiology and Infection*, 134(1), 13-20. <https://doi.org/10.1017/S0950268805004802>
- Croner, C. M. (2003). Public health, GIS, and the internet. *Annual Review of Public Health*, 24, 57-82. <https://doi.org/10.1146/annurev.publhealth.24.012902.140835>
- Cui, D., Ou, C., & Lu, X. (2024). Evolution of the global terrorist organizational cooperation network. *PLoS One*, 19(1), e0281615. <https://doi.org/10.1371/journal.pone.0281615>
- Çalışkan, C., Dağ, N., & Kınık, K. (2023). Analysis of the Medical Consequences of Global Terrorist Attacks in Turkic States in the Last 50 Years by Weapon and Attack Type. *Disaster medicine and public health preparedness*, 17, e514. <https://doi.org/10.1017/dmp.2023.172>

- Çitlioğlu, E. (2004). Global terrorism and its effects on Türkiye's security dimension: A case study (Küresel terör ve Türkiye'nin güvenlik boyutuna etkileri: Uygulama çalışması.). *Journal of Defense Sciences (Savunma Bilimleri Dergisi)*, 3(1), 92. <https://doi.org/10.17134/sbd.11336>
- Çitlioğlu, E. (2005). Terrorism in international law (Uluslararası hukukta terörizm). *Geopolitics (Jeopolitik)*, 4(19), 27-33.
- Çitlioğlu, E. (2006). Psychological operations (Psikolojik harekât). *Turkish Homeland (Türk Yurdu)*, 26(222), 87-90.
- Çitlioğlu, E. (2008). Terrorism and its 'globalization'. *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, Vol. 47, 5-14. <https://doi.org/10.3233/978-1-58603-930-1-5>
- Çitlioğlu, E. (2009). Understanding the roots of terrorism: An evaluation of its origins and future. *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, 54,5-12. IOS Press. <https://doi.org/10.3233/978-1-58603-997-4-5>
- Çitlioğlu, E. (2012). Terrorism today and tomorrow: An analysis and projection study. In Homeland security organization in defence against terrorism. *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, Vol. 97, 1-14). <https://doi.org/10.3233/978-1-61499-047-5-1>
- Çitlioğlu, E. (2012). Understanding terrorism. Analyzing different dimensions and new threats in defence against terrorism. *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, Vol. 104, 1-10. <https://doi.org/10.3233/978-1-61499-159-5-1>
- Çitlioğlu, E. (2024). *Is terrorism eternal?* Center for Eurasian Strategic Studies (Avrasya Stratejik Araştırmalar Merkezi) Publications. (in print)
- Dai, D., & Wang, R. (2020). Space-time surveillance of negative emotions after consecutive terrorist attacks in London. *International Journal of Environmental Research and Public Health*, 17(11), 4000. <http://doi.org/10.3390/ijerph17114000>
- Disaster Preparedness Advisory Council. (2016). Medical countermeasures for children in public health emergencies, disasters, or terrorism. *Pediatrics*, 137(2), e20154273. <https://doi.org/10.1542/peds.2015-4273>
- Dormady, N., Szelazek, T., & Rose, A. (2014). The potential impact of an anthrax attack on real estate prices and foreclosures in Seattle. *Risk Analysis*, 34(1), 187-201. <http://doi.org/10.1111/risa.12059>
- Eichelberger, F. P. (2018). Background to the four stages of emergency management: The role of enterprise GIS. *Journal of Emergency Management*, 16(4), 229-243. <https://doi.org/10.5055/jem.2018.0372>
- Eisenman, D. P., Wold, C., Setodji, C., Hickey, S., Lee, B., Stein, B. D., & Long, A. (2004). Will public health's response to terrorism be fair? Racial/ethnic variations in perceived fairness during a bioterrorist event. *Biosecurity and bioterrorism: Biodefense strategy, practice, and science*, 2(3), 146-156. <https://doi.org/10.1089/bsp.2004.2.146>
- Foran, J. A., & Brosnan, T. M. (2000). Early warning systems for hazardous biological agents in potable water. *Environmental Health Perspectives*, 108(10), 993-995. <https://doi.org/10.1289/ehp.00108993>

- Gershon, R. R. M., Gemson, D. H., & Qureshi, K. (2004). Terrorism preparedness training for occupational health professionals. *Journal of Occupational and Environmental Medicine*, 46(12), 1204-1209.
- Gostin, L. O. (2002). Public health law in an age of terrorism: Rethinking individual rights and common goods. *Health Affairs*, 21(6), 79-93. <https://doi.org/10.1377/hlthaff.21.6.79>
- Hegre, H., Allansson, M., Basedau, M., Colaresi, M., Croicu, M., Fjelde, H., Hoyles, F., Hultman, L., Högladh, S., Jansen, R., Mouhle, N., Muhammad, S. A., Nilsson, D., Nygård, H. M., Olafsdottir, G., Petrova, K., Randahl, D., Rød, E. G., Schneider, G., & Vestby, J. (2019). VIEWS: A political violence early-warning system. *Journal of Peace Research*, 56(2), 155-174. <https://doi.org/10.1177/0022343319823860>
- Hunt, R., Ashkenazi, I., Deitchman, S., Dorn, B. C., Enders, J., Falk, H., Garbarino, L., Kapil, V., Madden, J., Marcus, L., Sarmiento, K., & Sasser, S. (2010). Preparing for the predictable surprise of a terrorist bombing. *Prehospital and Disaster Medicine*, 25(S1). <https://doi.org/10.1017/S1049023X00021828>
- Hurşitoğlu, M., Erdal, G. S., Akdeniz, E., Koçoğlu, H., Kocamaz, N., Tevetoğlu, I. O., Yücel, H., Harmankaya, O., Güven, A., Akarsu, M., Tükek, T., Öztürk, G., Doğan, H., Yılmaz, B. K., Güneş, M. E., & Kumbasar, A. B. (2019). Early effect of the fear of terrorism on a hospital's emergency department use and on the incidence of cardiovascular events: A Turkish multicenter study. *International Journal of Health Planning and Management*, 34(2), 872-879. <https://doi.org/10.1002/hpm.2756>
- Institute for Economics & Peace. (2024). Global terrorism index 2024: Measuring the impact of terrorism. Sydney. Available from <http://visionofhumanity.org/resources> and <https://www.economicsandpeace.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf> (Accessed October 16, 2024)
- International Peace Institute. (2012). World Health Organization (WHO). [https://www.ipinst.org/wp-content/uploads/2012/06/pdfs\\_terrorism-directory\\_27-WHO.pdf](https://www.ipinst.org/wp-content/uploads/2012/06/pdfs_terrorism-directory_27-WHO.pdf)
- Johnson, R. (2000). GIS technology for disasters and emergency management. *ESRI*. <https://www.esri.com/~media/files/pdfs/library/whitepapers/pdfs/disastermgmt.pdf>
- Kassirer, J. P. (2002). A medical early warning system. *Canadian Medical Association Journal*, 166(9), 1151-1152. <https://doi.org/10.1503/cmaj.1040421>
- Khilji, F. U. R., Raziq, A., Shoaib, M., Baloch, N. S., Raza, S., Iqbal, Z., Ishaq, R., Haider, S., Iqbal, Q., Ahmad, N., & Saleem, F. (2021). "Expecting the unexpected:" Nurses' response and preparedness of terrorism-related disaster events in Quetta City, Pakistan. *Frontiers in Public Health*, 9, 695143. <https://doi.org/10.3389/fpubh.2021.695143>
- Lerner, E. B., O'Connor, R. E., Schwartz, R., Brinsfield, K., Ashkenazi, I., Degutis, L. C., Dionne, J. P., Hines, S., Hunter, S., O'Reilly, G., & Sattin, R. W. (2007). Blast-related injuries from terrorism: an international perspective. *Prehospital Emergency Care*, 11(2), 137-153. <https://doi.org/10.1080/10903120701204714>
- Lindert, J., Bilsen, J., & McKee, M. (2018). Terrorist attacks: A public health issue. *European Journal of Public Health*, 28(6), 986. <https://doi.org/10.1093/eurpub/cky139>

- Maddah, N., Verma, A., Almashmoum, M., & Ainsworth, J. (2023). Effectiveness of public health digital surveillance systems for infectious disease prevention and control at mass gatherings: Systematic review. *Journal of Medical Internet Research*, 25, e44649. <https://doi.org/10.2196/44649>
- Mazerolle, L., Eggins, E., Cherney, A., Hine, L., Higginson, A., & Belton, E. (2020). Police programmes that seek to increase community connectedness for reducing violent extremism behaviour, attitudes and beliefs. *Campbell Systematic Reviews*, 16(3), e1111. <https://doi.org/10.1002/cl.2.1111>
- Mughal, R., DeMarinis, V., Nordendahl, M., Lone, H., Phillips, V., & Boyd-MacMillan, E. (2023). Public mental health approaches to online radicalisation: An empty systematic review. *International Journal of Environmental Research and Public Health*, 20(16), 6586. <https://doi.org/10.3390/ijerph20166586>
- National Academies of Sciences, Engineering, and Medicine, Health and Medicine Division, Board on Health Sciences Policy, & Forum on Medical and Public Health Preparedness for Disasters and Emergencies. (2017). *Countering violent extremism through public health practice: Proceedings of a workshop*. National Academies Press. <https://www.ncbi.nlm.nih.gov/books/NBK537576/>
- National Research Council (US) Panel on Biological Issues. (2002). *Countering bioterrorism: The role of science and technology*. National Academies Press.
- North Atlantic Treaty Organization. (2024, July 25). *Collective defense*. NATO. [https://www.nato.int/cps/en/natohq/topics\\_77646.htm](https://www.nato.int/cps/en/natohq/topics_77646.htm) (Accessed October 16, 2024)
- Prieto-Curiel, R., Walther, O., & Davies, E. (2023). Detecting trends and shocks in terrorist activities. *PLoS One*, 18(9), e0291514. <https://doi.org/10.1371/journal.pone.0291514>
- Rodoplu, U., Arnold, J. L., Tokyay, R., Ersoy, G., Cetiner, S., & Yücel, T. (2004). Mass-casualty terrorist bombings in Istanbul, Turkey, November 2003: Report of the events and the prehospital emergency response. *Prehospital and Disaster Medicine*, 19(2), 133-145. <https://doi.org/10.1017/S1049023X00001643>
- Roy, N., Kapil, V., Subbarao, I., & Ashkenazi, I. (2011). Mass casualty response in the 2008 Mumbai terrorist attacks. *Disaster Medicine and Public Health Preparedness*, 5(4), 273-279. <https://doi.org/10.1001/dmp.2011.80>
- Sadiq, A. A., Okhai, R., Tyler, J., & Entress, R. (2023). Public alert and warning system literature review in the USA: Identifying research gaps and lessons for practice. *Natural Hazards*, 117(2), 1711-1744. <https://doi.org/10.1007/s11069-023-05926-x>
- Schorscher, N., Kippnich, M., Meybohm, P., & Wurmb, T. (2022). Lessons learned from terror attacks: thematic priorities and development since 2001-results from a systematic review. *European journal of trauma and emergency surgery: official publication of the European Trauma Society*, 48(4), 2613-2638. <https://doi.org/10.1007/s00068-021-01858-y>
- Taviloglu, K., Yanar, H., Kavuncu, A., Ertekin, C., & Güloğlu, R. (2005). 2003 terrorist bombings in Istanbul. *International Journal of Disaster Medicine*, 3(1-4), 45-49. <https://doi.org/10.1080/15031430600694053>

- Tunalıgil, V. (2024). Sometimes there is no easy answer: Health care protection in conflict zones. *Turkish Journal of Public Health*, 22(2), 238-242.
- Tunalıgil, V. (2024). Developing geographic information systems in health care for earthquake-prone metropolitan cities: A methodological approach. *Medical Science and Discovery*, 11(9), 260-268. <https://doi.org/10.36472/msd.v11i9.1191>
- United Nations Office on Drugs and Crime. (2018). Counter-terrorism module 1: Introduction to the study of terrorism. [https://www.unodc.org/documents/e4j/18-04932\\_CT\\_Mod\\_01\\_ebook\\_FINAL.pdf](https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINAL.pdf)
- US Institute of Medicine Committee on Responding to the Psychological Consequences of Terrorism. (2003). *Preparing for the psychological consequences of terrorism: A public health strategy*. Stith Butler A, Panzer AM, Goldfrank LR, editors. Washington DC: National Academies Press US; 2003. National Academies Press. <https://www.ncbi.nlm.nih.gov/books/NBK221639/>
- Velasco, E., Agheneza, T., Denecke, K., Kirchner, G., & Eckmanns, T. (2014). Social media and internet-based data in global systems for public health surveillance: A systematic review. *Milbank Quarterly*, 92(1), 7-33. <https://doi.org/10.1111/1468-0009.12038>
- Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. *Science and Engineering Ethics*, 26(6), 2975-2984. <https://link.springer.com/article/10.1007/s11948-020-00254-w>
- Weine, S., & Kansal, S. (2019). What should global mental health do about violent extremism?. *Global Mental Health (Cambridge, England)*, 6, e14. <https://doi.org/10.1017/gmh.2019.12>
- Yang, Y., Pah, A. R., & Uzzi, B. (2019). Quantifying the future lethality of terror organizations. *Proceedings of the National Academy of Sciences of the United States of America*, 116(43), 21463-8. <https://doi.org/10.1073/pnas.1901975116>



# Defence Against Terrorism Review DATR Magazine



DATR, 2025; 1 : 51-78

Electronic Online ISSN 1307 - 9190

## New Era New Challenges: Web3-Based Social Media and Terrorism

Dr. Onur Ceran\*

### **Abstract**

*Social media platforms have revolutionized communication, enabling individuals to instantly connect, share, and access information. However, these platforms have also been exploited by terrorist organizations for recruiting members and spreading propaganda. In response, many social media companies have implemented algorithms and reporting systems to identify and remove terrorism-related content. At the same time, governments have sought to enhance legal frameworks and foster collaborations with tech firms to improve monitoring and intervention strategies. New challenges emerge as we transition toward Web3-based social media, which leverages blockchain technology for decentralization. The pseudonymous nature of blockchain can hinder accountability, making it easier for extremist groups to operate without detection.*

*Additionally, the use of decentralized naming systems complicates the tracking and removal of harmful content. The shift to decentralized platforms raises concerns about moderation and the potential for the proliferation of extremist material as traditional oversight mechanisms become less effective. This study sheds light on the evolving nature of online terrorist propaganda and its global response while also addressing*

---

\* Gazi University IT Department,

The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the author/s is affiliated.

*the implications of emerging technologies for counter-terrorism efforts. This analysis highlights the urgent need for innovative strategies to address these challenges in a rapidly changing digital landscape.*

### **Keywords**

*Terrorism, Social Media, Recruitment, Propaganda, Radicalization, Blockchain, Web3*

## **1. Introduction**

The rapid rise of social media has created unprecedented opportunities for communication and community-building. Platforms like Facebook, X, YouTube, Instagram, and TikTok have billions of users worldwide. While these platforms have many positive uses, they have also become breeding grounds for malicious activities, including terrorist recruitment and propaganda dissemination. Social media platforms offer services that allow individuals to express themselves and connect with others with similar interests. These platforms function as virtual communities where users can exchange ideas and interests. What makes social media stand out are its unique features, such as the option to create personal accounts, enabling users to access the platform. By setting up profiles, users can share personal details like profile photos and recent activities and engage with others through friending, creating groups, or following. Additionally, users can stay updated on news and announcements from others. Social media allows users to create and modify content in various forms, such as text, photos, and videos. Users can also interact with posts by commenting, sharing opinions, or liking content (Althero et al., 2023).

Propaganda is information, ideas, opinions, or images that present only one side of an argument, often distributed through media to influence people's views. Propaganda seeks to persuade people to sacrifice and set aside their personal needs, desires, or even their lives for a more significant cause or something perceived as more critical (Laskin, 2019). It is commonly mentioned in political contexts. Terrorist groups have adeptly exploited social media for propaganda in addition to radicalizing and recruiting individuals globally (Baines & O'Shaughnessy, 2014; Chaudhari & Pawar, 2021). They create online echo chambers where extremist ideas can proliferate unchecked, allowing them to reach vulnerable individuals in ways that were previously unimaginable. Historically, terrorist propaganda was carried out through more conventional means, such as print media, TV, and radio (Wilkinson, 1997). However, with the widespread adoption of the internet, terrorists quickly realized that social media offers a powerful tool for reaching a much larger and more diverse audience. The propaganda source does not interact directly with

its audience through social media but relies on media to get them. Its primary aim is to alter public opinion, eventually prompting a behavior change (Lock & Ludolph, 2020). Platforms like Twitter, Facebook, and YouTube allow terrorists to broadcast their messages to a global audience instantly. Recruitment videos, propaganda posters, and even live streams of attacks have all been used to galvanize supporters and inspire acts of violence (Weimann, 2010).

