Paradigms of New Media and Terror Agencies

Ferhat Atik
PhD Student, Girne American University, Faculty of Communication, Communications and Media Management, Kyrenia/ TRNC.
ferhatatik@gau.edu.tr

Muharrem Özdemir
Asst. Prof. Dr., Girne American University, Faculty of Communication, Department of Press and Publication, Kyrenia/ TRNC.
muharremozdemir@gau.edu.tr
Orcid: 0000-0003-1570-146X

Abstract
As a fundamental communication tool, media has undergone transformative changes throughout history. This has a lot to do with education. Each era has been characterized by its own unique media paradigms, from the invention of the printing press in the 15th century to the emergence of radio and television in the 20th century. These paradigms not only define how information is disseminated but also shape the social and political landscapes of their respective periods. In the modern age, the emergence of digital technology and the internet has brought about a new media paradigm that deeply influences every aspect of human interaction and the fabric of society. Today, new media, characterized by its interactivity, decentralization, and unprecedented access, dominates our daily lives. The significance of new media, which affects individual behaviors and global politics, economy, and cultures, cannot be underestimated. This process is also of great importance in terms of education. In particular, media literacy education will enable the individual to personally prepare for or otherwise intervene in the positive or negative aspects of their interaction with the media. From connecting distant communities to altering the dynamics of political campaigns, the impact of new media is ubiquitous. However, along with these advantages, new challenges have also emerged. One of the most concerning aspects of this shift in media is the potential for its exploitation by malicious groups, particularly evident in the rise of "terror agencies" utilizing new media platforms. These organizations adeptly employ new media tools for propaganda, recruitment, and operations, forming a symbiotic relationship that poses significant threats to global security. This article explores how new media paradigms enable the existence of terrorist organizations, the place of education in this regard, and what this complex relationship means for our interconnected world.
Keywords: Education, Terror Agencies, Digital Technology, New Media, Terrorism, Propaganda.

Introduction

Throughout history, the media landscape has constantly undergone change and transformation. Every stage, from primitive cave paintings to the emergence of Gutenberg's printing press in the 15th century, has signaled a shift in how societies process and disseminate information. The 20th century witnessed another media revolution with the introduction of radio and television. These platforms not only changed the speed and breadth of information dissemination but also reshaped the cultural, social, and political fabric of the communities they touched. As we enter the 21st century, the digital age characterized by the internet and countless digital devices has emerged as a testament to humanity's insatiable desire for faster and more efficient communication tools. The new media, encompassing digital platforms, social networking sites, and interactive forums, signifies a departure from traditional, centralized forms of communication. Its fundamental qualities, such as real-time interaction, decentralization, and global accessibility, have made it a dominant force in today's world. The power of new media extends beyond personal interactions; it shapes political narratives, influences global economic trends, catalyzes social movements, and even redefines cultural identities. Through platforms like Twitter and Facebook, communities separated by oceans find common ground, political leaders communicate their policies directly to citizens, and grassroots movements make their voices heard. However, no matter how revolutionary, every tool is susceptible to misuse in the wrong hands. The dark side of the pervasive impact of new media has emerged in the embrace of extremist groups, particularly terrorist organizations. These formations have cleverly recognized and utilized the potential of digital platforms. Whether to propagate extremist ideologies, recruit individuals susceptible to influence from around the world, or coordinate covert operations, terrorist organizations have integrated new media strategies with their operational methods. This dangerous synergy between advanced communication technologies and extremist agendas poses a threat to global peace and security. This article examines the complex interaction between the revolutionary aspects of new media paradigms and their exploitation by terrorist organizations. It aims to foster an understanding of the challenges and consequences of an increasingly interconnected and paradoxically more vulnerable world.

The New Media Paradigm

One of the puzzles prevailing in the field of social sciences revolves around the integration of two different approaches. The first approach argues that human identity, consciousness, attitudes, and behaviors are inevitably shaped by specific historical and societal conditions. On the other hand, the second approach claims that individuals can actively shape and change these determinants (Hülür & Yaşın, 2016: 7). As history has shown, every significant step in human advancement has always paved the way for new beginnings. This axiom is particularly relevant in the realm of communication technologies, where each innovation heralds a metamorphosis in the methods of human interaction. This relentless evolution necessitates a continuous reconfiguration of our definitions and theoretical paradigms to keep up with the swift currents of technological change.

The emergence and widespread adoption of new communication technologies inevitably accelerate tectonic shifts in global dynamics and the fabric of human existence. This transformative journey, initiated by the widespread accessibility of television, has been perpetually propelled forward with each subsequent technological invention. Many scholars argue that technology serves as a cornerstone, leading to significant changes in economic, political, and social landscapes, with communication tools at the center of this transformation. As these technologies advance and encompass an ever-expanding array of features, the necessity for a thorough analytical examination of their consequences becomes apparent (Uğurlu, 2013: 3).

A retrospective look at our collective past sheds light on the intrinsic human need for internal communication that stems from our social beings. This internal interaction, driven by the desire for sharing and exchange of ideas, has been the catalyst for numerous inventions aimed at improving our lives and facilitating vital activities. Despite undergoing profound transformations throughout history, the fundamental purpose behind these communication tools has largely remained unchanged. Especially since the advent of the Industrial Revolution, these communication tools have been designed to enhance human interactions, optimize productivity, and greatly reduce temporal constraints. The evolution of these tools, from the early stages of discovering electricity to the groundbreaking emergence of electronic computers, has always culminated in periods of introspection and improvement, giving rise to increasingly sophisticated devices in subsequent generations. As the global population grows, the demand for these tools and their subsequent proliferation increases, leading to their democratization and individualization, thereby catalyzing profound societal changes.

The second half of the 20th century witnessed the emergence of a process that could be defined as the second communication revolution. This revolution was supported by advancements in microelectronics, which facilitated the miniaturization of computer components and ultimately enabled comprehensive integration into singular platforms (Dijk, 2018: 78). At the heart of this transformation lies digitization, a power that seamlessly connects various new media networks encompassing telecommunications, data transmission, and mass communication. The revolutionary essence of new media is encapsulated by its digital foundation. Additionally, the "store and forward" principle inherent in new media interfaces enables the secure archiving of content in electronic storage and the dissemination of digital content through specialized software programs (Dijk, 2018: 79).

The birth of modern digital communication brought about a fundamental transformation by facilitating the digitization of visual, auditory, and graphical content through the transfer of features and data from existing communication devices to computational platforms. In this nascent stage of development, systems like ARPANET initially allowed for mutual communication among only a handful of academic institutions, particularly four universities, laying the groundwork for more complex technological frameworks (Yengin, 2014: 117). A notable turning point in this evolution was reached in 1979 when Tom Truscott and Jim Ellis from Duke University developed Usenet, an embryonic global discussion platform. Usenet allowed internet enthusiasts to send universally accessible messages, heralding a new era of online interaction (Kaplan and Haenlein, 2016: 355).