Terrorist propaganda on social media comes in many forms, including:

**Videos:** Terrorist groups produce professional-quality videos, including speeches, battle footage, and calls to arms. For example, violent videos depicting mass killings, executions, and torture have been used by DAESH both to intimidate or provoke their enemies and to attract sympathizers from around the world for recruitment purposes (Ozeren et al., 2018).

**Articles and Essays:** Extremist groups regularly publish articles that promote their ideologies, attack their enemies, and justify violence. These articles are often disseminated through social media and reach a wide audience, especially among those sympathetic to the cause. For example, DAESH disseminates its ideology through various media outlets to reach a broad audience. It used publications like *Dabiq* and *Rumiyah* magazines, the *Al-Naba* newsletter (Glausch, 2020).

**Memes and Visuals:** In its broadest sense, an internet meme is described as a 'catchy idea' that spreads online through images, texts, videos, tunes, or other digital content as a 'contagious' piece of information, an internet meme rapidly circulates among users, influencing and shaping the mindsets, behaviors, and actions of a social group. If an image propagates in numerous copies around digital networks, it can become a meme (Kalkina, 2020). Terrorists also leverage visual media, such as memes and infographics, to spread their message (Huey, 2015). These visuals are often designed to be provocative and easily shareable, targeting younger audiences who are more active on social media.

Terrorist propaganda often targets individuals who are susceptible to radicalization. This includes people who feel disenfranchised, isolated, or marginalized within their communities. Online propaganda offers a sense of belonging and purpose to those who might feel alienated in the real world. Ellul (1962 as cited in Winter, 2020) argues that propaganda does not excel at introducing new ideas; instead, it is robust in solidifying existing beliefs, gradually pushing individuals to act. This influence is most potent when propagandists surround audiences with messages aligning with their existing views. In such cases, previously abstract ideas become normalized, potentially leading individuals to adopt perspectives and behaviors that feel foreign to their original identity. For example, DAESH has specifically targeted young Muslim

women who are seeking adventure, feeling alienated or dissatisfied, searching for new life paths, coping with romantic issues, experiencing adolescent rebellion, or responding to various forms of personal discontent. These factors contribute to their decisions to pursue alternatives or make significant life changes (Perešin, 2015).

Terrorists use various tactics to engage potential recruits on social media, often starting with seemingly benign conversations before introducing extremist content. Since a join link is necessary to enter a channel or private messaging group, encountering propaganda accidentally is far lower than in more public web spaces (Clifford & Powell, 2019). Terrorist organizations may employ peer-to-peer recruitment after using hashtags related to trending topics to attract a broad audience. Radicalization tends to start subtly in recruitment, gradually intensifying as a bond of friendship and trust develops between the recruiter and the potential recruit. Once this relationship is established, radicalization often deepens, making the recruit more receptive to the recruiter's ideas and influence (Gürbüz, 2022). Once an individual interacts with extremist content, they may draw into a closed community where radicalization can occur. This tactic involves established members contacting potential recruits through direct messages or private chats. Almost all social media platforms allow their users to start a conversation through direct messaging part of the social media platform as well.

The responsibilities of social media platforms in combating terrorist recruitment and propaganda have become a critical focus in the fight against online extremism. As conduits for both global communication and radicalization, these platforms face expectations from governments to take proactive steps in identifying and removing extremist content to combat terrorism (Ford, 2020). One of the most significant responsibilities of social media platforms is identifying and removing terrorist content before it can spread. Law enforcement agencies worldwide are collaborating with major social media companies like Twitter and YouTube to remove thousands of instances of violent terrorist content. This joint effort aims to prevent the spread of extremist material online by blocking and deleting harmful content at scale (Weimann, 2016). In response to growing concerns, major platforms such as Facebook, YouTube, Twitter, and Instagram have invested heavily in developing technologies capable of detecting extremist content. Machine learning and artificial intelligence (AI) have become critical tools in automating the process of flagging content that violates community guidelines. AI algorithms are used to scan user-generated content such as posts, videos, and images for patterns that match known extremist materials (Macdonald et al., 2019)2019. For example, YouTube's Content ID system is designed to detect copyrighted material automatically but

has been adapted to flag extremist videos. Facebook also employs PDQ and TMK + PDQF hashing technologies for automated detection systems to identify terror-related content, using databases of known propaganda videos and images to create algorithms that prevent such content from being uploaded or shared (Gorwa et al., 2020). In addition to automated tools, social media companies have also deployed large teams of human moderators who review flagged content. These moderators play a crucial role in assessing borderline cases where AI tools may struggle to differentiate between legitimate political discourse and extremist content. Organizations possess the financial means to develop specialized in-house teams that address complex issues, including terrorist content, extremism, hate speech, misogyny, and other forms of harmful online activity (Amarasingam et al., 2021).

Given the global nature of terrorism, social media platforms are increasingly collaborating with governments and NGOs to combat online extremism. These partnerships aim to share intelligence, best practices, and technical expertise to address the growing threat of terrorism on social media. For example, the Global Internet Forum to Counter Terrorism (GIFCT) was established in 2017 by companies such as Meta (formerly Facebook), Microsoft, X (formerly Twitter), and YouTube to foster cross-platform cooperation in removing terrorist content (GIFTC, 2017). Through initiatives like the GIFCT, social media companies share databases of known terrorist content, enabling faster identification and removal across multiple platforms. These shared databases are updated regularly, ensuring that platforms can stay ahead of evolving tactics used by terrorist groups to spread propaganda.

As the threat of online terrorism grows, many governments have implemented stricter regulations that require social media platforms to take swift action against terrorist content. Laws such as the European Union's regulation on preventing the dissemination of terrorist content online mandate that platforms remove extremist material within a set timeframe, typically one hour after it is reported (Robinson, 2018). Failure to comply can result in hefty fines and legal consequences. To ensure compliance, social media companies have had to invest heavily in legal teams and compliance officers who monitor changes in global regulations. Moreover, platforms must continually update their content moderation policies to reflect evolving laws, which can be resource-intensive. However, a growing consensus is that such regulatory frameworks are necessary to ensure these platforms take their responsibilities seriously in combating terrorism (Gorwa et al., 2020).

However, these partnerships also raise concerns about the overreach of government power and the potential for state-led censorship. Some fear that collaboration between governments and platforms suppresses dissent or

politically sensitive content (Howard et al., 2011). As regulations make social media companies act more decisively (Chen, 2023), platforms must navigate a complex legal landscape, especially in regions where government definitions of terrorism and extremism may vary or conflict with international standards (West, 2021). Alternative social media platforms facilitate the creation of tight-knit, almost inaccessible communities that can foster echo chambers for hate speech and violent extremism. Unlike mainstream platforms, which actively remove such content, these alternatives allow such discourse to persist unchecked, reinforcing extremist beliefs among members (Walther & McCoy, 2021).

While many social media companies have implemented content moderation policies, including the removal of terrorist material, terrorist groups are quick to adapt, often shifting their content to new platforms to evade detection. Twitter managed to curb DAESH's influence on its platform by enhancing spam detection and swiftly banning DAESH-affiliated accounts. Despite efforts by DAESH media supporters to reestablish accounts, Twitter's stricter controls weakened their network. However, as Twitter became less viable for DAESH, they shifted to Telegram, where they could reestablish and continue spreading their messages (Prucha, 2016). The increasing use of encrypted messaging platforms presents a significant challenge for law enforcement. While encryption is essential for protecting privacy, it also allows terrorists to communicate without fear of interception. This makes it difficult for governments to gather intelligence on potential threats or to intervene (Davis, 2021). The power of encryption led blockchain technologies to emerge. As we transition toward Web3-based social media, which leverages blockchain technology for decentralization, terrorist groups may also find it as a new playing ground for their purposes. The pseudonymous nature of blockchain can hinder accountability, making it easier for extremist groups to operate without detection. Additionally, the use of decentralized naming systems complicates the tracking and removal of harmful content. The shift to decentralized platforms raises concerns about moderation and the potential for the proliferation of extremist material as traditional oversight mechanisms become less effective.

## **2. Blockchain**

Blockchain is a decentralized digital ledger technology that records and verifies transactions across a distributed network of nodes, ensuring that data is secure, transparent, and difficult to alter. Each transaction is grouped into a "block," and these blocks are sequentially linked together to form a chain. By decentralizing data storage across a network, blockchain becomes resilient against tampering

and censorship. It is a valuable tool for protecting free speech, open access to information, and freedom from centralized control (Tanriverdi et al., 2019).

Blockchain operates through a peer-to-peer network where each node holds a complete, updated ledger copy. When a transaction is initiated, it is broadcast to all nodes for validation through a consensus mechanism. The most widely known consensus algorithm is Proof of Work (PoW), used by Bitcoin, where nodes, or “miners,” solve complex cryptographic puzzles to validate transactions. This process is computationally intensive, making it challenging for any entity to alter the blockchain since it would require controlling over 50% of the network’s computational power (Narayanan et al., 2016). Another consensus mechanism, Proof of Stake (PoS), requires nodes to validate transactions based on the amount of cryptocurrency they “stake” as collateral, making PoS blockchains more energy-efficient while still secure against attacks (Wood, 2014). Each block contains a cryptographic hash of the previous block, a timestamp, and the transaction data, linking blocks in an immutable sequence. If anyone attempts to alter data within a block, the block’s hash changes, breaking the chain’s continuity and alerting the network. The blockchain’s decentralized, consensus-based structure prevents any individual node or authority from modifying data unilaterally (Narayanan et al., 2016), making it a powerful technology for anti-censorship. Blockchain’s anti-censorship properties stem primarily from its decentralized architecture, transparency, and cryptographic security. Unlike centralized systems where data is stored on single servers that can be manipulated or controlled, blockchain data is shared across thousands of nodes, making it almost impossible for any single entity to alter or censor data.

With data distributed globally across nodes, blockchain is highly resistant to censorship. No single authority can alter or delete data, which is particularly beneficial in settings where centralized entities or governments restrict access to information. Decentralized applications (DApps) built on platforms like Ethereum leverage this feature, supporting censorship-resistant services. For instance, storage networks such as the Inter Planetary File System (IPFS) offer decentralized file storage (Benet, 2014), reducing the risk of data suppression by central authorities. Blockchain’s transparency ensures that every transaction is publicly visible and verifiable. Once a transaction is recorded on the blockchain, it cannot be altered or erased, preserving the integrity and availability of data. This immutability makes blockchain an ideal tool for anti-censorship, as it prevents any single entity from retroactively changing records. For example, HELIOS Citizen Journalism, a blockchain-based application, aims to provide a tamper-resistant platform for content creators, allowing them to publish content without fear of censorship (Guidi et al., 2021).

Blockchain transactions are generally pseudonymous, meaning users can participate without revealing their real identities. This feature is crucial in authoritarian environments where individuals might face consequences for expressing dissent. While not fully anonymous, pseudonymity protects users from identification-based censorship. Additionally, privacy-oriented blockchain platforms such as Monero and Zcash add cryptographic enhancements for even greater privacy, allowing users to communicate and transact more securely and anonymously (Alam et al., 2023). Blockchain-based cryptocurrencies, such as Bitcoin and Ethereum, enable users to bypass traditional banking systems, which can be susceptible to governmental and institutional control. Unlike traditional banking, where transactions may be blocked, monitored, or even frozen, cryptocurrencies enable peer-to-peer transactions without intermediaries. This financial autonomy is invaluable for individuals in regions with economic restrictions, allowing them to access funds, purchase goods, and support dissenting voices without centralized oversight.

### **3. Web1.0, Web2.0 and Web3**

The internet has evolved dramatically over the past few decades, transitioning from the static, information-sharing Web 1.0 to the interactive, social, and user-centered Web 2.0. Currently, we're witnessing the rise of Web3, often known as the "decentralized web," which is powered by blockchain technology. While Web 2.0 enabled unprecedented levels of connectivity and user-generated content, it is heavily centralized, with control and data ownership concentrated among a few powerful tech companies. Web3, by contrast, proposes a more decentralized, secure, and user-driven internet where individuals retain ownership of their data and digital assets. Web 2.0 represents the internet we interact with today. It transformed the early "read-only" internet (Web 1.0) into an interactive, user-focused platform where people could create, share, and collaborate on content (Gan et al., 2023).

To make websites accessible online, they must be hosted on servers that accept requests from web browsers and respond to the website's content. Developers use web hosting providers' storage space for this purpose, while companies often manage their own servers to achieve the same goal. Web 2.0 relies on a client-server architecture characterized by centralized cloud storage and management, with major cloud and Content Delivery Network providers storing substantial amounts of user data in centralized databases. The Domain Name System (DNS), an essential part of Web 1.0 and today's Web 2.0 internet is a distributed database that matches computer names with numerical IP (Internet Protocol) addresses or vice versa (Bellovin, 1995). DNS translates the name people use to find a website

into the IP address the computer uses to serve that website. For example, if a user wants to access the web address [www.example.com](http://www.example.com) via a browser, DNS matches this domain name to an IP address (e.g. 81.82.83.84). This match is distributed globally within a hierarchy of authorities (Khormali et al., 2021). ICANN (Internet Corporation for Assigned Names and Numbers) oversees the DNS root zone and manages the allocation of Top-Level Domains (TLDs) As Donahoe (2017) noted, ICANN's role is vital in maintaining the stability of the global internet system. When a user attempts to connect to a server through a domain name, the DNS performs the IP address mapping. However, if the DNS lookup fails for any reason, access to the desired service will not be possible even if the target server is operational.

Web 2.0 platforms are controlled by corporations, which store vast amounts of user data, personalize content, and drive advertising revenue. This centralization has brought about significant privacy concerns as platforms like Facebook gather, analyze, and monetize user data, often with limited transparency or user control (Andreou et al., 2018). Users become products within this structure, where their data and activity generate revenue for corporations rather than personal benefits. Furthermore, centralized control over data and platform algorithms makes censorship possible, as companies can choose to restrict or remove content.

Web3, the next generation of the internet, offers a user-centric, on-chain ecosystem. Built on blockchain technology, it ensures transparency for on-chain data and transaction records through the decentralized ledger (Sun et al., 2024). Unlike Web1.0 and Web2.0, Web3 operates on a decentralized architecture, aiming to offer distributed cloud storage by building on foundational principles of peer-to-peer (P2P) networking and content addressing. For instance, IPFS (Inter Planetary File System) is a distributed file system protocol and network that offers an alternative to the internet's centralization and fundamentally changes how information is stored and shared on the web. Unlike the traditional web structure, IPFS stores files on nodes across the network through content addressability rather than on centralized servers. This innovative approach enables users to access files based on hash values, removing the dependency on a specific server for access (Benet, 2014). One of the most significant differences in Web3 is the concept of digital ownership. With blockchain-based Web3, users can own digital assets in the form of tokens, NFTs (non-fungible tokens), and cryptocurrencies, giving them greater control over their digital lives. These assets are managed directly by users' wallets, the final authority of the data, eliminating intermediaries like banks or tech companies (Sheridan et al., 2022). Web3 also enhances transparency and reduces censorship (Krause, 2024); no single entity can alter data stored on a decentralized

blockchain without consensus, making it inherently censorship-resistant. In addition, decentralized naming systems represent an evolution of traditional DNS, leveraging blockchain technology to provide a more secure, resilient, and user-controlled method of mapping human-readable names to digital addresses.

Unlike traditional DNS, which is hierarchical and managed by centralized authorities, decentralized naming systems operate on a distributed network. Systems like the Ethereum Name Service (ENS), Namecoin, and Blockstack allow users to register names, enabling ownership that is recorded on the blockchain (Su et al., 2021). When a user inputs a decentralized name (e.g., an ENS name), the query is sent to the blockchain network. Smart contracts handle the resolution. The registry contract stores the mapping of the name to an address stored on the blockchain. The user seeking to resolve the name must query the registry to identify the appropriate resolver and then retrieve the resolution results from that resolver. The resolved address can directly facilitate interactions, such as decentralized application (dApp) access (Xia et al., 2022).

Web3 platforms have the potential to replace centralized systems by leveraging smart contracts (Dal Mas et al., 2020). Simply, smart contracts are essentially code containers that digitally represent and replicate the terms of real-world contracts. At their core, contracts are legally binding agreements between two or more parties, where each party is obligated to uphold its commitments (Taherdoost, 2023). A smart contract is a computer program with self-verifying, self-executing, and tamper-resistant features. It enables code execution without requiring third-party intermediaries. Taking a transaction as input, it runs the corresponding code and generates output events. Integrating smart contracts with blockchain technology has become a significant area of focus due to their ability to facilitate peer-to-peer transactions while maintaining a publicly accessible, secure, and trustworthy database. Smart contracts are transparent, trackable, and irreversible, with all transaction details embedded, ensuring automatic execution (Mohanta et al., 2018). The creation of smart contracts differs significantly from traditional software engineering due to their unique development life cycles, which make updating or fixing flaws in deployed applications challenging through conventional version updates (Destefanis et al., 2018). Deployed smart contracts on the blockchain are immutable and publicly accessible to everyone except through a hard fork, which is a chain separation operation causing the old version to be no longer compatible with the new one (Wan et al., 2024). Decentralized Autonomous Organizations (DAOs) are organizational structures governed by smart contracts on the blockchain instead of a central authority or hierarchical management. These smart contracts enable automated decision-making, and any changes to the organization require

the consensus of stakeholders (Saurabh et al., 2023). Web3-based social media firms operate without a central authority or hierarchical management structure, relying instead on predetermined algorithms and protocols for governance and operations. These firms achieve efficient, autonomous development, management, and operation through a democratic validation process involving network users. For example, platforms like Steemit have been extensively studied as examples of this model. The emergence of Web3-based social media startups has also driven a fundamental shift in organizational structures, giving rise to a new type of entity known as the Decentralized Autonomous Organization (DAO) (Zhan et al., 2023).

#### **4. Web3-based social media**

Centralized social networks like Facebook, X, or Instagram rely on servers that store all the information users provide. This data can be utilized to analyze user preferences and behaviors or to deliver targeted ads. Decentralization has been considered a promising approach for social media. (Datta et al., 2010). Web3 based social media is used in this study as an umbrella term. Researchers use different terminology for social media platforms that are based on blockchain technology. (2020) used the term “Blockchain-based Online Social Media (BOSM)”, Jiang & Zhang (2019) preferred the term “Blockchain-Based Decentralized Online Social Network (BCOSN),” and Li et al. (2021) chose “Blockchain-based Social Media Platform (BBSMP)”. Web3-based social media platforms function similarly to traditional online social networks, allowing users to interact with one another. However, these platforms are managed autonomously by users through decentralized consensus protocols.

Web3-based social media addresses the challenges of traditional web 2.0 social media models by offering decentralization, where users and content creators become the owners. Web3-based social media platforms are typically governed and operated by their users and the broader community. Unlike conventional platforms controlled by centralized corporate entities, Web3-based social media platforms distribute data across the network’s nodes, ensuring decentralization. These platforms encourage users to create high-quality content and actively engage with others to maintain a vibrant content ecosystem. Issues such as data privacy breaches, excessive content censorship, and unannounced algorithm changes can effectively vanish in this decentralized framework. In practice, Web3-based social media platforms lack both a central authority and a hierarchical management structure. Governance and operations are efficiently handled through predefined algorithms or protocols. These platforms enable

autonomous development, management, and operations by utilizing a democratic validation process involving the network's users (Zhan et al., 2023). Guidi et al., (2021) describe key features of Web3-based social media platforms related to this study as follows:

**Data control and content management:** Decentralized networks operate without a central authority to collect or store data, allowing users to participate in the network actively and set their own rules for the content they create. Users gain greater control over their data, including how their content is monetized. The blockchain authentication process ensures robust security, making data breaches nearly impossible and providing maximum confidentiality. Unlike traditional social media platforms like Facebook or X, decentralized networks empower users with full control over their private data and published content, including the ability to determine its visibility and intended audience.

**Censorship and democratized governance:** Censorship is a critical issue in social media, as users often oppose restrictions on sensitive topics to uphold freedom of speech and expression. In traditional online social networks, content is reviewed and removed if it violates specific guidelines, with some countries, like China, exerting significant control over published material. In contrast, decentralized networks empower users with independence by eliminating central authorities, allowing them to establish their own rules for censorship and governance.

A blockchain-based decentralized application (DApp) is an application that typically uses web pages or mobile interfaces as its front-end and smart contracts as its back end. (Front-end and back-end represent two essential components of any application. The front-end encompasses the elements visible to users, such as buttons, checkboxes, graphics, and text messages, facilitating user interaction with the application. Conversely, the back-end consists of the data and infrastructure that underpin the functionality of the application). The front-end enables users to create transactions and submit them to their blockchain wallets. Once the user signs and confirms the transaction via the wallet, it triggers the smart contract associated with the DApp (J. Zhou et al., 2023). Web3-based social media platforms, being as social DApps, also uses web pages or mobile application interfaces in order for users' interaction, and smart contracts in order to transact on blockchain. Different web3-based social media platforms adopt different approaches to store data on the blockchain. Here, some of the main web3-based social media platforms will be introduced.

**Steemit:** Steemit is a blockchain-based social media DApp that creates communities where users are rewarded for sharing their voice (*Steemit*, 2024).

One of the earliest blockchain-based social platforms, Steemit operates on the Steem blockchain. It rewards users with cryptocurrency for creating, curating, and interacting with content. The posts and interactions are stored immutably on the blockchain. Community-driven curation through voting determines the visibility and reward distribution for posts. Delegated Proof-of-Stake (DPoS) consensus mechanism ensures efficient validation of transactions (Li et al., 2021).

**Hive.blog:** Hive is a fork of the Steem blockchain created to promote decentralization after controversy around Steem's acquisition by TRON. Hive.blog is a social network owned and operated by its users (Hive, 2024). Hive has two native tokens: HIVE and for rewarding contributions on the platform. It emphasizes decentralization, community governance, and resistance to censorship. Hive also enables transparent voting for governance and reward allocation. To mitigate the risk of collusion and enhance protection against governance attacks on the network, the Hive DPoS algorithm underwent revisions. Voting is restricted to users who utilize coins held in their accounts for over thirty days (Guidi et al., 2021).

**SocialX:** SocialX is a community-driven social media platform allowing users to publish photo and video content. It has many similarities to established social media platforms such as Facebook and Instagram. Still, there is one major difference: SocialX is a decentralized blockchain platform where everyone can earn cryptocurrency SOCX token rewards. As users upload images or videos, SocialX recognizes them as raw files. A second media file, serving as a duplicate, is then produced to improve application performance. The application leverages IPFS to decentralize both the original and the optimized files. All media-related information is sent to the primary Infura IPFS node. The IPFS hashes of the media files are documented in the corresponding post. The application also features the IPFS media files, complete with their published hash viewer (*The SocialX Ecosystem*, 2024).

**PeakD:** PeakD is a decentralized social media platform built on the Hive blockchain. It enables users to create, share, and monetize content in a transparent and censorship-resistant environment. Unlike traditional platforms, PeakD stores data on the Hive blockchain, ensuring that content and interactions are publicly accessible, secure, and immutable. The platform empowers users with complete control over their data and content while providing tools for engagement, such as rewards and voting systems. The primary purpose of PeakD is to offer a decentralized alternative for content creators and consumers, promoting freedom of expression and fair content monetization (*PeakD*, 2024).

In addition to the examples described above, there are web3-based social media platforms such as Peepth, Minds, Mirror, Sapien, Indorse and more.

These platforms' key and common feature is that they have integrated blockchain technology at some point in their operations for decentralization purposes. In the following section, the rules for removing content from publication and freezing or deleting accounts on traditional social media platforms and web3-based social media platforms will be examined and compared. Then the problems that may be encountered within the scope of terrorist propaganda and recruiting will be discussed together with the existing legal regulations.

### **5. Efforts on the Content**

Governments, corporations, and non-profit organizations have engaged in efforts to combat terrorist propaganda and recruitment on the internet, confronting a multifaceted dilemma regarding the most effective strategies to address a worldwide issue that can manifest in various forms across diverse segments of the web.

All countries have implemented all kinds of legal regulations regarding terrorist activities since their establishment and have made the necessary arrangements for online propaganda and recruitment. In addition, international organizations continued their global and regional studies; member countries tried to implement best-case practices. Security Council resolution 2354 (United Nations, 2017) expands upon the Council's presidential statement from 11 May 2016 (S/PRST/2016/6) and the "Comprehensive International Framework" (S/2017/375PDF). This resolution aims to implement legal and law enforcement strategies, foster public-private collaborations, and promote the creation of counter-narratives (*CTED Facesheet*, 2023). The European Union has provided both member states and stakeholders, such as online hosting providers, with a significant framework aimed at preventing and combating terrorist activities. This framework includes legislative measures, specifically directive 2017/541/EU and the proposal for a regulation concerning terrorist content online, as well as non-binding instruments like the Commission Recommendation (EU) 2018/3347 and various voluntary agreements established by states or stakeholders. Europol actively engages in the prevention of terrorism through its dedicated branch, the European Counter-Terrorism Centre (ECTC). This center has initiated the establishment of Internet Referral Units (IRUs), which are tasked with detecting, investigating, and referring terrorist-related illicit content found online to Member States and hosting providers (Sachetti, 2021)2021. The European Commission, in its document titled "Communication on Tackling Illegal Content Online: Towards Enhanced Responsibility of Online Platforms," has advised technology companies to actively seek out illegal content on their platforms utilizing artificial intelligence. It emphasized that online platforms should have the capability to make prompt decisions without the necessity of a court order

or administrative directive. The Commission believes that online platforms can implement these suggested proactive strategies without jeopardizing their liability exemption as outlined in the e-Commerce Directive (Huszti-Orban, 2018).

The Global Internet Forum to Counter Terrorism (GIFCT), founded in 2017 by Meta, Microsoft, YouTube, and X, is an NGO dedicated to preventing the misuse of digital platforms by terrorists and violent extremists. With over 30 member platforms, GIFCT fosters technical collaboration, research, and knowledge-sharing to combat extremist content online. Its efforts align with the Christchurch Call to Action, initiated after the 2019 Christchurch Mosque shootings, and a nine-point plan to eliminate extremist content. Guided by four core goals, it empowers tech companies, engages stakeholders, promotes civil dialogue, and enhances understanding of extremist operations. To achieve this, GIFCT adheres to a nine-point plan with five individual actions and four collaborative initiatives (GIFTC, 2017):

Five Individual Actions:

**Terms of Use Updates:** Platforms will explicitly prohibit terrorist and violent extremist content in their terms of use, community standards, and acceptable use policies, providing a clear basis for content removal and account actions.

**User Reporting Tools:** Platforms will implement user-friendly mechanisms for reporting inappropriate content, ensuring clarity and prompt action on flagged terrorist or extremist materials.

**Enhancing Technology:** Continued investment in advanced technology, such as digital fingerprinting and AI, will improve the detection and removal of terrorist content.

**Livestreaming Checks:** Measures like streamer ratings, account validation, and event moderation will be introduced to reduce the risk of livestreaming extremist content tailored to the context of each service.

**Transparency Reports:** Regular reports will provide data on detecting and removing extremist content, supported by clear and explainable methodologies.

Four Collaborative Actions:

**Shared Technology Development:** Collaborative efforts with governments, NGOs, and academic institutions will focus on creating shared data sets, open-source tools, and collective contributions to improve detection and removal technologies.

**Crisis Protocols:** A unified crisis response protocol will ensure quick and coordinated action during active or emerging events, with incident management teams facilitating information sharing among stakeholders.

Public Education: Joint efforts will aim to educate the public on recognizing and reporting extremist content, as well as discouraging its spread.

Combatting Hate and Bigotry: Collaborative research and support for NGOs will address the root causes of extremism and hate, emphasizing the connection between online hate and offline violence while promoting pluralism and respect.

Web3-based social media platforms also notify their users about content related to violence in a broad sense and terrorism in particular, according to the roadmaps they have determined. Steemit warns users on their terms and services section: “When accessing or using the Services, you agree that you will not commit any unlawful act, and that you are solely responsible for your conduct while using our Services. Without limiting the generality of the foregoing, you agree that you will not use our Services to pay for, support or otherwise engage in any activity prohibited by law, including, but not limited to illegal gambling, fraud, money-laundering, or terrorist financing activities” (*Steemit*, 2024). Hive.blog warns users on their terms and services section: “By accessing or utilizing the Services, you acknowledge your commitment to refrain from engaging in any illegal activities and accept full responsibility for your actions while using our Services. Furthermore, without restricting the broad scope of this obligation, you agree not to use our Services for any unlawful purposes, including but not limited to illegal gambling, fraud, money laundering, or financing of terrorism” (*Hive*, 2024). SocialX announces that they strictly forbid child porn, human trafficking, drugs, terrorism, and more. It also empowers their community to forbid content if they think it does not follow the SocialX community guidelines (*The SocialX Ecosystem*, 2024). PeakD offers mechanisms to filter NSFW (Not Safe for Work) content, which are enabled by default settings. However, these filters’ functionality depends on users accurately tagging their posts. While being aware that some inappropriate content may still be present due to user mislabeling or negligence (*PeakD*, 2024).

## **6. Comparison of Efforts and the Possible Challenges**

Major traditional web 2.0-based social media platforms share a general approach to removing terrorism-related content; their effectiveness varies based on factors like enforcement strategies, reliance on AI, and the balance between privacy and content moderation. Although there has not been a hundred percent success in detecting terrorist propaganda or recruitment content published on social media platforms, it is technically very easy for platforms that host the content on their centrally managed servers to remove it from publication and/or block access to it. Altering the value of the database or even deleting it finalizes all the transactions.

The laws and policies designed to tackle violent extremism similarly encounter issues related to definitions. The phrase ‘violent extremism,’ along with associated terms like ‘extremism’ and ‘radicalization,’ is widely used in current political dialogue across international, regional, and national platforms. Nevertheless, there are no internationally recognized definitions for these terms. Many definitions present in domestic legislation and policies have been criticized for their lack of clarity and for sometimes covering activities that are lawful according to international human rights standards. As Huszti-Orban, (2018) describes online platforms as “De Facto Content Regulators,” it is common for terms of service and community standards to be written in imprecise language, which does not adequately clarify the scenarios that could result in blocked content. Heller, (2020) points out that the definition of terrorism presents significant challenges, as articulated by Tech Against Terrorism, a nonprofit partner of GIFCT. Tech Against Terrorism acknowledges the lack of a universal definition for terrorism. This uncertainty complicates their content moderation efforts.

Moreover, it is often hard to determine if a video is promoting terrorist ideologies or if it is an essential news report highlighting human rights violations. For this reason, it is possible that an application for content removal or access blocking made by the applicant country for content that it defines as terrorist propaganda or advocacy may be rejected because the social media platforms do not describe the content in question similarly. In such a case, even if states cannot ensure that the content is removed from publication, they can choose to block access to the content by applying national legal rules to reduce the access of content containing terrorist propaganda to more people. This is possible with the traditional Domain Name System and the hosting method on central servers on which web1.0 and web2.0 are built.

For example, The Turkish Law for Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications No. 5651 regulates the prevention of access to publications or removal of illegal content by court order. Article 8/17 declares that prevention of access is processed by blocking the related content through an individual URL if technically possible; if not, the entire website may be blocked from being accessed. In the context of managing terrorism-related content on Web 1.0 or Web 2.0, two distinct blocking techniques may be utilized. The first technique is referred to as “DNS tampering,” which consists of modifying the internal DNS records of a website to redirect user requests to a different IP address. For example, if the social media site [www.facetweetgam.com](http://www.facetweetgam.com) is hosted at the IP address 10.0.0.5, an ISP could alter the DNS entry for this site to redirect to 192.168.0.5, a

hypothetical address that could display a message regarding a court order against accessing [www.facetweetgam.com](http://www.facetweetgam.com). As a result, users querying [www.facetweetgam.com](http://www.facetweetgam.com) would be redirected to 192.168.0.5. The second technique is known as IP blocking, which involves blocking access to the entire website by restricting traffic to its hosting IP address. In this scenario, if a user attempts to access the IP address 10.0.0.5, the ISP will block all incoming and outgoing traffic to that address.

The content removal and access blocking efforts described above will be more challenging when it comes to web3-based social media environments. To explain this situation better, it would be appropriate first to examine the white papers and terms of services published by those mentioned above on web3-based social media platforms.