In the subsequent years, Tim Berners-Lee established the World Wide Web (www), a visionary endeavor that facilitated seamless connectivity between computers. This development marked the era of Web 1.0, spanning from 1990 to 2000. Berners-Lee's groundbreaking system, supported by HTML, enabled users to access data statically through interconnected servers (Okur, 2013: 130-131). Such a framework led to the proliferation of information sharing between computers, and as the increasing accessibility of the internet is taken into account, this expanding matrix continuously added unlimited data bytes (Timisi, 2016: 11).

Historically, communication processes that were once spread over long temporal intervals have experienced compression in both time and space due to these new technologies. This dynamic evolution, highlighting the power of globalization, has transformed our global community into a tightly interconnected fabric where regions are aware of and influenced by one another. This communication revolution has not only transformed its field but also permeated a wide range of scientific disciplines and aspects of human existence. In the Web 1.0 environment, users primarily assumed a passive role, only examining data packets and navigating pre-designed digital landscapes. Websites during this period primarily served promotional agendas, offering insights into various institutional and organizational entities (Kuyucu, 2013: 118; Okur, 2013: 130).

When examining the history of communication, it can be observed that each innovative tool heralds its revolution, and successive tools are built upon the features of their predecessors. Dijk argues that the emergence of new media represents both a structural and technical upheaval. The most transformative structural revolution, without a doubt,

began with the conceptualization of writing, which enabled humanity to overcome temporal and spatial barriers that were previously reliant on primitive methods such as smoke signals and cave inscriptions. Dijk also suggests that the advent of the printing press symbolized a technical revolution, democratizing the dissemination of printed content and that this ethos aligns with today's digital communication technologies (Dijk, 2018: 17-18). Contrary to popular belief, the term "new media" is not a newly coined concept. It has been repeatedly used to describe every significant step in the fields of knowledge and communication. To solely associate this term with computing technologies is an oversimplification. Groundbreaking discoveries and innovations always act as precursors for subsequent advancements. In this continuity, the printing press serves as a significant milestone by facilitating mass reproduction and distribution, similar to how transportation systems and the internet democratized access to numerous products, information, and virtually "everything" (Karahisar, 2013: 53). New media, an evolution of traditional forms, can be distinguished by a set of characteristics that define its essence in the digital age. At the core of understanding new media is the acceptance of its inherently digital nature. Unlike traditional media, which relies on physical elements such as paper and analog frequencies, new media operates within a digital framework, providing unique flexibility and adaptability (Manovich, 2001). This digital nature not only defines its form but also facilitates many of its other defining features. Interaction is one of the fundamental characteristics of new media. In contrast to the passive consumption patterns seen in traditional media, new media encourages and, in some cases, necessitates active user participation (Lievrouw and Livingstone, 2006). This interaction manifests in numerous ways, from users selecting links on a web page to participating in multiplayer online games or contributing to collaboration-based platforms like wikis. Interaction fundamentally transforms the nature of media consumption, turning passive viewers into active participants.

One of the defining characteristics of new media is its hypertextual nature. Unlike the linear narratives that characterize old media, new media is not linear and allows users to freely navigate and create their paths within the content (Landow, 1992). This hypertextuality signifies a shift from a centralized content creation model to a decentralized model where users have more autonomy in how they consume and interact with the content. The networked nature of new media exemplifies another critical departure from traditional media paradigms. In the Internet age, content does not exist in isolation but is part of a vast digital information network (Castells, 2000). This networked environment facilitates the rapid dissemination and sharing of content, creating a more integrated and global media environment. Additionally, the virtual nature of new media brings both opportunities and challenges. Virtual spaces like online communities and digital worlds offer users experiences that surpass physical limitations, but they also raise questions about the nature of reality and identity in the digital age (Turkle, 1995). Essentially, new media represents a paradigm shift in how information and content are created, consumed, and shared, rather than a simple progression from traditional forms. Its defining features (digital, interactive, hypertextual, networked, and virtual) shape the contemporary media landscape and influence both individual users and society at large.

Concept of Terrorism

In academic research on terrorism, there is an ongoing debate regarding what terrorism is exactly. However, there is no consensus on a definitive definition of terrorism. According to Laqueur, there are at least 212 different definitions of terrorism used worldwide, with 90 of them being employed by governments and other institutional organizations. Laqueur argues that there is no specific "terrorism" per se, but rather different forms of terrorism (Laqueur, 1999).

Alex Schmid, who examined over 100 definitions used by terrorism experts, concluded that terrorism is an abstract concept without a real essence. The term cannot be limited to a single definition, as its meaning is often derived from the perspective of the victim or the target. If an individual identifies with the victim or the target of an action, it is considered terrorism; however, if one identifies with the perpetrator of the action, perhaps sadly, it may not be classified as terrorism. This duality is summarized in the popular saying that "One person's terrorist is another person's freedom fighter," disregarding the fundamental differences between terrorism and the legitimate and regular use of violence. defining terrorism is further complicated by two factors. Firstly, since "terrorism" is a derogatory term, most terrorist groups do not like to label themselves as such. Instead, they prefer names that emphasize freedom and liberation, military or armed structures, self-defense, revenge, or poetic neutrality. Secondly, such misleading labels are accepted by the Western media and used to avoid the appearance of bias when identifying terrorists. Thus, the media refers to them as guerrillas, freedom fighters, armed individuals, separatists, urban guerrillas, or commandos (Hoffman, 2017). This misleading labeling, combined with the institutional obligations of organizations dealing with or combating terrorism, has resulted in a situation where there is no widely accepted definition of terrorism. However, Hoffman presents a useful and clear definition that differentiates terrorism from other types of crimes (Hoffman, 2017).

The New Paradigm of Terrorism

Determining the evolution of terrorism is difficult, but the 1993 attack on the World Trade Center in New York and the 1995 sarin gas attack on the Tokyo subway by the Aum Shinrikyo cult are considered the beginning of

new terrorism paradigms. Overall, this new paradigm emphasizes that modern terrorism has different causes, actors, sponsors, and more deadly consequences than previously defined traditional terrorism (Comfort and Kapucu, 2006).