In Steem whitepaper (S. Whitepaper, 2018b) it is declared that “Steem is a decentralized network operated by witnesses in jurisdictions around the world. All user actions are publicly recorded on the blockchain and can be publicly verified. This means that no single entity can censor content that STEEM holders value. Individual websites such as [steemit.com](http://steemit.com) may censor content on their particular site. Still, content published on the blockchain is inherently broadcast traffic, and mirrors worldwide may continue to make it available”. Like Steem, the Hive platform announces that “Hive is by design a decentralized blockchain that is sustained by geographically distributed servers and nodes. Every transaction is transparently and chronologically entered into blocks and signed onto the public ledger. All transactions entered onto the Hive blockchain have the element of finality and, once confirmed in its three-second blocks, are irreversibly signed. Altering the content of recorded transactions and blocks is not possible as that would alter the state of the blockchain post-finality. Therefore, taking the default unalterability into account, no content on the Hive blockchain may be arbitrarily censored or altered in any way, shape, or form. Hive does not regulate its APIs or provide constraints on the type of endpoints that may be built on it. Individual front-ends and websites may present or not present segments of Hive content as they deem fit. This does not adversely impact the availability of the material stored on the Hive blockchain. With its censorship-resilient design, Hive is a dedicated proponent of free speech and transparency” (H. Whitepaper, 2020).

As can be seen from the Steem and Hive whitepapers, they are decentralized blockchain platforms that prioritize transparency and censorship resistance through their architecture. Both platforms record all actions on their respective blockchains, which are public, immutable, and globally accessible. Content is permanently recorded on the blockchain and remains accessible globally through decentralized

nodes. However, individual websites, such as Steemit.com or Hive.io, can choose what content to display. This enables platform-level moderation without affecting the availability of the underlying data. Steem's blockchain supports mirrored nodes worldwide, making content available regardless of moderation decisions by specific websites. Hive's design emphasizes unregulated APIs, allowing developers to build diverse endpoints and ensuring that no constraints hinder access to blockchain-stored content, which means that they empower individual platforms to decide how content is presented, creating a nuanced interplay between moderation and accessibility. In this way, since all terrorist content is written on the blockchain, even if Steem or Hive blocks access to this content through their own user interfaces, another coder can create a design that will make all of the content publicly available through their own web user interface. In this case, content created for terrorist propaganda or recruiting purposes will be accessible through a website published anywhere in the world.

SocialX also declares that, "We will empower our community to forbid content if they think it is not following the SocialX community guidelines. Everyone who engages within the community to maintain this environment will also be rewarded so that we set a healthy incentive for people to manage content. As SocialX will be decentralized, we are not able to fully forbid or prevent the abovementioned topics, but we will help our voted community managers with tools and algorithms to easily access NSFW (Not Safe for Work) content and flag it as inappropriate" (S. Whitepaper, 2018a).

As noted also in the whitepaper of SocialX, when a user posts an image or video to the platform, it is stored on IPFS. The Interplanetary File System (IPFS) is a peer-to-peer protocol that facilitates storing and accessing files and websites, as described in the IPFS whitepaper. This open-source initiative focuses on developing a sustainable and decentralized data storage and distribution method. It comprises a protocol and a network, and it is widely utilized by various projects and users, aiming for effective and seamless file sharing. In contrast to the traditional location-based addressing system used by HTTP through DNS, where a single server hosts multiple files, IPFS disperses files throughout the network, uniquely identifying each file by its cryptographic hash, which is determined by its content. IPFS resists censorship using a decentralized and distributed architecture to store and share content. Instead of locating files using URLs tied to specific servers, IPFS uses content addressing. This ensures that as long as someone has the hash, they can retrieve the file, regardless of where it is stored. Files on IPFS are broken into smaller chunks and distributed across multiple nodes in the network. No single server or central authority controls the data, making it impossible for a government

or a platform itself to block or remove content from the entire network. Anyone with a copy of the content can act as a host. This redundancy ensures that even if one node is taken down, the content remains accessible from other nodes. Users retrieve files directly from other nodes instead of centralized servers, bypassing traditional internet infrastructure that governments might control. Traditional censorship often involves blocking websites or servers, as mentioned above. IPFS, however, has no central server. Even if governments shut down specific nodes, the content remains accessible through other nodes globally—for instance, a controversial document shared on IPFS. Even if a government blocks a website hosting the file, users with the file’s hash can still retrieve it from other nodes in the network. The distributed nature of IPFS makes it virtually impossible to remove all copies of the content. That is why SocialX declares that they are not able to forbid or prevent the topics fully, but it can flag the content as not safe for work.

PeakD declares in the Legal Terms of Service section (*PeakD*, 2024) that the platform interacts with Hive blockchain via Hive.io. It is also specified that “PeakD offers tools to filter NSFW (Not Safe for Work) content, which is enabled by default. However, these filters rely on users properly tagging their posts. Guardians should ensure these filters remain in place but understand that some inappropriate content may still appear due to user mislabeling or neglect. PeakD gives users control over their content consumption and creation while requiring them to comply with local laws and responsibly mark NSFW material. By using PeakD, you acknowledge that it is your responsibility to understand the impact of your actions. PeakD provides tools to help you interact with the Hive blockchain, but you are solely responsible for your actions and the consequences of those actions. PeakD is a frontend tool for interacting with the Hive blockchain and does not control or manage the blockchain itself. By posting content through PeakD, you acknowledge that your content is stored on the Hive blockchain, which is public and decentralized. PeakD cannot control where or how your content is displayed on third-party services using the same blockchain data. Once content is posted on Hive, it is beyond PeakD’s control to delete or modify it. You are responsible for understanding the permanent nature of blockchain and making informed choices before posting any data. Once your content is on the blockchain, it cannot be deleted or altered by PeakD or any other service. While you can modify how it is displayed on PeakD, the original data remains part of the permanent blockchain record.” When the terms of service is examined, it is obvious that PeakD has no power to moderate the content on the blockchain like in Steemit or Hive.io. Even if PeakD moderates or filters certain content’s display, the data remains immutable and accessible through other nodes, frontends, or tools interacting with the blockchain. This decentralization ensures no single authority can

fully remove or suppress the content. PeakD warns its users that they will be held responsible for any illegal content and that users should tag the content as NSFW. However, it would be against the natural flow of life for users to tag their own terrorist propaganda and/or recruitment purposeful posts as NSFW.

## **7. Discussion**

While Web 2.0 revolutionized communication and content creation, its centralized structure has led to data privacy, control, and censorship issues. Blockchain-based Web 3.0 aims to address these problems by creating a decentralized, user-centric internet where individuals have greater control over their data and digital assets. As Web 3 evolves, it holds the potential to transform the digital landscape by returning power to users, fostering transparency, and enabling new forms of ownership and governance. The integration of IPFS and blockchain technology is being expanded by projects such as Filecoin, which is evolving into a marketplace that offers economic incentives for file storage and access services (Psaras & Dias, 2020). Users can earn tokens in exchange for hosting files. This symbiotic relationship increases the ecosystem's robustness and offers a decentralized alternative to traditional cloud storage solutions. Network users collect tokens through engaging in various social activities, apply tokens to gain corresponding rights and interests, and receive network growth dividends through the value of tokens, therefore framing a two-way value co-creation between online users and web3-based social media platforms (Zhan et al., 2023).

However, web3-based social networks present challenges related to resource limitations. The scalability challenge becomes evident as the number of nodes and transactions within a blockchain network grows. This concern is particularly significant in prominent public blockchain applications, where each node is required to store and perform computational tasks to validate every transaction. Consequently, public blockchains consistently require substantial computational resources, high-bandwidth internet connectivity, and extensive storage capacity (Khan et al., 2021). Transaction throughput and latency are the primary performance metrics under scrutiny in the blockchain domain, and many contemporary public blockchain systems have yet to achieve an acceptable level of Quality of Service (QoS) in these areas (Q. Zhou et al., 2020). Although there are a lot of studies in literature trying to mitigate scalability problems (Kim & Park, 2024; Rao et al., 2024), no one will use a decentralized social media platform if it takes several seconds to load an image or a minute to load a video as noted in the whitepaper of SocialX. The nature of propaganda requires it to reach a large number of people, and traditional social media platforms make this possible. Social media can be

said to reduce the cost of participating in violent extremist and terrorist activity (Argomaniz, 2015) as well; hence, public blockchain requirements may not satisfy the purpose of terrorist propaganda in this regard.

Husztí-Orban, (2018) argues that the terms of service and community standards are often articulated in a manner that fails to provide adequate clarity regarding the specific conditions under which content may be blocked, removed, or restricted, as well as the circumstances that may lead to the limitation or termination of access to a service. Users face significant challenges in contesting decisions related to the restriction of content or access. Furthermore, as private entities, these platforms typically operate with minimal democratic or independent oversight. Nevertheless, the increasing involvement of private organizations, such as social media companies, in roles traditionally associated with public interest within Internet governance appears inevitable, given that public authorities often lack the necessary human or technical resources to fulfill these responsibilities effectively. In addition, Saltman, (2020) emphasizes that it is insufficient to rely solely on technology to combat malicious activities. The reality is that human involvement is essential in this endeavor. To effectively curb the dissemination of terrorist content across the internet, collaboration with various stakeholders is imperative. Achieving the right equilibrium among technology, human insight, and partnerships is crucial. While technology aids in managing the vastness and rapidity of online content, human expertise is vital for comprehending the complex nature of terrorism and violent extremism globally, as well as for monitoring shifts in adversarial tactics. Moreover, GIFCT's criteria do not consider freedom of expression, particularly regarding the risk of excessive enforcement that could occur when combined with existing technical limitations (Heller, 2020).

The immutability and public availability offered by blockchain technology can benefit both Web 2.0-based social media platforms and governments engaged in combating terrorism. Data stored publicly on a blockchain is accessible to everyone. The transparency provided by the transaction ledger facilitates the real-time observation of nefarious actors, ensuring that their transactions can be traced from virtually any location. Many governments are currently harnessing these tools to effectively counteract the actions of these individuals (Consensus, n.d.). Government institutions fighting terrorism could mirror the data relevant to their country and apply big data analysis and natural language processing (NLP) techniques. Through such analyses, they could gain new insights about the terrorist organizations being propagandized. Sharing these analyses with traditional social media platforms would enable them to better understand the complex global/regional nature of terrorism, as mentioned earlier. It would also allow these platforms

to outsource human or technical resources for these purposes. This collaboration could lead to more informed decisions regarding content removal and information requests in the future.

## **8. Conclusion**

This study has examined the complex interplay between social media, terrorism, and counter-terrorism efforts, focusing on the transition from Web 2.0 to the emerging Web3 paradigm. While Web 2.0 offered unprecedented connectivity and content creation opportunities, it created vulnerabilities exploited by terrorist organizations for recruitment and propaganda dissemination. In response, platforms and governments implemented algorithms, reporting systems, and legal frameworks, often facing challenges related to content moderation, freedom of expression, and resource limitations. The advent of Web3, with its decentralized, blockchain-based architecture, promises user empowerment and enhanced data privacy but introduces new complexities for counter-terrorism.

While the pseudonymous nature of blockchain and decentralized naming systems hinders accountability and complicates the tracking and removal of harmful content, Web3's inherent scalability challenges, particularly concerning transaction throughput and latency, pose significant obstacles to its widespread adoption for social networking, potentially limiting the reach of terrorist propaganda compared to Web 2.0 platforms. This contradicts the fundamental requirement of propaganda to reach a large audience quickly and efficiently. Although projects offer decentralized storage solutions and incentivize user participation, the resource-intensive nature of public blockchains necessitates substantial computational power, bandwidth, and storage, potentially hindering the user experience and further limiting scalability. The very nature of terrorist propaganda, which benefits from the broad reach and low cost of participation afforded by Web 2.0, may be incompatible with the current limitations of Web3.

Despite these challenges, blockchain technology offers potential benefits for counter-terrorism efforts. The immutability and public availability of blockchain data provide transparency and facilitate real-time illicit activity tracking. Governments can leverage this data, applying big data analytics and NLP techniques to gain insights into terrorist networks and propaganda strategies. Sharing these analyses with Web 2.0 platforms can enhance their understanding of the complex global landscape of terrorism and inform content moderation decisions. Combining technological tools with human expertise and inter-organizational partnerships, this collaborative approach is crucial for effectively combating online terrorism.

Relying solely on technology is insufficient. Clear terms of service, independent oversight, and international collaboration are essential to balance security concerns with freedom of expression and prevent excessive enforcement. Therefore, while Web3 presents new challenges for counter-terrorism, its underlying technology also offers valuable tools that, when combined with human intelligence and strategic partnerships, can contribute to a more effective and nuanced approach to combating online extremism. Future research should focus on developing legal regulations and fostering collaboration between stakeholders to mitigate the risks posed by online terrorism in both Web 2.0 and the evolving Web3 landscape.

## 9. References

- Alam, M. H., Basit, A., & Arif, F. (2023). A Comparative Analysis of Implementation of Privacy by Design Principles on different Blockchain platforms. *2023 International Conference on Communication Technologies (ComTech)*, 111–116. <https://ieeexplore.ieee.org/abstract/document/10165248/>
- Althero, Z., Syahreza, J., & Ortiz, A. (2023). Blockchain Technology for Authentication and Validation Social Network Accounts. *Blockchain Frontier Technology*, 3(1), 32–38. <https://doi.org/10.34306/bfront.v3i1.358>
- Amarasingam, A., Maher, S., & Winter, C. (2021). How Telegram disruption impacts jihadist platform migration. *Centre for Research and Evidence on Security Threats*, 27.
- Andreou, A., Venkatadri, G., Goga, O., Gummadi, K. P., Loiseau, P., & Mislove, A. (2018). Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. *Proceedings 2018 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. <https://doi.org/10.14722/ndss.2018.23191>
- Argomaniz, J. (2015). European Union responses to terrorist use of the Internet. *Cooperation and Conflict*, 50(2), 250–268. <https://doi.org/10.1177/0010836714545690>
- Baines, P. R., & O'Shaughnessy, N. J. (2014). Al-Qaeda messaging evolution and positioning, 1998–2008: Propaganda analysis revisited. *Public Relations Inquiry*, 3(2), 163–191. <https://doi.org/10.1177/2046147X14536723>
- Bellovin, S. M. (1995). Using the Domain Name System for System Break-ins. *USENIX Security Symposium*. [https://www.usenix.org/publications/library/proceedings/security95/full\\_papers/bellovin.pdf](https://www.usenix.org/publications/library/proceedings/security95/full_papers/bellovin.pdf)
- Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System* (arXiv:1407.3561). arXiv. <https://doi.org/10.48550/arXiv.1407.3561>
- Chaudhari, D. D., & Pawar, A. V. (2021). Propaganda analysis in social media: A bibliometric review. *Information Discovery and Delivery*, 49(1), 57–70. <https://doi.org/10.1108/IDD-06-2020-0065>
- Chen, Z. (2023). Limitations of Chinese Social Media Censorship and Their Relationships with Government Policies. *Journal of Education, Humanities and Social Sciences*, 8, 204–209.