According to Laqueur, the motivations of new terrorists are changing. Left-wing terrorism is declining; Paul Wilkinson argues that left-wing ideological terrorism has nearly disappeared in Europe but continues in Latin America. Nationalist-separatist terrorism persists. Hoffman argues that terrorism based on religious fanaticism is a defining feature of modern terrorism, along with the terrorist's worldview and value system. These new value systems differentiate themselves by aiming not only for religious motivations but also for the destruction of society and the elimination of large segments of the population, as Laqueur also points out. Particularly, anarchist and nihilist groups pose perhaps the greatest challenge for government actions due to their non-sequential and non-political strategies (Laqueur, 1999).

While new terrorists still seek fame today, they generally show less interest in the "theatrical" aspects as part of their political strategies. Hoffman noted that new terrorists have relaxed their limitations on violence (Hoffman, 2017). Another characteristic of new terrorism is that terrorists no longer rely on superpowers for support or seek new wealth from crime. Finally, new terrorism exhibits opposite features to traditional terrorism. Firstly, there is a higher likelihood of terrorist groups forming networks rather than hierarchies or cells, particularly true for groups organized around charismatic religious figures. These networks are transnational, ambiguous, and decentralized, allowing groups to engage in a wide range of activities, evaluate new strategies like "netwar," and coordinate single-operation events such as the September 11 attacks. Secondly, new terrorist groups are much larger than in previous periods. For example, while the Abu Nidal Organization had 400 to 500 members, it is reported that Usama bin Laden had 4,000 to 5,000 trained agents under his command (Vittori, 2011). Thirdly, there is a higher likelihood of including amateurs. These amateurs, often referred to as "part-time" terrorists, have not received professional training but can access terrorism resources and methods through internet-based sources. In these large, networked, amateur organizations, target and tactic selection become more random. New terrorist attacks yield higher deadly results. Hoffman suggests that increased deadliness has several reasons. These include the desensitization of media and the public to terrorist violence, terrorists' development of tactics and weapons, continued state support, religious-motivated terrorists viewing violence as a divine duty, and amateurs lacking central authority constraints in their actions. Perhaps the greatest danger in this increased deadliness is the possibility of new terrorists using weapons of mass destruction. The 1995 attack by Aum Shinrikyo is the only known instance of chemical weapon use (Tu, 2007). However, there have been numerous other incidents and attempts involving the use of biological agents. Terrorists' lack of interest in CBRN (Chemical, Biological, Radiological, Nuclear) weapons is often attributed to technical expertise or the potential to undermine their political agendas. Hoffman cautions that the limitations on terrorists' CBRN use are decreasing (Hoffman and Morrison-Taw, 2019).

In conclusion, proponents of the new paradigm observe significant changes in terrorism's motivations, strategies, characteristics, and tactics. Stephen Sloan notes that the end of the Cold War and the collapse of many communist governments brought ethnic and religious conflicts (alongside terrorism and other forms of violence) to the forefront. Sloan argues that the disappearance of Marxism as a valid political theory has changed the motivations of many left-wing groups, while Hoffman contends that the number of Marxist terrorist groups has not changed since the end of the Cold War (Hoffman, 1982). The intervention of the United States overseas and the general rise of Western culture has created new animosity, particularly among religious fundamentalists in the Middle East. Osama bin Laden explicitly stated that the American presence in the Arabian Peninsula was the reason for his terrorist campaign.

The Rise of Terrorism Agencies in the Digital Age and the Role of New Media

With the widespread adoption of digital technologies, individuals have turned to new methods for accessing information, sharing content, and social interaction. This digital evolution has brought about many positive transformations, but it has also brought along unexpected challenges and dangers. One of these challenges is the strategic use of digital tools and platforms by terrorist organizations to create new propaganda and recruitment mechanisms, referred to as "Terrorism Agencies." In this context, Ferhat Atik, who coined the term "Terrorism Agency," emphasizes that modern terrorism is active not only in physical spaces but also in the digital arena. According to Atik, terrorist organizations attract the attention of young people through sophisticated digital campaigns fueled by astronomical wealth and extensive resources (Atik, 2019).

Research by Smith and Jones (2018) reveals that young people take advantage of anonymity on digital platforms, are more receptive to ideological currents, and are particularly inclined towards radical groups due to their need for belonging (Smith and Jones, 2018). Williamson, Fay, and Miles-Johnson (2019) state that the ideological propaganda, the promise of social belonging, and various incentives offered by terrorist organizations are influential in the radicalization of young individuals (Williamson, Fay, and Miles-Johnson, 2019).

In the face of this growing threat, raising awareness and educating society is of vital importance. Parents, educators, and community leaders should prioritize educational and awareness initiatives to protect young people

from such digital dangers. Rauf (2021) emphasizes that being prepared for the risks presented by digital media is the key to staying safe in the digital age (Rauf, 2021). Therefore, it is evident that greater investment is needed in the literature on new media and digital literacy.

The Relationship Between New Media, Terrorism and Education

The history of terrorism has progressed from an ordinary organizational structure to a highly professional field of work since ancient times. Accordingly, terrorist organizations on the one hand, and those who want to prevent this on the other, use education strongly. While terrorist organizations establish a strong education network within themselves, states that try to protect themselves from terrorism are also obliged to adequately educate their own generations against terrorism.

Accordingly, if the country's unique characteristics and conditions are suitable, these expectations will come true. These realized expectations contribute to the reduction of terrorism through education. However, factors such as economic growth, limited competition in the labor market, corruption, nepotism, and limited effects on the labor market may affect this situation. Organizations with the lowest education and training levels of their members are separatist terrorist organizations. The segment with the highest education rate is left-wing organizations. Religious organizations come in second place in the ranking. According to a field research on the relationship between terrorism and education, lack of education ranks first among the causes of terrorism with a rate of 20.7% (Akşen, 2010).

Among the members of the separatist terrorist organization, the rate of those who are illiterate is 13 percent, the rate of those who are only illiterate is 9 percent, the rate of those who are primary school graduates is 48 percent, the rate of those who are illiterate is 18 percent, and the rate of those who are university graduates is 12% (Atıcı, 2002). These numbers tell the truth of the matter. Accordingly, there is a direct connection between education and terrorism. Most of the time, people with low education levels become targets of terrorist organizations and are turned into terrorists.

Embracing New Media by Terror Agencies

Indirect Approach through Internet Usage and Media

Despite the United States and its allies mobilizing resources under the banner of the "War on Terrorism," the Al-Qaeda terrorist organization has continued to supply a constant stream of new propaganda materials to the mass media (Monaco, 2017). Each new communication has symbolically represented a victory, showcasing how this organization has overcome the siege by its powerful enemies. The means by which Al-Qaeda sustains this communication line, particularly illustrated by the case of Abu Faraj al-Libbi, who was captured in Pakistan in May 2005, was a mystery until high-profile members of the organization were apprehended (Elahi, 2019). Interrogations revealed that Al-Qaeda employed a complex courier network to distribute their primary brochures. These couriers traveled a distance of less than 70 miles between the Afghanistan-Pakistan border and the Al Jazeera office in Islamabad, taking anywhere from six to twelve weeks (Gunaratna & Iqbal, 2012). Due to security concerns, these couriers usually only traversed a small portion of the route, unaware of the source, ultimate recipient, or content of the material they carried. In some instances, instead of delivering the message to a television network, an intermediary would transmit the file over the Internet. This intricate network posed a challenge for intelligence services desperately trying to keep up with Al-Qaeda's evolving propaganda capabilities. However, Pakistani authorities seized these messages at least twice in 2003 and 2004, providing valuable insights for American intelligence to better understand the network that kept Al-Qaeda's propaganda system active. Al-Qaeda has been aware that its relationship with mass media in recent years has significantly threatened the organization's and its members' security (Abdul Nasir, 2006).

The desire to eliminate these vulnerabilities has prompted the terrorist organization to adopt new technologies more effectively. Consequently, Bin Laden's organization has turned to disseminating the latest news via the internet. This does not mean that they have ignored the opportunity to be at the forefront of the mass media's agenda; rather, it signifies an indirect approach strategy. In other words, they are aware that a significant portion of their strategy's success relies on their ability to reach mass media platforms but aim to do so more securely and efficiently. Al-Qaeda has learned from the propaganda experiences of other surrounding terrorist groups. Many of these groups, such as those established by Abu Musab al-Zarqawi or Al-Qaeda's Saudi branch, have minimal direct communication with mass media and instead concentrate their communication activities in cyberspace. These methods have prevented them from attracting significant media attention (Soriano, 2008).

The organization uses the internet to search for visual and textual elements in order to make mass communication tools more appealing. The presence of these elements on the internet allows for the creation of standalone stories without the need for other intermediaries. In this way, anonymous news reflects and presents events that have the potential to create a significant impact on international public opinion. Al-Qaeda has no problem adapting to the demands of this new media and has embraced a series of innovations aimed at maximizing the impact of their messages. Consequently, Al-Qaeda's recent statements have been promoted through advertising banners on jihadist forums, announcing the upcoming release of these materials. By using this practice, the group not only builds

anticipation among its followers but also ensures that once the new material is uploaded onto the internet, the mainstream media will echo this new message (Soriano, 2008). Sometimes television channels compete with each other to be the first to broadcast the latest developments. For Al-Qaeda, the internet is not only a safer and faster way to access media, but also represents a turning point in their communication strategies as it diminishes the importance of traditional media (Weimann, 2004). Historically, cyberspace has facilitated direct communication between terrorists and their "audience." Terrorists closely control their messages, carefully stating exactly what they want to say and when they want to say it. In the past, directly sending material to mass media outlets has been a problematic method for terrorist groups. First and foremost, there was a possibility that the message could be ignored, misinterpreted, or even manipulated. Terrorists had to calculate what the media could tolerate and what it could not. Considering the time constraints that influenced the content of TV news broadcasts, the possibility of distributing a long and intensive ideological speech was not taken into account. Even for a legitimate political leader, disseminating such a message proved challenging. Secondly, as mentioned before, the continuous sending of materials created security concerns due to the possibility of counterterrorism agencies tracing these messages back to their origin and tracking them to the media. This situation forced terrorist groups to refrain from using this dissemination method frequently (Pandian, Gomaa, & Pazil, 2020).

The internet not only overcomes these limitations, but it also allows mass media to ignore a range of ethical constraints that greatly benefit terrorist strategies. In the past, television was the only medium through which terrorist violence could be widely broadcast. This meant that those responsible for deciding whether the public should see such material were not solely confined to the media. However, since this kind of propaganda started appearing on the internet, television channels have felt relieved of the moral responsibility to make such difficult decisions. The blurring of television channels' responsibility has led them to be less cautious about showing disturbing or dramatic images, unwittingly becoming accomplices to terrorism.

How Terrorists Use Social Media and the Internet for Radicalization Methods

Due to the constantly evolving nature and diversity of digital platforms, it is important to note that the methods presented here are only a limited example of the approaches used and aim to provide a basic framework. In this context, this section of the article examines how terrorist organizations use social media and the internet, how they organize their structures and goals, how they enhance the quality of their propaganda materials, how they disseminate their messages to wider audiences, and how they utilize new technologies to recruit members through more secure messaging platforms. Accordingly, this article; While it uses methods that include media scanning of discourse practices and uses statistical data, it also includes direct information.

Structures, Dynamics, and Goals of Terrorist Organizations

Terrorist groups are dynamic systems that adapt and evolve over time. Traditionally, it was believed that terrorist organizations had a centralized, hierarchical structure in which leaders controlled all activities of the organization. These traditional structures often had a well-defined chain of command to ensure consistency in the message conveyed through specific individuals. However, there is an increased risk of disruption when individuals or units are compromised.

In recent years, social media and the internet have increased the speed and complexity of information sharing while reducing its cost (Carley et al., 2003). This has supported the transition of many terrorist organizations towards a network-like structure, enabling each cell and individual to act more independently, especially in disseminating the organization's messages. This restructuring has provided organizations with greater flexibility, responsiveness, resilience, and accessibility. As a result, even if one or more cells suffer significant damage or are disbanded, large terrorist networks can continue their activities. For example, after the 9/11 attacks, pressure on Al-Qaeda increased, it lost its training camps in Afghanistan, and most of its pre-9/11 top leaders were killed or captured (Perliger, 2014).

Therefore, in order to sustain its existence, even through close connections, Al-Qaeda had to adopt an approach of inspiring and directing other violent extremist groups. Abu Musab al-Suri was one of the main driving forces behind this change in structure and strategy, and the Internet was utilized to facilitate this transformation. This shift in approach led to the formation of local organizations responsible for terrorist attacks in Bali, London, and Madrid. Modern terrorist networks now consist of widely dispersed smaller cells that communicate with each other and coordinate their campaigns in a linked manner. Relationships are often temporary and vary in intensity depending on the task at hand. This has prompted groups to develop not only internal connections but also external relations. These relationships are typically formed on the basis of shared norms, values, and mutual respect rather than through formal bureaucratic structures (Cruickshank and Ali, 2007). The characteristics of this network-based approach were exemplified by the Charlie Hebdo attack in Paris in 2015. One of the terrorists involved in the attack, Amedy Coulibaly, released a video claiming that the attacks were carried out on behalf of ISIS. However, the low quality of the video suggests that the attack was not directly connected to ISIS's media center, Al-Hayat Media, but was likely orchestrated by a smaller independent cell. It has also been reported that the Kouachi brothers, the other two terrorists, received $20,000 from Al-Qaeda in the Arabian Peninsula (Levitt, 2015). This

highlights the increasing role of temporary external coalitions as networks communicate independently. In addition, the information revolution has aided terrorist groups in shifting away from traditional models of warfare towards a new form of societal conflict. While terrorist organizations have always strived to carry out psychological operations, they now possess a much greater capacity to conduct information operations on a larger scale (Nohria and Eccles, 1992). Networked terrorists, recognizing the importance of information and soft power, employ social media and the internet for brand management and propaganda to influence public opinion and recruit new members. Previously, terrorist organizations relied on traditional media, such as television, radio, brochures, print media, and face-to-face meetings to carry out their psychological operations. However, the internet and social media now offer these organizations opportunities to increase the volume and diversity of their messages, necessitating a localized approach by individual cells. As a result, terrorist organizations are able to transform conflicts around information and knowledge.