- Clifford, B., & Powell, H. (2019). Encrypted extremism: Inside the English-speaking Islamic state ecosystem on telegram. *The George Washington University Program on Extremism*, 27–53.
- Consensys. (n.d.). *Crypto Regulations*. <https://consensys.io/crypto-regulations>
- CTED Facesheet. (2023). United Nations Security Council Counter-Terrorism Committee Executive Directorate. [https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/cted\\_factsheets\\_feb\\_2023\\_0.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/cted_factsheets_feb_2023_0.pdf)
- Dal Mas, F., Dicuonzo, G., Massaro, M., & Dell'Atti, V. (2020). Smart contracts to enable sustainable business models. A case study. *Management Decision*, 58(8), 1601–1619. <https://doi.org/10.1108/MD-09-2019-1266>
- Datta, A., Buchegger, S., Vu, L.-H., Strufe, T., & Rzdca, K. (2010). Decentralized Online Social Networks. In B. Furht (Ed.), *Handbook of Social Network Technologies and Applications* (pp. 349–378). Springer US. [https://doi.org/10.1007/978-1-4419-7142-5\\_17](https://doi.org/10.1007/978-1-4419-7142-5_17)
- Davis, A. L. (2021). Artificial Intelligence and the Fight Against International Terrorism. *American Intelligence Journal*, 38(2), 63–73.
- Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 19–25. <https://ieeexplore.ieee.org/abstract/document/8327567/>
- Donahoe, E. (2017). Governance Challenges in the Global Digital Ecosystem. *Innovations in Global Governance*, 24.
- Ford, P. (2020). Combatting terrorist propaganda. *Journal of Policing, Intelligence and Counter Terrorism*, 15(2), 175–186. <https://doi.org/10.1080/18335330.2020.1780298>
- Gan, W., Ye, Z., Wan, S., & Yu, P. S. (2023). Web 3.0: The Future of Internet. *Companion Proceedings of the ACM Web Conference 2023*, 1266–1275. <https://doi.org/10.1145/3543873.3587583>
- GIFTC. (2017). [Corporation]. Global Internet Forum to Counter Terrorism. GIFTC.org
- Glausch, M. (2020). Infographics and their role in the IS propaganda machine. *Contemporary Voices: St Andrews Journal of International Relations*, 1(3), 32–50.
- Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, 7(1), 205395171989794. <https://doi.org/10.1177/2053951719897945>
- Guidi, B. (2020). When Blockchain meets Online Social Networks. *Pervasive and Mobile Computing*, 62, 101131. <https://doi.org/10.1016/j.pmcj.2020.101131>
- Guidi, B., Ricci, L., Nyffenegger, R., & Ribback, R. (2021). HELIOS CJ App: The decentralization of the Citizen Journalism. *Proceedings of the Conference on Information Technology for Social Good*, 31–36. <https://doi.org/10.1145/3462203.3475901>
- Gürbüz, Ö. (2022). Internet-Supported Recruitment of Terrorist Organizations: An Analysis of the Early Stages of the Recruitment Process and Countermeasures to Prevent Terrorist Recruitment. *Defence Against Terrorism Review*, 16, 35–69.
- Heller, B. (2020). Combating terrorist-related content through AI and information sharing. *Algorithms*, 1–8.
- Hive. (2024). [Social Media]. Hive Blog. <https://hive.blog/>

- Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media. *The Communication Review*, 14(3), 216–232. <https://doi.org/10.1080/10714421.2011.597254>
- Huey, L. (2015). This is not your mother's terrorism: Social media, online radicalization and the practice of political jamming. *Contemporary Voices: St Andrews Journal of International Relations*, 6(2). <https://cvir.st-andrews.ac.uk/index.php/up/article/view/1159>
- Husztí-Orban, K. (2018). Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement. *2018 10th International Conference on Cyber Conflict (CyCon)*, 227–244. <https://ieeexplore.ieee.org/abstract/document/8405019/>
- Jiang, L., & Zhang, X. (2019). BCOSN: A Blockchain-Based Decentralized Online Social Network. *IEEE Transactions on Computational Social Systems*, 6(6), 1454–1466. <https://doi.org/10.1109/TCSS.2019.2941650>
- Kalkina, V. (2020). Between Humour and Public Commentary: Digital Re-appropriation of the Soviet Propaganda Posters as Internet Memes. *Journal of Creative Communications*, 15(2), 131–146. <https://doi.org/10.1177/0973258619893780>
- Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, 11(20), 9372. <https://doi.org/10.3390/app11209372>
- Khormali, A., Park, J., Alasmay, H., Anwar, A., Saad, M., & Mohaisen, D. (2021). Domain name system security and privacy: A contemporary survey. *Computer Networks*, 185, 107699. <https://doi.org/10.1016/j.comnet.2020.107699>
- Kim, D., & Park, S. (2024). Blockchain-Based Scalable and Reliable Social Networking Platform. *IEEE Access*, 12, 140277–140294. <https://doi.org/10.1109/ACCESS.2024.3465665>
- Krause, D. (2024). The Rise of Web3: Opportunities and Challenges. Available at SSRN 4895353. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4895353](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4895353)
- Laskin, A. V. (2019). Defining propaganda: A psychoanalytic perspective. *Communication and the Public*, 4(4), 305–314. <https://doi.org/10.1177/2057047319896488>
- Li, C., Palanisamy, B., Xu, R., Xu, J., & Wang, J. (2021). SteemOps: Extracting and Analyzing Key Operations in Steemit Blockchain-based Social Media Platform. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 113–118. <https://doi.org/10.1145/3422337.3447845>
- Lock, I., & Ludolph, R. (2020). Organizational propaganda on the Internet: A systematic review. *Public Relations Inquiry*, 9(1), 103–127. <https://doi.org/10.1177/2046147X19870844>
- Macdonald, S., Correia, S. G., & Watkin, A.-L. (2019). Regulating terrorist content on social media: Automation and the rule of law. *International Journal of Law in Context*, 15(2), 183–197. <https://doi.org/10.1017/S1744552319000119>
- Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in blockchain technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4. <https://ieeexplore.ieee.org/abstract/document/8494045/>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

- Ozeren, S., Hekim, H., Elmas, M. S., & Canbegi, H. I. (2018). An Analysis of ISIS Propaganda and Recruitment Activities Targeting the Turkish-Speaking Population. *International Annals of Criminology*, 56(1–2), 105–121. <https://doi.org/10.1017/cri.2018.14>
- PeakD. (2024). [Social Media]. Decentralize Social Media With True Ownership. <https://peakd.com/>
- Perešin, A. (2015). Fatal attraction: Western muslimas and ISIS. *Perspectives on Terrorism*, 9(3), 21–38.
- Prucha, N. (2016). IS and the Jihadist information highway—Projecting influence and religious identity via Telegram. *Perspectives on Terrorism*, 10(6), 48–58.
- Psaras, Y., & Dias, D. (2020). The interplanetary file system and the filecoin network. *2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*, 80–80. <https://ieeexplore.ieee.org/abstract/document/9159174/>
- Rao, I. S., Kiah, M. L. M., Hameed, M. M., & Memon, Z. A. (2024). Scalability of blockchain: A comprehensive review and future research direction. *Cluster Computing*, 27(5), 5547–5570. <https://doi.org/10.1007/s10586-023-04257-7>
- Robinson, G. (2018). The European Commission’s Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online. *Eucrim - The European Criminal Law Associations’ Forum*. <https://doi.org/10.30709/eucrim-2018-024>
- Sachetti, V. (2021). The EU Response to Terrorist Content Online: Too Little, (Maybe not) Too Late? [Text/html,PDF]. *European Papers - A Journal on Law and Integration*, 2021 6, 967986. <https://doi.org/10.15166/2499-8249/509>
- Saltman, E. (2020). Countering Terrorism and Violent Extremism at Facebook: Technology, Expertise and Partnerships. *In a Pandemic World*, 80.
- Saurabh, K., Upadhyay, P., & Rani, N. (2023). A study on blockchain-based marketplace governance platform adoption: A multi-industry perspective. *Digital Policy, Regulation and Governance*, 25(6), 653–692.
- Sheridan, D., Harris, J., Wear, F., Jr, J. C., Wong, E., & Yazdinejad, A. (2022). *Web3 Challenges and Opportunities for the Market* (arXiv:2209.02446). arXiv. <https://doi.org/10.48550/arXiv.2209.02446>
- SocialX. (2024). [Social Media]. <https://socialx.network/>
- Steemit. (2024). [Social Media]. <https://steemit.com/>
- Su, S., Tian, Z., Li, S., Deng, J., Yin, L., Du, X., & Guizani, M. (2021). IoT root union: A decentralized name resolving system for IoT based on blockchain. *Information Processing & Management*, 58(3), 102553. <https://doi.org/10.1016/j.ipm.2021.102553>
- Sun, J., Saddik, A. E., & Cai, W. (2024). Smart Contract as a Service: A Paradigm of Reusing Smart Contract in Web3 Ecosystem. *IEEE Consumer Electronics Magazine*, 1–9. <https://doi.org/10.1109/MCE.2024.3353178>
- Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, 14(2), 117. <https://doi.org/10.3390/info14020117>
- Tanriverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir ? Ne Değildir ? : Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203–217. <https://doi.org/10.17671/gazibtd.547122>

- United Nations. (2017). *Resolution 2354*. Security Council. <https://documents.un.org/doc/undoc/gen/n17/149/22/pdf/n1714922.pdf>
- Walther, S., & McCoy, A. (2021). US extremism on Telegram. *Perspectives on Terrorism*, 15(2), 100–124.
- Wan, S., Lin, H., Gan, W., Chen, J., & Yu, P. S. (2024). Web3: The Next Internet Revolution. *IEEE Internet of Things Journal*, 11(21), 34811–34825. <https://doi.org/10.1109/JIOT.2024.3432116>
- Weimann, G. (2010). Terror on facebook, twitter, and youtube. *The Brown Journal of World Affairs*, 16(2), 45–54.
- Weimann, G. (2016). The Emerging Role of Social Media in the Recruitment of Foreign Fighters. In A. De Guttry, F. Capone, & C. Paulussen (Eds.), *Foreign Fighters under International Law and Beyond* (pp. 77–95). T.M.C. Asser Press. [https://doi.org/10.1007/978-94-6265-099-2\\_6](https://doi.org/10.1007/978-94-6265-099-2_6)
- West, L. J. (2021). Counter-terrorism, social media and the regulation of extremist content. In *Counter-Terrorism* (pp. 116–128). Edward Elgar Publishing. <https://www.elgaronline.com/edcollchap-oa/book/9781800373075/book-part-9781800373075-16.xml>
- Whitepaper, H. (2020, September 25). *Hive: Fast. Scalable. Powerful. The Blockchain for Web 3.0*. Decentralized Hive Ecosystem. <https://hive.io/whitepaper.pdf>
- Whitepaper, S. (2018a). *SocailX Whitepaper*. SocialX Ecosystem. <https://socialx.network/wp-content/uploads/2018/12/Whitepaper-SocialX-v1.2.pdf>
- Whitepaper, S. (2018b, June). *An incentivized, blockchain-based, public content platform*. Steem. <https://steem.com/steem-whitepaper.pdf>
- Wilkinson, P. (1997). The media and terrorism: A reassessment. *Terrorism and Political Violence*, 9(2), 51–64. <https://doi.org/10.1080/09546559708427402>
- Winter, C. (2020). Redefining 'Propaganda': The Media Strategy of the Islamic State. *The RUSI Journal*, 165(1), 38–42. <https://doi.org/10.1080/03071847.2020.1734321>
- Wood, G. (2014). *Less-techy: What is Web 3.0?* <https://gavwood.com/web3it.html>
- Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., Xu, G., & Tyson, G. (2022). Challenges in decentralized name management: The case of ENS. *Proceedings of the 22nd ACM Internet Measurement Conference*, 65–82. <https://doi.org/10.1145/3517745.3561469>
- Zhan, Y., Xiong, Y., & Xing, X. (2023). A conceptual model and case study of blockchain-enabled social media platform. *Technovation*, 119, 102610. <https://doi.org/10.1016/j.technovation.2022.102610>
- Zhou, J., Jiang, T., Wang, H., Wu, M., & Chen, T. (2023). DAppHunter: Identifying Inconsistent Behaviors of Blockchain-based Decentralized Applications. *2023 IEEE/ACM 45th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, 24–35. <https://doi.org/10.1109/ICSE-SEIP58684.2023.00008>
- Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, 8, 16440–16455. <https://doi.org/10.1109/ACCESS.2020.2967218>



# Defence Against Terrorism Review DATR Magazine



DATR, 2025; 1 : 79-98

Electronic Online ISSN 1307 - 9190

## Türkiye's Security Assistance to Somalia and Its Implications for Somalian Counterterrorism Efforts

*Nebahat Tanrıverdi Yaşar\**

### **Abstract**

*Türkiye has been playing a pivotal role in shaping Somalia's security forces through training programs, arms supplies, and strategic partnerships. This research will examine Türkiye's extensive security assistance to Somalia, focusing on its implications for the country's counter-terrorism landscape, as well as the operational effectiveness of Somali security forces in combating Al-Shabaab and other extremist threats. By analyzing Türkiye's security assistance approach, this paper evaluates the successes, challenges, and long-term implications of Türkiye's counter-terrorism assistance in Somalia. The findings highlight the potential for NATO and other international actors to draw lessons from Türkiye's model, particularly regarding the balance of military support and capacity-building in fragile states.*

### **Keywords**

*Security assistance, Counterterrorism, Al-Shabaab, Türkiye, Somalia.*

### **1. Introduction**

Somalia has long been a focal point of international counterterrorism and stabilization efforts due to its persistent fragility and the enduring threat posed by extremist groups (Phillips, 2020). The country's protracted conflict, compounded

---

\* The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the author/s is affiliated.

<sup>1</sup> Researcher and Policy Analyst, [nebahat.tanriverdi@gmail.com](mailto:nebahat.tanriverdi@gmail.com)

by weak governance, entrenched clan divisions, and recurring insurgencies, has rendered external security assistance indispensable in combating groups such as Al-Shabaab. Over the past decade, international actors have played a pivotal role in Somalia's counterterrorism landscape, with Türkiye emerging as a prominent partner through its multifaceted engagement in security, development, and state-building.

As part of a broader foreign policy shift toward Africa, Türkiye has positioned itself as a critical security partner in conflict-ridden Somalia, a nation plagued by decades of conflict and the persistent threat of extremist groups such as al-Shabaab. Anchored by the establishment of the Turkish Task Force Command in Somalia (STGK), known also as Camp TURKSOM in 2017—Türkiye's largest overseas military base—Türkiye's approach combines military assistance, development aid, and cultural diplomacy. This model diverges from the overly bureaucratic, slow and conditionality-heavy frameworks of Western powers, Türkiye's approach warrants closer scholarly examination for its innovative and adaptive strategies. Its soft power, humanitarian and development aid aspects this model, also called 'the Ankara consensus', rendering Türkiye a unique non-traditional actor, has drawn substantial academic interest (Akpınar, 2017) (Kaya, 2020) (Murphy & Sazak, O., 2012).

Despite a growing body of literature on Türkiye's security assistance (Şahin & Karabekir, F., 2022), analyses of this dimension of Turkish foreign policy in Africa remain underdeveloped. Security cooperation has been a consistent theme in Türkiye-Africa relations since the inaugural Türkiye-Africa Summits in 2008 and 2014, yet mainstream scholarship often neglects this new dimension of Türkiye's foreign policy. Among existing studies, considerable focus has been directed toward Türkiye's military base in Somalia, the first Turkish base in Africa, which "remain perfect examples of proactivity in the new grammar of Türkiye's foreign policy of security in Africa." (Kitio, 2020, p. 44-45) Somalia serves as a significant case study in understanding Türkiye's overseas military basing strategy (Kasapoğlu, 2020a) (Rossiter & Cannon, B. J., 2019). Compared to those studies, However, less scholarly attention has been paid to Türkiye's broader security practices and their implications for enhancing the Somali National Army's (SNA) capacity to combat terrorism.

Türkiye's security assistance to Somalia is both ambitious and multidimensional, accounted as embarking on a holistic approach to transform Somalia's security apparatus in line of peacebuilding activities (Ipek, 2021). It has provided extensive support to the SNA through training programs, arms supplies, and logistical

assistance, with the Camp TURKSOM in Mogadishu serving as a cornerstone of these efforts (Williams & Ali, H. Y. , 2020). Türkiye's comprehensive security sector assistance has been widely recognized as successful, contributing to the development of institutional capacity and enhancing the effectiveness of Somalia's security forces (Williams & Ali, H. Y. , 2020).

Despite these positive contributions, significant challenges remain. Türkiye's security assistance has enhanced the SNA's operational capabilities, particularly against Al-Shabaab, yet broader stabilization efforts face persistent obstacles. The SNA's ability to sustain territorial gains is hindered by governance gaps, logistical weaknesses, and the fragmented nature of Somali security forces (Williams, 2018). Reclaimed territories often revert to insurgent control due to the federal government's inability to establish effective governance and provide essential services (Menkhaus, 2016). Furthermore, Türkiye's state-centric model, aligned with Somalia's central government, has been criticized for overlooking the decentralized political and clan dynamics that shape the Somali conflict landscape. While this approach has strengthened the state's military capacities, it struggles to address local grievances that hinder long-term stabilization. These recurring patterns highlight the need to evaluate the effectiveness of Türkiye's counterterrorism assistance in addressing Somalia's broader security and stabilization challenges.

This study examines Türkiye's security assistance to Somalia, focusing on its implications for the SNA's operational effectiveness and the country's counterterrorism landscape. By analyzing Türkiye's security assistance to Somalia, the study evaluates the successes, challenges, and long-term implications of Türkiye's engagement. It argues that while Türkiye's initiatives have significantly bolstered Somali military capabilities, insufficient attention to local reconciliation and governance limits the overall effectiveness of its efforts. The analysis highlights the stabilization gap in reclaimed territories, where governance failures have allowed Al-Shabaab to resurge. The study is structured as follows. The first section provides an overview of Türkiye's security assistance to Somalia- its military training programs, operational support and military equipment provisions. The second section evaluates the impact of Türkiye's efforts on the SNA's capabilities, emphasizing successes and ongoing challenges in combating Al-Shabaab.