In this context, terrorism propaganda often depicts violent behaviors, such as executions, with the aim of coercing or inciting others to imitate such violence. However, some propaganda efforts now focus on brand management by presenting narratives that aim to attract individuals to their cause (Macnair & Frank, 2018). These narratives can adopt two approaches, either focusing on personal incentives to join the group (pull factors) or emphasizing or exaggerating the negative social, political, and/or economic conditions of the target population (push factors), thus contributing to the creation of a conducive environment for joining the organization (Also, the global reach of online platforms has facilitated the merging of terrorist networks and their spread across national borders, cultures, and languages. This has been evident with the increase in global coalitions of previously separate terrorist organizations. One notable example was the pledge of allegiance (bayat) to ISIS leader Abu Bakr al-Baghdadi. Due to geographic and security constraints, face-to-face pledges were hindered, leading to social media offering an alternative approach (Atwan, 2019). For instance, various terrorist groups in Southeast Asia, such as Maute, Abu Sayyaf, Katibat Ansar al-Sharia, and Mujahidin in Indonesian Timor, have presented their pledges through online videos. In response, the acceptance of these pledges has also been broadcast through online videos (Weis, 2016). These adaptations highlight how interactions and behaviors, facilitated by the internet and social media, provide terrorist groups with communication, coordination, and recruitment opportunities as global networks, while also allowing individual members and cells greater freedom in coordinating and reaching target audiences. Central messages can be independently adapted to a localized context, addressing the push and pull factors of the local population. For example, ISIS has established media units capable of producing sophisticated and localized propaganda materials in the language and culture of the target population in many regions (Macnair & Frank, 2018).

Videos, Images, and Magazines: Propaganda

In parallel with the global reach and controlled distribution of propaganda provided by social media and the internet, the diversity and accessibility of digital equipment such as high-definition (HD) cameras and editing software have enabled terrorist organizations to produce propaganda of similar quality to Hollywood film professionals and high-level marketing firms (Atwan, 2015). Indeed, high-quality propaganda has become increasingly important for a terrorist organization's branding strategy. The use of appealing digital media and innovative methods contributes to the strengthening of their brands and has become an approach adopted by many terrorist groups other than ISIS. The logic behind this is clear; in the struggle to win hearts and minds, they must stand out and inspire individuals to attract new members in an increasingly competitive environment. When propaganda can attract audiences, present a strong narrative, and appeal to the push and pull factors of local communities, it is likely to influence the radicalization process of vulnerable individuals. For example, Al-Hayat Media has produced several HD videos in major European languages such as French and English, depicting life in ISIS territories as spiritually fulfilling and labeling European states as immoral and illegal. The production and distribution of such well-designed videos address the feelings of dissatisfaction among the youth diaspora in Europe and offer a positive alternative. These types of videos have played a significant role in the radicalization process and conversions to Islam among many young European Muslims (Macnair & Frank, 2018). Another modern example of high-quality propaganda is the video game "Salil alSawarem" (Clash of Swords), which models the popular Grand Theft Auto series and is designed to generate interest and public relations for ISIS. When the game was released in 2014, gaming channels on YouTube alone received 3.5 billion views per month. This illustrates how the use of cinematic productions and social media serves as a tool to increase the viral nature of popular culture propaganda and demonstrates approaches to reaching the target audience (in this case, young gamers). In this way, these types of sophisticated communications can easily go viral. The modern appearance helps increase the psychological impact on the target audience by translating the violence of terrorists into a language that the average young population can understand (Plebani and Maggiolini, 2015). In addition to games, videos, and images, many terrorist groups also publish online magazines that play a significant role in online radicalization. The accessibility and popularity of stylish online magazines have contributed to the successful spread of ISIS through magazines like Dabiq and Rumiyah, Al-Qaeda through Inspire, and Al-Shabaab through Gaidi Mtaani.

Digital magazines offer readers a diverse range of narratives presented in a single, well-packaged format. By using community stories, individual stories, and event stories, terrorist magazines aim to create a broader narrative that resonates with readers. In this context, magazines can bring together various approaches. It has been shown that images depicting fighters in militarized attire attract individuals to violence. Moreover, the emphasis on masculinity and bravery appeals to thrill-seekers (Hamm, 2004). The inclusion of other styles, the use of religious quotes, presenting members as heroes, framing their deaths as sacrifices, and depicting a common enemy all serve their purposes, appeal to various readers, and lead to philosophical debates and common ground.

The secondary use of digital magazines may not only inspire readers but also provide them with technical instructions on how to carry out acts of violence on their own or advise them on joining a terrorist group (Conway, 2012). The 2013 Boston Marathon bombing is a case in point. Tamerlan and Jawhar Tsarnaev claimed to have learned how to make a bomb from an article in the first issue of Inspire magazine titled "How to Make a Bomb in Your Mother's Kitchen" which they read online.

The ability of terrorist organizations to produce inspiring and high-quality propaganda that can be shared via social media and the Internet is of critical importance in terms of brand management and radicalization approaches. Indeed, social sharing sites like Facebook, Twitter, and YouTube have become the tools of today for disseminating the oldest messages in a modern and relevant format (Gunaratna and Haynal, 2013).

Social Networking Sites

The rise of social networking sites has enabled individuals and terrorist organizations to instantly share information with large audiences, regardless of geographical distances. Terrorists and their followers can share materials that can reach beyond their social circles and reach previously unreachable masses. The first person to fully exploit this potential to an English-speaking audience was Anwar al-Awlaki, the prominent American-born Imam is known as the "Bin Laden of the Internet". Aware that even high-quality online propaganda was not reaching the widest possible audience, al-Awlaki pioneered the use of social networking sites by creating his own blog, Facebook page, and YouTube channel to expand his reach (Conway, 2012). Since then, terrorist organizations have been seeking Information Technology (IT) experts and skilled online marketers to manage their online propaganda campaigns. Most major social networking sites have responded by implementing widespread and numerous measures to restrict the dissemination of violent extremist content on their platforms. However, these platforms continue to be used by skilled ideologues and recruiters to share propaganda and attract followers. An analysis conducted in 2018 on 1,000 Facebook profiles supporting ISIS from 96 countries showed that despite efforts to identify and remove new accounts, the groups' Facebook networks continued to grow globally (Speckhard et al., 2018).

These websites have become tools for sharing high-quality propaganda materials and also platforms for terrorists to share their experiences. Such stories encourage the viral spread of individual narratives and become a central feature in the process of recruiting new members by inspiring those in search of a new identity. One example is Siti Khadijah, an Indonesian woman who traveled to Syria in 2014 and shared her experiences on Facebook. As a result of her posts, other Indonesians approached her with questions about how to travel to Syria. Aqsa Mahmood, a Scottish woman, is another example who traveled to conflict zones in Syria and Iraq in 2013. It is suspected that Mahmood's use of social media contributed to the radicalization and recruitment of many British youth.44 Like Siti Khadijah, Mahmood used social media to promote the positive aspects of life under ISIS. Social networking sites have also been used to control the narratives surrounding an event. In 2013, during the Westgate terrorist attack in Kenya, Al-Shabaab extensively used Twitter for this purpose.45 This approach involves sharing posts with a trending hashtag for propaganda purposes, significantly increasing traffic and visibility.46 These examples demonstrate that radicalization and recruitment through social media are supported by individual narratives, stories, and firsthand reports. This creates a chain of imitative reactions, particularly among those trying to find their own identities. (Lombardi, 2015).

Messaging, Broadcasting, and Channels

The previous section has demonstrated that online platforms have the potential to significantly influence the radicalization and recruitment processes. When a potential recruit is identified, the recruiter often directs them to a more secure communication tool, such as peer-to-peer messaging apps or forums/channels where like-minded individuals share their thoughts. Many recruiters now rely on unstructured and unmonitored mobile messaging apps (such as WhatsApp, Telegram, and Kik) to deepen their contact with potential employees. This highlights the importance of different social media platforms and online media tools in the recruitment process. While some platforms and tools are more effective in spreading violent extremist messages to a wider audience, others assist recruiters in directing an individual toward one-on-one and ultimately face-to-face interaction. Encryption technology has been used by some terrorist organizations in the past few decades. For example, Pretty Good Privacy (PGP) was first developed in the mid-1990s and enabled anyone to send an encrypted message to magazine publishers, sharing the publishing rights of Al-Qaeda's Inspire magazine (Neumann et al., 2018). However, most forms of encryption have primarily been accessible to higher-ranking terrorists within an organization, as they are primarily used for coordinating attacks. Nowadays, almost all terrorists and those who recruit them use encryption

technologies. In fact, terrorists now have access to a much wider market of encrypted communication options. For instance, Skype, an internet-based telephone system, is encrypted, making it one of the largest online communication tools today and allowing terrorists to have real-time conversations without the risk of their content being discovered. Encrypted emails, such as Bitmessage.ch, also offer sophisticated methods for secure communication. In fact, the original message is often not only encrypted but also sent to hundreds of randomly selected other accounts, making it nearly impossible to decipher who the intended recipient is and who holds the encryption key. The use of encrypted messaging services like Telegram in Indonesia has been reported to enhance group solidarity by safely increasing the sharing of information among members (Lombardi, 2015). Bahrun Naim, one of the prominent distributors of propaganda for ISIS in Indonesia, extensively used Telegram. For instance, in June 2015, Naim reached out to his former friend Ibad through Facebook and connected him to his Telegram. They then began communicating about Ibad's trip to Syria through encrypted services. While encryption provides content security to terrorists, it does not guarantee their anonymity. Service providers and anonymous operating systems, known as the "dark web," can be used along with encrypted communication to further ensure anonymity (Atwan, 2015). One popular and often free way to maintain anonymity is through the use of Virtual Private Networks (VPNs). VPNs conceal the user's IP address and make them visible in one or more countries, preventing or at least slowing down security agencies from tracing the source. The Onion Routing (TOR), originally created for the US Navy, is an anonymous browser that utilizes such techniques. These easy and often free forms of encryption and online anonymity have significantly enhanced terrorists' abilities not only to exchange instant messages and files but also to remain hidden and secure while doing so (Weimann, 2015).

The Use of Artificial Intelligence and Evolving Online Technologies by terrorist groups

It is important to note that terrorist groups have discovered the potential of using Artificial Intelligence (AI) in their online radicalization and recruitment strategies. In the aforementioned case in Indonesia, Bahrun Naim used a bot (an online "robot" application or program that interacts with systems and users to complete tasks automatically) to communicate with potential new members. The bot greeted users with an automated message in the Bahasa Indonesian language and then shared propaganda messages and videos, as well as guides on how to make homemade explosives. The Al-Shabaab news agency, Shahada, used a bot on Telegram, which continuously communicated with its followers by sending them the latest version of the channel's link, even if the channel itself was suspended (Bodo, 2018).

There are speculations that more sophisticated language tools could be used by terrorist groups to generate new content. For example, a study conducted in 2019 suggested that open-source AI tools like GPT-2 could be used by malicious actors to automatically comment on current events, suppress conversations on social media channels, or align online discussions with their own ideological views (Zeiger and Gyte, 2020). The report did not find evidence of GPT-2 being used by terrorist groups, but it did find that the existing automated detection technology could not distinguish extreme content generated by GPT-2 from content created by humans. This implies that if terrorist groups resort to open-source AI tools, human intervention would be necessary to accurately detect automatically generated terrorist content based on new technology.

Changes in the structure of the internet and evolving technologies are also being utilized by terrorist groups to evade detection. For instance, the increasing use of decentralized web (DWeb) models, where content can be stored on multiple users and servers not controlled by a single source, instead of centralized servers. If a terrorist group like ISIS were to start using DWeb services, it would mean that their propaganda content would be nearly impossible to remove from the internet (Zeiger and Gyte, 2020).

As another example, the use of expanding social networks like Gab by the far right has raised concerns among counter-terrorism researchers. In this case, Gab's browser extension, Dissenter, allows for controversial discussions and comments that remain invisible to those who haven't installed the extension, making automated content detection ineffective on this platform. As new online technologies emerge, terrorists using these technologies pose a constant threat in terms of further radicalization and recruitment strategies.