## 2. Framing Türkiye's Security Assistance in Somalia

Türkiye's security assistance to Somalia is built upon three key pillars: military training, capacity-building through military equipment, and operational support. Since 2012, Türkiye has delivered security aid to Somalia through diverse and increasingly institutionalized mechanisms. The foundation for this cooperation has been established through an array of bilateral agreements and protocols, which outline comprehensive frameworks for collaboration in military training, policing, security, and defense industries (Kitio, 2020). A landmark agreement, the "Military Training Cooperation Agreement," was signed on April 13, 2012, marking the beginning of Turkish training programs for Somali military and police personnel. This was later supplemented by the "Defense Industrial Cooperation Agreement" of January 25, 2015, which expanded cooperation into the defense industry. A significant milestone in this partnership was reached in February 2024 with the signing of a ten-year defense and economic cooperation agreement. This agreement emphasizes enhancing Somalia's maritime security through the modernization and training of its naval forces, the construction of infrastructure, and the conduct of joint air, land, and sea operations along the Somali coastline.

Türkiye's military training programs in Somalia are closely aligned with NATO standards, particularly in operational protocols, certification frameworks, and broader strategic concepts (Karataş, 2022). In May 2018, the Federal Government of Somalia (FGS) formalized its commitment to adopting NATO standards by signing an agreement with the EU, Türkiye, the UK, and the USA to standardize the SNA training along these lines (Williams & Ali, H. Y. , 2020). Türkiye's efforts aim to elevate the quality of training to Turkish Armed Forces (TAF) standards, while simultaneously fostering regional military capabilities modeled on "the Turkish version of NATO practices" (Rossiter & Cannon, B. J., 2019, p. 182). These programs draw heavily on Türkiye's extensive experience in NATO peacekeeping operations since the 1990s, including participation in the Partnership for Peace (PfP) program and the establishment of the PfP Training Centre in Ankara in 1998 (Oğuzlu & Güngör, U., 2006).<sup>1</sup>

Türkiye's peacekeeping and military support experiences ranging from Kosovo, Bosnia-Herzegovina, to Lebanon, Afghanistan, and Somalia have played a formative role in shaping its training modules, which are tailored to the specific

---

<sup>1</sup> The NATO Partnership for Peace (PfP) program, established in 1994, "a programme of bilateral co-operation between individual Euro-Atlantic partner countries and NATO". Its primary objectives are to enhance cooperation on defense and security matters while contributing to broader European security and stability. (NATO, 2024)

needs of conflict-affected states (Ibas, 2007) (Kinacioğlu & Gürzel, A. G., 2013) (Hacaoglu, 2001) (Turkish Daily News, 2002) (NATO OTAN., 2021). Over time, Türkiye expanded its PfP contributions to encompass officer training, logistical support, arms provision, and joint military exercises. This holistic approach aims to professionalize partner forces, enhance interoperability, and foster collaborative defense capacities. Türkiye has also leveraged expertise in military medicine, technology, and defense industries to provide comprehensive capacity-building solutions.

Experiences in Kosovo, Afghanistan, and Somalia have been instrumental in shaping Türkiye's approach to providing training modules tailored to the needs of conflict-affected countries. Following the basic peacekeeping duties, Türkiye expanded its PfP contributions to include officer training, material support, arms sales, and joint exercises where Turkish armed forces engaged in peacekeeping missions. Vecdi Gönül, then-Minister of Defence, for instance stated that "The Turkish Armed Forces has trained more than 9,000 Afghan personnel either in Afghanistan or in Türkiye since 2001 and additionally 11 Afghan companies (1295 Afghan personnel) are being trained in Türkiye within October 2009 and December (Gönül, 2010, p. 18)" addressing Türkiye's contributions to NATO Afghanistan Training Mission (NTM-A). As well, Türkiye also engaged in equipment donation to supports to the Kosovo Security Force, during the same era (Gönül, 2010). The TAF PfP Training Centre, between 2002 and 2015, trained 2,335 personnel in 19 countries (Yüce, 2016). These programs aimed to enhance military professionalism, foster mutual collaboration, and ensure technological and logistical interoperability among partner nations.

In a similar vein, in Somalia, Türkiye's military training programs mirror NATO's emphasis on maintaining capability, readiness, and long-term interoperability. These efforts extend beyond training individual personnel to include the development of organizational frameworks necessary for a self-reliant military. Türkiye's contributions are informed by its PfP experience and aim to establish robust command and control systems within the SNA. Furthermore, Türkiye's security assistance model is distinguished by its provision of high-performance systems, comprehensive training, and operational expertise, offered without the imposition of restrictive political conditions. This model adopts a holistic approach, integrating training, equipment provision, technical cooperation, and defense industry development. By combining hard power capabilities with tailored capacity-building initiatives, Türkiye has positioned itself as a critical and adaptive partner in Somalia's security landscape. This structured and resource-intensive approach

provides Türkiye with a competitive advantage in its security partnerships with African nations, where sustained support of this nature is often absent (Rossiter & Cannon, B. J., 2019, p. 181).

Additionally, Türkiye's security assistance incorporates elements of the TAF's counterterrorism strategies, which have been honed over decades of military operations. These strategies prioritize border security, neutralizing terrorist threats, and maintaining territorial control. During the mid-1980s to mid-2000s, Türkiye relied heavily on air power, complemented by ground operations, to project military strength and neutralize cross-border threats.<sup>2</sup> This operational experience now informs Türkiye's assistance to Somalia, particularly in enhancing area control and border security (Alemdar, 2021).

Given the Somali federal government's continued struggle to exert authority even over Mogadishu, Türkiye's transfer of its territorial control strategies and counterterrorism tactics to Somali forces represents a crucial aspect of its security assistance. The Somali government remains reliant on external actors, including the African Union Transition Mission to Somalia (ATMIS), whose over 12,000 peacekeeping force is essential for securing key installations in Mogadishu (ISW Press, 2024).<sup>3</sup> However, challenges persist, as the SNA and police forces often lack integration, with some units functioning as clan militias rather than a unified national security apparatus. Al-Shabaab continues to exploit these weaknesses, penetrating Mogadishu to conduct terrorist attacks targeting governmental and civilian infrastructure.

<sup>2</sup> Türkiye's defence and military strategy has evolved significantly in response to various security challenges; Cross-border operations to combat terrorism also constitute an important aspect of this evolution. Turkish Armed Forces (TAF) has carried out many air and land operations targeting PKK camps in Northern Iraq since 1983, when the first operations against the PKK were carried out. These efforts first increased with three major operations between 1983 and 1990 and intensified in the 1990s with a total of 42 operations, consisting mainly of hot pursuits and air strikes. Although there was a lull in the early 2000s, momentum for cross-border operations resumed notably in 2007, with six significant operations conducted in December alone. The conflict continued with three operations in 2008, two in 2011, and was revived in 2016, a year after Türkiye's military intervention in Syria began ( (Al Jazeera Türk, 2011) (Hancılar, 2021) (Şener, 2013, pp. 700-701). Since 2016, Türkiye has conducted a series of military operations in Syria and Iraq, targeting, PKK, YPG and ISIS as follows: Operation Euphrates Shield (2016-2017), Operation Olive Branch (2018), Operation Peace Spring (2019), Operation Spring Shield (2020), Claw operations (2019-present) (including Claw-Eagle, Claw-Tiger (2020), Claw-Lightning, Claw-Thunderbolt (2021), and Claw-Lock (2022)), Operations Winter Eagle (2022) and Claw-Sword (2022).

<sup>3</sup> The African Union Transition Mission in Somalia (ATMIS), which commenced operations in 2012 with over 20,000 troops, has been undergoing a phased drawdown since 2023, reducing its personnel to 12,626 uniformed members. These forces are expected to remain in Somalia until the mission's conclusion at the end of 2024. According to the African Union Strategic Concept of Operations (AUSSOM CONOPS), the mission will ultimately be restructured to include 11,911 personnel operating across four sectors. This reorganization necessitates the consolidation of areas by AU forces or the transfer of control to Somali authorities within the six existing ATMIS sectors. : ISW Press. (2024, August 22). Africa file, August 22, 2024: "AUSSOM" new AU mission in Somalia; Burkina Faso reaches boiling point. Institute for the Study of War.

## **2.1. Military Training and the TURKSOM**

A cornerstone of Türkiye's security assistance to Somalia is its comprehensive military training programs. Following the signing of a military training agreement in May 2010, which came into effect in November 2012, Türkiye began providing formal training for Somalia's security personnel. One of the earliest initiatives involved the training of 60 Somali police cadets in Istanbul, representing a broader effort to rebuild Somalia's institutional capacities (Somaliland Press, 2012). Simultaneously, Türkiye initiated the training of Somali military officers domestically while constructing Camp TURKSOM in Mogadishu.

Türkiye's training programs aim to develop a disciplined and cohesive national force, which is also capable of conducting effective counterterrorism operations against Al-Shabaab (Abdulle & Gurpinar, B. , 2019, p. 57-61) (Görmez, 2023). A key aspect of Türkiye's engagement has been the organizational modernization of the Somali Army, with professional training provided to numerous Somali soldiers and police officers (Kasapoğlu, 2020b) (Siradag, 2022, p. 398).

Moreover, the establishment of the TURKSOM military training base in Mogadishu in 2017 marked a significant institutionalization of Türkiye's military engagement in Somalia. As one of Türkiye's largest overseas training facilities, TURKSOM has become the focal point of efforts to professionalize and modernize the SNA (Paksoy, 2017). The facility was designed to enhance the operational effectiveness and capacity of the Somali military, with its the capacity to train more than 1,500 troops at any one time and approximately 200 Turkish personnel stationed at the base to provide on-ground training since its inception (Şahin Z. , 2016). The Turkish training program is designed to produce three Somali battalions annually, with subsequent specialized commando training in Türkiye (Kasapoğlu, 2020b). Turkish officials have highlighted the strategic importance of these efforts, stating: "These battalions will form the backbone of the Somali National Army in the future. We believe that the personnel trained by the Turkish Armed Forces will serve not only the security of Somalia but also the security of Africa and beyond" (Maruf, 2022). Similarly, during the Camp TURKSOM's opening ceremony, Somali Prime Minister Hassan Ali Khaire explain their perspective as such, saying "This training base has a unique significance for us because it is a concrete step taken toward building an inclusive and integrated Somali National Army" (VOA, 2017).

Türkiye's training efforts primarily focus on the elite Gorgor (Eagle) commando brigades and, to a lesser extent, the Haram'ad (Cheetah) special police units, alongside hundreds of non-commissioned officers (Donelli, 2021, p. 109). The

Gorgor brigades are trained for rapid-response and counterinsurgency operations, while the Haram'ad units specialize in crisis management and counterterrorism within urban and metropolitan environments.<sup>4</sup> Training includes rigorous basic instruction at Camp TURKSOM, followed by advanced commando specialization courses in Türkiye (Anadolu Agency, 2021). These forces have consistently participated in counterinsurgency and counterterrorism campaigns, including operations to liberate towns occupied by Al-Shabaab insurgents (Xinhua, 2023) (Halqabsi News, 2023).

As mentioned before, in addition to special forces, Türkiye's contribution extends to training hundreds of officers and non-commissioned personnel (Işık, 2022). By 2022, President Erdoğan stated that Türkiye had trained over 5,000 Somali soldiers and 1,000 special operations police. A TRT documentary broadcast in March 2024 updated these figures, reporting that 6,000 Somali military personnel had been trained by Türkiye since 2017 (TRT World, 2024). Türkiye aims to train approximately one-third of Somalia's national army (Ilhan & Demirci, 2020), aligning with Somali authorities' broader objective of recruiting and training 15,000–16,000 soldiers (Maruf, 2023). By 2023, reports suggested that Somalia had achieved its goal of building a 20,000-strong army (Africa Defence Forum, 2023).

## **2.2. Operational Support**

Somalia currently lacks a functional air force or navy, rendering it heavily reliant on external actors for aerial and maritime operations. The United Nations and the African Union Transition Mission in Somalia (ATMIS) provide air support to the SNA and has conducted major offensives against Al-Shabaab on the ground with ATMIS troops, while the United States has conducted airstrikes targeting Al-Shabaab since 2011. In comparison, Türkiye's operational support, in terms of direct combat role, is relatively recent and more limited in scope.

The Mogadishu base, although modest when compared to conventional overseas military installations, primarily functions as a training hub for Somali forces (Rossiter & Cannon, B. J., 2019). Turkish land forces stationed in Mogadishu operate within the Turkish Task Force Command in Somalia (STGK). The STGK complex houses three military schools, dormitories, barracks, depots, lounges,

---

<sup>4</sup> Since 2012, U.S. security assistance has primarily focused on developing the Danab brigade. Meanwhile, the European Union Training Mission, established in 2010, has trained approximately 7,000 Somali National Army (SNA) troops. Between 2019 and 2023, Eritrea provided training for around 5,000 Somali recruits. In January 2023, Somalia's National Security Advisor reported that the government had sent 12,000 recruits to Eritrea, Ethiopia, Egypt, and Uganda for training, with partial funding sourced from the United Arab Emirates. (Williams, *The Somali National Army Versus Al-Shabaab: A Net Assessment*, 2024)

sports fields, and facilities for weapons testing and combat training (Şahin Z. , 2016). This contingent comprises around 200- 300 Turkish personnel (Rossiter & Cannon, B. J., 2019, p. 169) (Şahin Z. , 2016). Consequently, some analysts argue that, in practical terms, Camp TURKSOM is not a traditional overseas military base but rather a capacity-building center (Rossiter & Cannon, B. J., 2019). With its relatively modest military capacity and limited capital investment, TURKSOM prioritizes military training and capacity-building missions over the projection of hard power (Donelli, 2024) (Al Jazeera, 2017) (Tanrıverdi Yaşar, 2021).

Yet, Camp TURKSOM provides logistical support to the Gorgor forces and air cover to the national army (Donelli, 2024). Since late 2022, Türkiye has also deployed Bayraktar TB2 drones to enhance the SNA's operational capabilities. Alongside with the United States, Türkiye has reportedly conducted drone strikes against Al-Shabaab (Caato, 2022). This operational support has improved the precision of SNA operations and enhanced surveillance capabilities, contributing to more effective counterterrorism efforts (Middle East Eye, 2022).

Türkiye's naval contributions further underscore its operational role in Somalia. Since 2009, Türkiye has maintained a naval presence in the Gulf of Aden, off the coast of Somalia, and in the Arabian Sea, in coordination with United Nations mandates. Following the Turkish Parliament's authorization on February 10, 2009, a Turkish naval frigate was deployed to the Gulf of Aden region, joining Combined Task Force 151 (CTF-151), which conducts counter-piracy operations in and around the Gulf of Aden and off the coast of Somalia (Republic of Türkiye Ministry of Foreign Affairs, 2009). Türkiye has participated in both CTF-151 and the Standing NATO Maritime Group 2 (SNMG-II), contributing a total of seven frigates to these missions (Republic of Türkiye Ministry of Foreign Affairs). The Turkish Navy commanded CTF-151 from May 3 to August 13, 2009, and again from September 1 to November 29, 2010. Türkiye Assumes Command of Combined Maritime Forces' Combined Task Force 151 (Combined Maritime Forces, 2024).

### **2.3. Arms Supplies and Military Equipment**

The SNA is a relatively low-tech force, composed of small battalions of approximately 400 soldiers. It operates with limited vehicles, a small number of armored vehicles, and primarily small arms and light weapons due to a long-standing international arms embargo. Most SNA units remain under-equipped,

which constrains their operational effectiveness. Among the SNA's forces, only the approximately 8,000 Danab and Gorgor units constitute the so-called "freedom units" or "maneuver units"—forces equipped with the necessary vehicles to conduct operations such as long-range patrolling and special operation raids (Williams, 2024, s. 37) (Williams & Elmi, A. , 2023, p. 22). In addition to that, SNA units often lack sufficient armored transport and rely on soft-skin vehicles, frequently operating without explosive ordnance disposal teams. This equipment deficit has contributed to higher casualty rates from improvised explosive device (IED) attacks, leaving SNA units particularly vulnerable to Al-Shabaab's roadside bombs and grenades. As one report noted, the SNA suffers from "lack of equipment of all types, not least weapons. To form other types of units, such as engineer units and logistic units, a considerable amount of equipment needs to be donated." (Williams & Elmi, A. , 2023, p. 10)

In response to these challenges, Türkiye has prioritized the provision of vehicles and equipment to address immediate operational needs in the field. Türkiye has supplied Somali forces with light arms, vehicles, and other military equipment, enhancing their ability to conduct more effective operations against Al-Shabaab (Africa News, 2017). "Türkiye equipped them, and Türkiye promised to equip every soldier who is being trained at the camp" stated Somali State Minister for Defense Mohamed Ali Haga in 2018 (Maruf, 2018). For instance, Türkiye has provided Somali infantry units with Mine-Resistant Ambush-Protected (MRAP) vehicles, designed specifically to withstand improvised explosive device (IED) attacks by al-Shabaab (Alemdar, 2023). These provisions complement Türkiye's extensive training efforts, ensuring that Somali troops are better prepared for the demands of modern counter-insurgency warfare.