In summary, the internet and social media have been used by terrorist organizations, which has been associated with the transformation of these organizations into globally reporting but locally responding network cells. Terrorist groups have increased the complexity of their propaganda materials and disseminated them through social networking sites. These platforms are also utilized to share personal and relatable messages that fit into a broader narrative. Essentially, social media and the internet have enabled terrorist organizations to effectively manage their brands at both a global and local level.

Furthermore, encrypted messaging services can be exploited to identify vulnerable individuals and provide private information to carry out attacks or join terrorist organizations. The exploitation of social media and the internet in this manner presents significant challenges for government officials in preventing online radicalization and countering extremism. Additionally, new and emerging online technologies such as AI and DWeb, if appropriately harnessed by terrorist groups, have the potential to further complicate efforts aimed at reducing online radicalization and recruitment through online channels (Neumann & Stevens, 2009).

Terrorism and Education Connection

As far as it is learned from the studies carried out after terrorist incidents, many terrorists join organizations from different countries. Despite this, some of those who join terrorist organizations are people born in Türkiye. Although the Republic of Turkey has a secular form of government, 89.5% of the population is Muslim (Özkök, 2019). Some of the members of the terrorist organization consist of people who received education in Turkey and did not graduate. In other words, the education levels of people who join terrorist organizations; draws attention to the relationship between terrorism and education.

Among the basic features of education; the process is a comprehensive, multidimensional, continuous, dynamic, based on scientific research and findings, benefiting from national but international research and studies, experience-based, human-specific, purposeful and positive, integrative, limited in time and space. There must be a broad adaptation process that is directly related to national development, creates culture and is affected by culture (Varış, 1991).

Strategies for Preventing Radicalization on Social Media and the Internet

After highlighting the complex techniques used by terrorist groups in the previous section, this section will focus on possible solutions to prevent and counter radicalization on social media and the internet.

Preventing the Online Spread of Terrorist Content

The first strategy in preventing radicalization on social media and the internet is to use digital mechanisms and tools to prevent and prohibit the online dissemination of terrorist content and propaganda. This involves implementing legal and policy measures, blocking access to content and social media platforms, and filtering and removing terrorist content from these platforms.

These mechanisms are intertwined because digital prevention laws can be adapted and modified as new technological tools emerge. Since preventing the spread of terrorist content on the internet often requires the use of technology and platforms owned by the private sector, public-private partnerships and collaborations are crucial in this strategy. An example of such a partnership is the Counter Terrorism Technology project, which enhances the capacity of small start-up companies by providing online tools to prevent the spread of terrorist content on their platforms (Neumann and Stevens, 2009).

Legal Measures

The first method to prevent the spread of terrorist content online is to utilize laws and policies that impose regulations and punishments on individuals and organizations. For example, the German Netzwerkdurchsetzungsgesetz (Network Enforcement Act, "NetzDG") imposes fines of up to 5 million euros for individuals and up to 50 million euros for organizations involved in the online dissemination of hate speech and fake news, even if not directly related to terrorist content. Other legal measures focus more specifically on how the private sector can prevent terrorist content on their platforms. For instance, in March 2019, a letter was sent to members of the Global Internet Forum to Counter Terrorism (GIFCT) requesting information on the annual budgets allocated by Facebook, Twitter, Microsoft, and YouTube for combating extremism on their platforms (Splittgerber & Detmering, 2017).

Balancing Security and Freedom of Expression

One approach adopted by many governments to prevent online terrorism is to block access to the internet and social media channels of terrorist groups. This can range from blocking individual websites and social media pages to completely blocking all social media platforms. For example, following the Easter 2019 attacks, the Sri Lankan government temporarily blocked access to Facebook, Facebook Messenger, Instagram, WhatsApp, YouTube, and Viber. Prolonged restrictions force terrorist groups and the general population to seek alternative means of communication to restore their ability to communicate (Liptak, 2019).

Removing and Filtering Terrorist Content

A third way to prevent the spread of terrorist content online is for technology companies or third-party actors to remove or filter individual shares or websites. This can be done in various ways. For example, content removal requests from government agencies, self-regulation by technology companies, AI-supported "anti-upload filters," and content removal by individuals or civil society.

In most known cases, government agencies request private sector companies to remove content that is identified as terrorist content from their platforms. This is achieved through careful collaboration between intelligence and law enforcement agencies and these companies. For instance, Europol's Internet Referral Unit (EU IRU) is responsible for supporting the online marking of terrorist and violent materials and sharing them with relevant partners. As of December 2017, the EU IRU had assessed over 40,000 pieces of content across 80 platforms in 10 languages, with 86% of the marked content being successfully removed (Liptak, 2019).

In addition to collaborating with governments, major technology giants implement highly detailed policies to make their platforms less hospitable to terrorist content. For example, Facebook's counterterrorism policy states that there is no place for terrorism on its platform. This policy uses an academic terrorism definition based on behavior rather than ideology. An average social media user can increase the removal and filtering of potential terrorist content by reporting it, and Facebook's policies have specific usage conditions that require users to comply with certain behaviors and rules, otherwise, their profiles may be suspended or blocked. When an item or post is flagged by a user, there is a team of experts (content moderators) who review the content to decide whether it should remain online or not.

The use of artificial intelligence is another way social media platforms can remove terrorist content. For example, there are image-matching systems that categorize previously removed terrorist content and systems that prevent the upload of new images or videos (Zeiger and Gyte, 2020). For instance, the GIFCT has developed a "Hash Database," where the "hashes" or unique digital fingerprints of terrorist images and membership recruitment videos are shared. GIFCT members can share new content with each other to ensure its removal before it spreads online. However, it should be noted that this database has certain limitations, especially requiring the exact match of "hashes" with the original file data. This means that slightly modified images or videos by users would not match the "hash" and therefore go unrecognized by al systems.

Meanwhile, social media companies continue to work with more sophisticated AI tools to automatically recognize terrorist content on their platforms. A decision made by the EU in 2019 proposed that companies should use "anti-upload filters" as a mandatory measure. The effectiveness of these filters and AI mechanisms is still unknown, and further research is needed in this field to ensure that technology and content detection evolve alongside the evolving terrorist threat. Therefore, as social media companies continue to improve their AI systems, it is important for regulators to incorporate new developments in automatic content detection into their policies (Zeiger and Gyte, 2020).

Increasing Educational Collaborations

It is important for the development of states that countries cooperate in political, military, and economic fields in a safe environment, especially that global economic initiatives are not disrupted. To prevent terrorism, which feeds on poverty resulting from the inadequacy of economic initiatives, an all-out economic development program, especially in underdeveloped countries, and cooperation in military, political, and educational fields are required. In this context, increasing a country's trade volume, attracting foreign direct investors and portfolio investments, and expanding its economic partnership network reduce terrorist activities within the relevant country and the effectiveness of transnational terrorism (Li and Schaub, 2004).