Recent years have seen continued donations of military equipment and vehicles from Türkiye to Somalia. Türkiye's military aid is coordinated through the Ministry of National Defence, which oversees direct procurement from Turkish defense firms. This system operates under financial frameworks such as the Military Financial Cooperation Agreement (AMIBA), the Cash Assistance Implementation Protocol (NYUP), and various Logistics Implementation Protocols (Ministry of National Defence, 2022). Somalia has benefited significantly from this aid system, receiving both military equipment and financial assistance. For instance, in 2020, Türkiye delivered 12 off-road vehicles as part of bilateral military and financial cooperation agreements (Özkaya, 2020). This was followed in 2021 by the delivery of additional mine-protected armored personnel carriers, including eight BMC-produced KİRPİ I vehicles and 14 AKTAN fuel tankers (Turkish Defence Ministry, 2020). Furthermore,

Türkiye has provided essential equipment to bolster Somalia's coastguard and navy (FTL Somalia, 2024).

### **3. The Limitations of Türkiye's Assistance on the Somali National Army's Operational Effectiveness**

Türkiye's security assistance has significantly contributed to the development of the SNA. Specifically, Türkiye's training programs, arms supplies, and strategic partnerships have led to notable improvements in the SNA's capabilities. Turkish-trained units, alongside with Danab special forces, trained by the US consistently demonstrate higher levels of operational effectiveness compared to other SNA segments, reflecting the success of Türkiye's targeted capacity-building approach (Williams, 2024). By emphasizing discipline and operational readiness, Türkiye has enhanced the SNA's ability to conduct coordinated offensives against Al-Shabaab, particularly in southern and central Somalia. Türkiye's provision of arms, vehicles, and other military equipment has further strengthened the SNA's operational capacities. Somali forces, equipped with Turkish support, have successfully reclaimed critical territories, including towns and transport corridors previously controlled by Al-Shabaab (Petrócz, 2023).

Despite these successes, the SNA faces persistent challenges that undermine the long-term impact of Türkiye's assistance. At the operational level, even elite units like the Turkish-trained Gorgor forces face limitations. Chronic issues such as irregular salary payments, inadequate supplies, and poor maintenance of equipment have limited the SNA's operational capacity. Many soldiers trained by Türkiye have struggled to sustain prolonged operations due to these logistical deficiencies (Menkhaus, 2016). Türkiye has provided direct budgetary support to the Federal Government of Somalia, except for a brief pause in 2013. These payments have ranged from \$4.5 million to \$6 million in recent years, as noted in Olgan Bekar's speech at the Rising Powers Conference in 2016 (Sazak & Woods, 2017). Financial assistance from Türkiye and other partner countries remains essential under current conditions; however, without significant improvements in its internal capacity, the SNA risks becoming indefinitely reliant on external support.

In August 2022, the SNA, supported by clan militias known as Ma'awisley, initiated an offensive against al-Shabaab, reclaiming over 215 locations in central regions such as Hiraan and Galgaduud (Muibu, 2024). This effort was bolstered by U.S. and Turkish drone strikes targeting al-Shabaab's command structures. Support from the Ma'awisley militias and local power brokers played a critical role in these initial successes, providing essential operational intelligence and

bolstering the legitimacy of the government's efforts (Williams, 2024). Gorgor commandos, alongside with the Danab were also intensively involved in these operations (VOA, 2022). In July 2023, under the leadership of Captain Abdiwali Ahmed Hussein, the 9th Gorgor Battalion conducted successful operations in the Galgaduud Region, dismantling Al-Shabaab outposts in towns such as Barag Sheikh Aamir, Eel-Dhitar, and Eel-Aid, in central Somalia (Halqabsi News, 2023). On September 2023, the unit launched successful operations in southern Somalia (Xinhua, 2023). SNA's operations have disrupted Al-Shabaab's control and supply lines. The early successes generated cautious optimism about significantly weakening al-Shabaab.

However, despite these early successes, significant challenges emerged. Al-Shabaab mounted counterattacks, reclaiming previously liberated areas, particularly in Hirshabelle and Galmudug. The second phase of the offensive, Operation Black Lion, which aimed to target Al-Shabaab strongholds in Jubaland and Southwest states, was postponed to consolidate gains in central Somalia (Garowe Online, 2023). Leadership and coordination challenges among Somali forces and allied militias further hampered the offensive's momentum, leaving Al-Shabaab in control of substantial territories as of early 2024 (International Crisis Group, 2023) (Muibu, 2024) (Williams, 2024). Historically, Somali and African Union (AU) forces have struggled to consolidate gains, with reclaimed territories often falling back under Al-Shabaab control after a temporary retreat. This recurring cycle highlights a critical stabilization gap, as the SNA has not effectively transitioned battlefield successes into sustainable governance.

This pattern of temporary gains and rapid reversals weakens public confidence in the Somali government's ability to provide security (Muibu, 2024) (Williams, 2018). For residents in rural territories, the lack of sustained governance and services discourages collaboration with government forces. To bridge this stabilization gap, the Somali government must prioritize establishing local administrations in liberated areas, delivering essential services, and promoting inclusive political processes to address grievances that Al-Shabaab exploits. A focus on civilian security structures, developed in collaboration with local clans, is essential to maintaining control over reclaimed regions. Türkiye's interventions should acknowledge the hybrid nature of Somali governance and incorporate mechanisms to engage informal actors, such as clan elders and local security stakeholders.

Somalia's reliance on a clan-based power-sharing model, formalized through the '4.5' formula in 1997, complicates efforts to build a cohesive national security structure (The Somali Dialogue Platform and Somali Public Agenda,

2023). This formula, which allocates representation in the Federal Parliament among major clans and marginalizes minority clans, exacerbates inequality and fuels competition for resources. These dynamics, coupled with Somalia's history of proxy conflicts involving Ethiopia, Kenya, Eritrea, and Djibouti, further destabilize the security landscape. Ethiopia's 2006 intervention to oust the Union of Islamic Courts exemplifies the geopolitical rivalries that continue to shape Somali politics and the rise of insurgent groups like Al-Shabaab (Barnes & Hassan, H., 2007).

This fragmentation weakens the chain of command, complicates coordination, and undermines the cohesion of military operations (Williams, 2018). Türkiye's programs also seek to instill a sense of national unity among recruits, countering the clan-based fragmentation that has historically undermined the SNA's effectiveness. Efforts to create a unified national army have been slow, with Turkish-trained units sometimes operating in isolation from other segments of the SNA.

Improving coordination among Somali security forces, clan militias, and international partners is critical to overcoming these challenges. However, cooperation among security assistance providers remains limited. For instance, in 2013, Turkish efforts to collaborate with African Union Mission in Somalia (AMISOM) partners faced resistance, prompting Türkiye to adopt a bilateral approach with the SNA. While bilateral models like Türkiye's offer advantages in efficiency and flexibility, they also present challenges, including coordination issues, language barriers, and a lack of robust monitoring mechanisms. Moreover, without improved collaboration between assistance providers, the SNA risks remaining fragmented along clan lines, undermining national cohesion and operational effectiveness.

Internal political struggles within Somalia further complicate the success of Türkiye's assistance. Intra-Somalian power struggle is also challenging the success of Türkiye's security assistance. It is rumored that Gorgor units has been facing issues, such as significant personnel losses, declining morale, and leadership deficiencies (The Somali Digest, 2024). The loss of experienced commanders and high attrition rates weaken the unit, enabling Al-Shabab to exploit these vulnerabilities. Perceived political targeting within the military risk further division, complicating efforts against the insurgency (The Somali Digest, 2024).

Türkiye's reliance on bilateral development assistance raises questions about the SNA's long-term sustainability. Many soldiers trained at Camp TURKSOM face

logistical challenges, including insufficient salaries, inadequate equipment, and weak command structures. Chronic issues such as irregular payments and poor equipment maintenance further limit the SNA's operational capacity (Menkhaus, 2016). Türkiye has also provided direct budgetary support to the Somali government, with contributions ranging from \$4.5 million to \$6 million annually in recent years (Sazak & Woods, 2017, p. 175).

Regional cooperation in countering Al-Shabaab remains insufficient, underscoring the need for integrated efforts with neighboring countries (Muibu, 2024). Türkiye's security assistance could achieve greater impact if incorporated into broader, multi-partner initiatives that address the economic and logistical challenges of sustained operations.

Regional support in the fight against Al-Shabaab remains below the desired level, highlighting the need for enhanced operational cooperation with neighboring countries. In this context, Türkiye's security assistance could yield greater benefits if integrated into more comprehensive initiatives. The challenges faced, particularly in financing operations, underscore the economic factors driving this need.

#### **4. Conclusion**

Türkiye's security assistance to Somalia represents a complex and multifaceted engagement, encompassing military training, arms provision, operational support, and capacity-building initiatives. The establishment of Camp TURKSOM and Türkiye's adoption of NATO-standard practices reflect a methodical approach to enhancing the SNA's operational capabilities. Notable achievements, such as the training of the elite Gorgor commando brigades and, the Haram'ad special police units, alongside hundreds of non-commissioned officers as well as the provision of advanced military equipment, underscore Türkiye's pivotal role in Somalia's counterterrorism efforts against Al-Shabaab.

However, the analysis highlights several structural and operational challenges that hinder the long-term effectiveness of these initiatives. Persistent governance deficits, logistical inadequacies, and the fragmentation of Somalia's security forces have continued to impede the stabilization of territories reclaimed from Al-Shabaab. Even though Türkiye's assistance to Somalia encompasses multiple dimensions, including capacity building, support provision, stability promotion, development initiatives, and humanitarian aid, the challenges remain robust and necessitate different approaches.

The findings suggest that Türkiye's efforts could achieve greater sustainability and impact through a more coordinated and inclusive approach. Engaging local stakeholders, including clan elders and community actors, and fostering stronger collaboration with other international partners can better align security assistance with Somalia's broader stabilization and governance objectives. Addressing the stabilization gap in liberated territories through the establishment of local governance structures and services will be critical to consolidating gains against Al-Shabaab. Türkiye and other Western allies' contribution to Somalia could be further enhanced by addressing existing challenges through improved coordination—both within Somali society and with neighboring countries in the region, as well as with other partners providing security assistance to Somali institutions.

Türkiye's combination of hard power with development-oriented interventions offers a distinctive model for external engagement in fragile states. However, the sustainability of its contributions depends on addressing Somalia's underlying structural weaknesses in governance and security institutions. As this study has shown, while Türkiye's approach provides valuable lessons for other international actors, its success ultimately hinges on adapting to the hybrid nature of Somali politics and adopting a more integrated, long-term strategy.

## **Bibliography**

- Özkaya, T. (2020, August 25). *Turkey delivers 12 off-road vehicles to Somalia*. Anadolu Agency. [https://www.aa.com.tr/en/africa/turkey-delivers-12-off-road-vehicles-to-somalia/1951698#:~:text=Turkey%20has%20delivered%2012%20off,3rd%20\(Eagle\)%20Infantry%20Battalion.](https://www.aa.com.tr/en/africa/turkey-delivers-12-off-road-vehicles-to-somalia/1951698#:~:text=Turkey%20has%20delivered%2012%20off,3rd%20(Eagle)%20Infantry%20Battalion.)
- Abdulle, A. Y., & Gurpinar, B. . (2019). Turkey's engagement in Somalia: A security perspective. *Somali Studies: A Peer-Reviewed Academic Journal for Somali Studies*, 4, 53-71.
- Africa Defence Forum. (2023, July 11). *Somalia Recruits 20,000 Soldiers as ATMIS Begins Drawdown*. Africa Defence Forum. <https://adf-magazine.com/2023/07/somalia-recruits-20000-soldiers-as-atmis-begins-drawdown/>
- Africa News. (2017). *Turkey delivers new assault rifles to Somalia to fight al Shabaab insurgency*. Africa News. <https://www.africanews.com/2017/11/02/turkey-delivers-new-assault-rifles-to-somalia-to-fight-al-shabaab-insurgency/>

- Akpınar, P. (2017). Turkey's peacebuilding in Somalia: The limits of humanitarian diplomacy. *Turkish Studies*, 18(3), 395-415.
- Al Jazeera. (2017, October 1). *Turkey sets up largest overseas army base in Somalia*. <https://www.aljazeera.com/news/2017/10/1/turkey-sets-up-largest-overseas-army-base-in-somalia>
- Al Jazeera Türk. (2011, September 19). *TSK'nın sınır ötesi operasyonları*. Al Jazeera Türk . <https://www.aljazeera.com.tr/haber/tsknin-sinir-otesi-operasyonlari>
- Alemdar, A. (2021). Rekabetçi Afrika pazarında Türk savunma sanayiinin artan varlığı. *Kriter Dergisi*, 6(63).
- Alemdar, A. (2023). Afrika'nın savunma ve güvenlik anlayışında Türk savunma sanayii etkisi. *Kriter Dergisi*, 8(82).
- Anadolu Agency. (2021, December 4). *Somali commandos arrive home after training in Turkey*. <https://www.aa.com.tr/en/africa/1-of-3-somalian-troops-to-be-trained-by-turkey-en-voy/1931275>
- Barnes, C., & Hassan, H. (2007). The rise and fall of Mogadishu's Islamic Courts. *Journal of Eastern African Studies*. *African Studies*, 1(2), 151-160.
- Caato, B. M. (2022, October 1). *Turkey's Bayraktar TB2 drones join offensive against al-Shabab*. Middle East Eye. <https://www.middleeasteye.net/news/somalia-turkey-bayraktar-tb2-drones-join-offensive-shabab>
- Combined Maritime Forces. (2024, July 24). *Türkiye Assumes Command of Combined Maritime Forces' Combined Task Force 151 from Brazil*. Combined Maritime Forces. <https://combinedmaritimeforces.com/2024/07/24/turkiye-assumes-command-of-combined-maritime-forces-combined-task-force-151-from-brazil/>
- Donelli, F. (2021). *Turkey in Africa: Turkey's strategic involvement in Sub-Saharan Africa*. London: I.B. Tauris.
- Donelli, F. (2024, February 28). *Red Sea politics: Why Turkey is helping Somalia defend its waters*. The Conversation. <https://theconversation.com/red-sea-politics-why-turkey-is-helping-somalia-defend-its-waters-224377>
- FTL Somalia. (2024, October 31). *Somali Coastguard Receives New Response Boat from Turkey*. FTL Somalia. <https://www.ftlsomalia.com/somali-coastguard-receives-new-response-boat-from-turkey/#:~:text=This%20handover%2C%20attended%20by%20State,capabilities%20along%20the%20Somali%20coast.>
- Gönül, V. (2010). Turkey-NATO relations and NATO's new strategic concept. *Turkish Policy Quarterly*, 9(1), 15-21.
- Görmez, H. (2023). Security cooperation in Somalia: The role of Turkey. *Security and Defense Quarterly*, 35(1), 112-128.

- Garowe Online. (2023, August 17). *Why Somalia is delaying phase II of Al-Shabaab crackdown. Why Somalia is delaying phase II of Al-Shabaab crackdown*
- Hacaoglu, S. (2001, October 18). *Turkey warms up for peacekeeping.*
- Halqabsi News. (2023, July 10). *Gorgor Commandos Dismantle Al-Shabaab Outposts in Central Somalia.* Halqabsi News.
- Hancılar, Ö. (2021). 1983-1987 Kuzey Irak'taki Türk Sınır Ötesi Operasyonlarının Hukukîliği. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* (46), 347-359.
- İşık, Y. E. (2022, June 6). *Türkiye 6 bin Somalili askeri ve özel hareket polisini eğitti.* Defence Turk.
- Ibas, S. (2007, February 15). *Contributions of the Turkish Armed Forces to Middle East Peace Operations.* The Washington Institute. <https://www.washingtoninstitute.org/policy-analysis/contributions-turkish-armed-forces-middle-east-peace-operations>
- Ilhan, L., & Demirci, Z. (2020, July 4). *'1 of 3 Somalian troops to be trained by Turkey: Envoy'.* Anadolu Agency.
- International Crisis Group. (2023, March 21). *Sustaining gains in Somalia's offensive against al-Shabaab.* International Crisis Group. <https://www.crisisgroup.org/africa/horn-africa/somalia/b187-sustaining-gains-somalias-offensive-against-al-shabaab>
- Ipek, V. (2021). Revisiting liberal peacebuilding: BRICS and Turkey in Somalia. *Perceptions*, 26(1), 152–176.
- ISW Press. (2024, August 22). *Africa file, August 22, 2024: "AUSSOM" new AU mission in Somalia Burkina Faso reaches boiling point.* Institute for the Study of War. <https://understandingwar.org/backgrounders/africa-file-august-22-2024-%E2%80%9Caussom%E2%80%9D-new-au-mission-somalia-burkina-faso-reaches-boiling>
- Karataş, İ. (2022). Turkey's Military Presence in Somalia: Doing What, Why, and for Whom? . In A. O. Farah, & Mohamed Eno, *Theorising Somali Society: Hope, Transformation and Development* (pp. 167-190). New Delhi: Authors Press.
- Kasapoğlu, C. (2020a). Turkey's burgeoning defense technological and industrial base and expeditionary military policy. *Insight Turkey*, 22(3), 45-66.
- Kasapoğlu, C. (2020b, November 20). Turkey's 'African Eagle' trains Turkish-speaking troops in Somalia: Where next? *Terrorism Monitor*, 18(21).
- Kaya, O. (2020). Turkey's development assistance in Somalia: Beyond humanitarianism. *Journal of Development Studies*, 56(4), 511-527.
- Kinacioğlu, M., & Gürzel, A. G. (2013). Turkey's contribution to NATO's role in post-Cold War security governance: The use of force and security identity formation. *Global Governance*, 19(4), 589-610.

- Kitio, A. F. (2020). The rising security cooperation of Turkey in Africa: An assessment from the military perspective. *Journal of Rising Powers and Global Governance*, 1(2), 43-59.
- Maruf, H. (2018, January 5). *Turkey Gives Weapons to Somali Soldiers*. VOA. <https://www.voanews.com/a/turkey-gives-weapons-to-somali-soldiers-/4193724.html>
- Maruf, H. (2022, November 30). *Somalia Military Rebuilding Shows Signs of Improvement*. VOA. <https://www.voanews.com/a/somalia-military-rebuilding-shows-signs-of-improvement/6856894.html>
- Maruf, H. (2023, January 31). *Exclusive: Somalia Sends Thousands of Army Recruits Abroad for Training*. VOA. <https://www.voanews.com/a/exclusive-somalia-sends-thousands-of-army-recruits-abroad-for-training-/6941868.html>
- Menkhaus, K. (2016). Stabilization in practice: The Somali experience. *International Journal of Security & Development*, 5(1), 1-14.
- Middle East Eye. (2022, October). *Somalia: Turkey's Bayraktar TB2 drones join offensive against al-Shabab, October 2022*. Middle East Eye. <https://www.middleeasteye.net/news/somalia-turkey-bayraktar-tb2-drones-join-offensive-shabab>
- Ministry of National Defence. (2022). *Annual Activity Report* .
- Muibu, D. (2024, February). Somalia's stalled offensive against al-Shabaab: Taking stock of obstacles. *Combating Terrorism Center Sentinel*, 7(2), 18-26.
- Murphy, T., & Sazak, O. (2012). *Turkey's civilian capacity in post-conflict reconstruction*. Sabancı University. Istanbul Policy Center.
- NATO. (2024). *Partnership for Peace programme*. [https://www.nato.int/cps/en/natohq/topics\\_50349.htm](https://www.nato.int/cps/en/natohq/topics_50349.htm)
- NATO OTAN. (2021, March 30). *Turkey continues its efforts for Afghanistan's lasting security, through the NATO-led Resolute Support Mission*.
- Oğuzlu, H. T., & Güngör, U. (2006). Peace operations and the transformation of Turkey's security policy. *Contemporary Security Policy*, 27(3), 472-488.
- Paksoy, Y. (2017, May 25). *'Turkish Ambassador to Somalia Olgan Bekar: Turkey helping build state, military, infrastructure from scratch'*. Daily Sabah. <https://www.dailysabah.com/diplomacy/2017/05/25/turkish-ambassador-to-somalia-olgan-bekar-turkey-helping-build-state-military-infrastructure-from-scratch>
- Petrócz, J. O. (2023). Turkey in the Horn of Africa: Turkish-Somali military connections focused on the Turkish military camp in Mogadishu, Somalia. *Journal of Central and Eastern European African Studies*, 3(4), 44-57.
- Phillips, S. G. (2020). *When there was no aid: War and peace in Somaliland*. Cornell University Press.

- Türkiye's Security Assistance to Somalia and Its Implications for Somalian Counterterrorism Efforts* 97
- Republic of Türkiye Ministry of Foreign Affairs. (2009, May 4). *Press Release: No:61, 04 May 2009, Press Release Regarding the Assumption of the Command of CTF-151 by Turkey.*
- Republic of Türkiye Ministry of Foreign Affairs. (n.d.). *Piracy (Armed Robbery) off the Coast of Somalia.* [https://www.mfa.gov.tr/piracy-\\_armed-robbery\\_-\\_off-the-coast-of-somalia.en.mfa](https://www.mfa.gov.tr/piracy-_armed-robbery_-_off-the-coast-of-somalia.en.mfa)
- Rossiter, A., & Cannon, B. J. (2019). Re-examining the “base”: The political and security dimensions of Turkey’s military presence in Somalia. *Insight Turkey*, 21(1), 167-188.
- Sazak, O., & Woods, A. E. (2017). Thinking outside the compound: Turkey’s approach to peacebuilding in Somalia. In C. T. Coning, *Rising powers and peacebuilding* (pp. 167–189). Springer.
- Siradag, A. (2022). Turkey’s growing role as a security actor in Somalia: Dynamics and motivations. *Akademik İncelemeler Dergisi*, 17(2), 389-404.
- Somaliland Press. (2012, July 4). *Turkey begins training Somali forces.*
- Şahin, M., & Karabekir, F. (2022). Turkey in the Horn of Africa: Geopolitical strategy and security assistance. *African Security Review*, 31(2), 102–121.
- Şahin, Z. (2016). *Interview with Olgar Pekar: Why is Turkey launching a new military training camp in Somalia?* TRT World. <https://www.trtworld.com/middle-east/why-is-turkey-launching-a-new-military-training-camp-in-somalia-13089153>
- Şener, B. (2013). *Türk Dış Politikasında Güç Kullanma Seçeneği (1923–2010): Teorik, Tarihsel ve Hukuksal Bir Analiz.* Ankara: Barış Platin Kitabevi.
- Tanrıverdi Yaşar, N. (2021). *Syria and Libya’s contributions to the evolution of the Turkish “forward defence” doctrine’.* Geneva Center for Security Policy. Geneva Center for Security Policy, 14 June 2021.
- The Somali Dialogue Platform and Somali Public Agenda. (2023, May). *The role of 4.5 in democratization and governance in Somalia: Implications and considerations for the way forward.*
- The Somali Digest. (2024, December 3). *Gorgor forces in crisis: Desertions and leadership failures.*
- TRT World. (2024, March 12). ‘6,000 Somali military personnel trained by Türkiye since 2017’. TRT World. <https://www.youtube.com/watch?v=Xdi36dM9XWA>
- Turkish Daily News. (2002, June 21). *Turkey taking over ISAF command.* .
- Turkish Defence Ministry. (2020, September 1). X (formerly Twitter). <https://twitter.com/tcsavunma/status/1300357891346649088>
- VOA. (2017, September 30). *Turkey opens largest foreign military base in Mogadishu.* VOA.
- VOA. (2022, November 30 ). *Somalia Military Rebuilding Shows Signs of Improvement.* VOA.

- Williams, P. D. (2018). Building the Somali National Army: Anatomy of a failure. *Journal of Strategic Studies*, 43(1), 150-178.
- Williams, P. D. (2024, April). The Somali National Army Versus Al-Shabaab: A Net Assessment. *CTC Sentinel*, 35-43. CTC West Point. (2023). "The Somali National Army Versus Al-Shabaab: A Net Assessment." Combating Terrorism Center.
- Williams, P. D., & Ali, H. Y. . (2020). *The European Union Training Mission in Somalia: An assessment*. Stockholm International Peace Research Institute (SIPRI).
- Williams, P. D., & Elmi, A. . (2023). *Security sector reform in Somalia*. Mogadishu: Heritage Institute for Policy Studies.
- Xinhua. (2023, September 10). *Somali army kills over 20 al-Shabab militants in southern Somalia*. Xinhua.
- Yüce, A. (2016). Azerbaijan-Turkey military cooperation within the context of NATO and Partnership for Peace (PfP) program. *The Caucasus and the World: International Scientific Journal*, 21(7), 56-64.



## Defence Against Terrorism Review

### DATR Magazine

Electronic Online ISSN: 1307-9190

<https://dergipark.org.tr/tr/pub/datr>

### *English Article Title (Times New Roman, 14 pt, İtalik, single line)*

Name Surname <sup>1,\*1</sup>  Name Surname <sup>2</sup> 

<sup>1</sup>Xxxx Univeristy Xxxx Department,

<sup>2</sup>Xxxx Univeristy Xxxx Department,

#### **Abstract (must)**

*"Times New Roman" font should be used in all fields of the article. Line spacing must be "single" in all article fields.*

*There should be 12 nk space before the title, and 6 nk space after the title. The title should be written in 10 font size, bold, flat and left aligned.*

*There should be no space before the text (paragraph), and 6 nk space should be left after the text (paragraph). The text should be written in 10 font size, plain and justified.*

*In this section, a minimum of 100 and a maximum of 400 words in English should be written. In essence, the purpose, scope, research questions of the research should be included, methods, findings and results should be briefly mentioned.*

*English Keywords: 10 font size, italic. At least 3 keywords must be given. (Times New Roman, 9 pt, single space italic) (Between 200-250)*

#### **Keywords**

Xxxz, yyyy, ssss, dddd

\* The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the author/s is affiliated.

## **1. Introduction**

In this section, the purpose of the research should be specified, then the methods, processes and tools used should be detailed.

The articles should be numbered, including the entry. Subtitles should be numbered hierarchically. The first letter of each word should be capitalized in the titles and subheadings.

The entry title should be written in 11 font size, bold, flat and left aligned. There should be 12 nk space before the entry title and 6 nk space after.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

In the whole article, paragraph heads should be left-justified. Line spacing must be "single" in all article fields.

Page margins should be "Normal" (bottom, top, right, left 2.5 cm).

## **2. Title**

First level titles should be written in 11 font size, flat, bold and left aligned. The first letter of each word must be capitalized. First level should be 12 pt before the title and 6 pt after the title.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

First level title can be used as required.

### **- Section headings**

Section headings should be left justified, bold, with the first letter capitalized and numbered consecutively, starting with the Introduction. Sub-section headings should be in capital and lower-case italic letters, numbered 1.1, 1.2, etc, and left justified, with second and subsequent lines indented. All headings should have a minimum of two text lines after them before a page or column break. Ensure the text area is not blank except for the last page.

### **- Illustrations**

All figures should be numbered with Arabic numerals (1, 2, 3,...). Every figure should have a caption. All photographs, schemas, graphs and diagrams are to be referred to as figures. Line drawings should

be good quality scans or true electronic output. Low-quality scans are not acceptable. Figures must be embedded into the text and not supplied separately.

### 3. Tables and Figures

Tables and figures should be included in the relevant text. All tables and figures should be numbered separately. Figure and Table titles should be placed below the figure, aligned in the middle. Figures and tables should indicate the source (according to APA 7 Style).

Tables and figures should be placed in the text as pictures (.jpeg, .png) and also the original formats should be loaded into the system by adding table and figure numbers.

All figures and tables should be cited in the main text as Figure 1, Table 1, etc.



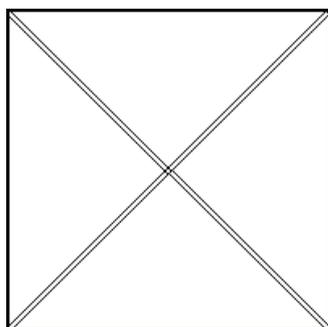
**Figure 1.** This is a figure. Schemes follow the same formatting.

**Table 1.** This is a table. Tables should be placed in the main text near to the first time they are cited.

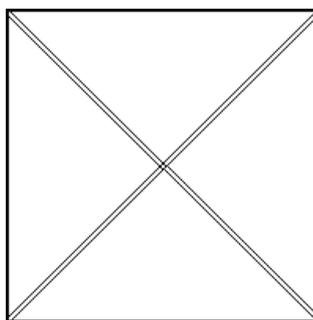
Title 1	Title 2	Title 3
entry 1	data	data
entry 2	data	data <sup>1</sup>

<sup>1</sup> Tables may have a footer.

The text continues here (Figure 2 and Table 2).



(a)



(b)

**Figure 2.** This is a figure. Schemes follow another format. If there are multiple panels, they should be listed as: **(a)** Description of what is contained in the first panel; **(b)** Description of what is contained in the second panel. Figures should be placed in the main text near to the first time they are cited.

**Table 2.** This is a table. Tables should be placed in the main text near to the first time they are cited.

<b>Title 1</b>	<b>Title 2</b>	<b>Title 3</b>	<b>Title 4</b>
	data	data	data
entry 1 *	data	data	data
	data	data	data
entry 2	data	data	data
	data	data	data
entry 3	data	data	data
	data	data	data
entry 4	data	data	data
	data	data	data

#### **4. Conclusions**

First level titles should be written in 11 font size, flat, bold and left aligned. The first letter of each word must be capitalized. First level should be 12 pt before the title and 6 pt after the title.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

If necessary, attachments may also be included in the article.

#### **5. Acknowledgments**

In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments). Acknowledgements and Reference heading should be left justified, bold, with the first letter capitalized but have no numbers. Text below continues as normal.

## 6. Construction of references

The title of the bibliography should be written in 11 font size, flat, bold and left aligned. The first letter should be capitalized. 12 nk space before the title of the bibliography and 6 nk after the title should be left.

There should be no space before each bibliographic identity given in the bibliography and 6 nk space should be left after the bibliographic identity. The text should be written in Times New Roman font, 11 font size, plain and justified. The second line of the bibliographic identity must be written inside 0.5 cm.

The names of "Journal" and "Book" should be written in italic in the bibliographic identity.

APA 7.0(American Psychological Association) style should be taken into consideration when sending in-text and bibliography. References cited in the text should be listed alphabetically at the end of the study.

### Examples:

Aktan, E . (2018). Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu. Bilgi Yönetimi, 1 (1), 1-22.

Al, U., Sezen, U., Soydal, İ., Taşkın, Z. ve Düzyol, G. (2012). Collaboration of Turkish scholars: Local or global? Collnet Journal of Scientometrics and Information Management, 6, 145-159.

Arısoy, Y . (2018). Elektronik Arşivlere Yönelik Uluslararası Yaklaşımlar Çerçevesinde Türkiye Değerlendirmesi. Bilgi Yönetimi, 1 (1), 63-77. Erişim Adresi: <http://dergipark.gov.tr/by/issue/37228/415166>

Bilgi Mimarisi. (2014, 20 Aralık). Vikipedi İçinde. Erişim Adresi (8 Mayıs 2015): [http://tr.wikipedia.org/wiki/Bilgi\\_mimarisi](http://tr.wikipedia.org/wiki/Bilgi_mimarisi)

Chan, H. F., Guillot, M., Page, L. ve Torgler, B. (2015). The Inner Quality Of An Article: Will Time Tell? Scientometrics, 104, s. 19-41. doi:10.1007/s11192-015-1581-y

EBYS Zirvesi 2016. ( 2016). Erişim adresi: <http://bilbem.ankara.edu.tr/2016/04/21/ebys-zirvesi-2016/>

Özdemirci, F. ve Torunlar, M. (2015) Bilgi Çağında Arşivsel Bilgi Analizi: Bilgi-İktidar- İdeoloji-Devlet. Ankara Üniversitesi Basımevi.







"Scan to reach the software of this publication and the other products of COE-DAT"  
[www.coedat.nato.int](http://www.coedat.nato.int)