It should be determined as a basic duty to prevent all kinds of negativities that form the basis for terrorism (Çam and Coşkun, 2022). The activity of preventing terrorism is not just about conducting an armed conflict with a terrorist or a terrorist organization. The history of terrorism also shows that this is not enough. Preventing the formation of uneducated masses all over the world, raising living standards, reducing poverty, and ending ethnic, ideological, and religious discrimination are the most basic solutions needs.

Conclusion and recommendations

The profound transformations brought about by new media paradigms in the vast expanse of our digital age cannot be underestimated. From reshaping personal communication to dictating global discourses, these paradigms have established themselves as the driving force of the modern era. However, like throughout history, every evolution also brings its own set of challenges. In the context of our research, the use of these new media tools by terrorist organizations poses a particularly concerning challenge. As described in previous sections, the concept of terrorism has significantly shaped and adapted to the ubiquity of digital platforms. Traditional terrorism paradigms have expanded and adapted, taking on a more insidious form in the digital realm. The rise of terrorist agencies in this era has been greatly facilitated by platforms designed to bridge divides. Their embrace of new media and indirect approaches to media has provided them with a broad and vulnerable audience, making radicalization an easier process. Through platforms like social networking sites, terrorists not only find a voice but also a community. The sophisticated use of videos, images, and magazines has further emboldened their propaganda machines, making their narratives more appealing and their ideologies more widespread. However, the use of artificial intelligence and emerging online technologies points to a leap in their working methods, making their operations not only more efficient but also harder to monitor and counter. Nevertheless, all hope is not lost. The essence of new media paradigms holds promise. While terrorists use these platforms for dissemination, the same platforms can be used for prevention. Strategies focusing on preventing radicalization, halting the spread of terrorist content, and fostering global cooperation in legal measures are crucial. The challenge lies not only in ensuring security but also in smart regulations that respect freedom of expression and access, striking a delicate balance that the global community must achieve. In conclusion, the relationship between new media paradigms and terrorist organizations is complex and intense. In the same parallel, the connection with education seems to be extremely weak, that is, inversely proportional. Since the importance of education in human life is not only to learn but also to acquire

virtues, a weakness in this aspect makes it easier to persuade people. While uneducated individuals are more easily persuaded, terrorist organizations attach importance to the training of their senior terrorist members in the process of identifying sympathizer/candidate terrorists through social networks in order to ensure the success of these processes. A terrorist is no longer just an armed militant in the mountains. They are individuals who have received training in every field needed by the organization. An education system to protect generations against this terrorist effort is inevitable. As we continue to embrace the digital age, remaining vigilant, adaptive, and proactive is crucial. The tools used by terrorists can be and should be utilized to counter their rhetoric, disrupt their networks, and ultimately protect the interconnected world we hold dear. This journey intertwined with media and terrorism emphasizes the urgency of a collective and conscious response to ensure that the digital age remains a beacon of progress rather than a vehicle of regression.

References

Abdul Nasir, S. (2006). Al-Qaeda's clandestine courier service. Terrorism Focus, 3(7).
Akşen, H., & Koç, B. (2010). Terör olaylarına karışanların sosyo-ekonomik ve eğitim durumları ile bazı demografik değişkenler açısından değerlendirilmesi. Polis Akademisi Yayınları, 195-210.
Atıcı, B., & Gümüş, Ç. (2002). Bireylerin terör hareketlerine katılım durumları ile eğitim düzeyleri arasındaki ilişki. Türkiye'nin Güvenliği Sempozyumu, 17-19.
Atwan, A. B. (2019). Islamic state: The digital caliphate. University of California Press.
Bilhan, S. (1991). Eğitim felsefesi. Ankara Üniversitesi.
Bodo, L. (2018). Decentralised terrorism: The next big step for the so-called Islamic State (IS)? VOX-Pol Network of Excellence.
Brockhoff, S., Krieger, T., & Meierrieks, D. (2015). More education = less terrorism? Studying the complex relationship between terrorism and education.
Carley, K. M., Dombroski, M., Tsvetovat, M., Reminga, J., & Kamneva, N. (2003). Destabilizing dynamic covert networks. In Proceedings of the 8th international Command and Control Research and Technology Symposium (pp. 79-92). Washington DC: National Defense War College.
Castells, M. (2011). The rise of the network society. John Wiley & Sons.
Comfort, L. K., & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. Natural Hazards, 39, 309-327.
Conway, M. (2012). From al-Zarqawi to al-Awlaki: The emergence and development of an online radical milieu. CTX: Combating Terrorism Exchange, 2(4), 12-22.
Cruickshank, P., & Hage Ali, M. (2007). Abu Musab Al Suri: Architect of the new Al Qaeda. Studies in Conflict & Terrorism, 30(1), 1-14.
Yasin, Ç. A. M., & Coşkun, S. (2022). Küresel kamusal bir kötü: Terörizm. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 48, 56-66.
Dijk, J. Van. (2018). Ağ toplumu. (Ö. Sakin, Çev.). İstanbul: Epsilon Yayınevi.
Elahi, N. (2019). Terrorism in Pakistan: The Tehreek-e-Taliban Pakistan (TTP) and the challenge to security. Bloomsbury Publishing.
Gunaratna, R., & Iqbal, K. (2012). Pakistan: Terrorism ground zero. Reaktion Books.
Gunaratna, R., & Haynal, C. (2013). Current and emerging threats of homegrown terrorism: The case of the Boston bombings. Perspectives on Terrorism, 7(3), 44-63.
Hamm, M. S. (2004). Apocalyptic violence: The seduction of terrorist subcultures. Theoretical Criminology, 8(3), 323-339.
Hoffman, B. (2017). Inside terrorism. Columbia University Press.
Hoffman, B. (1982). Right-wing terrorism in Europe. Santa Monica, CA: Rand Corporation.
Hoffman, B., & Morrison-Taw, J. (2019). A strategic framework for countering terrorism. In European democracies against terrorism (pp. 3-29). Routledge.
Hülür Himmet, Y. C. (2016). Yeni medya, toplum ve iletişim biliminin dönüşümü. Ankara: Siyasal Kitapevi.
Kaplan, A. M., & Haenlein, M. (2016). Dünyanın bütün kullanıcıları birleşin. In H. Hülür & C. Yaşın (Eds.), Yeni medya kullanıcının yükselişi (pp. 352-372).
Karahisar, T. (2013). Sosyal medyanın psikolojik ve toplumsal yansımaları. In M. Kuyucu & T. Karahisar (Eds.), Yeni İletişim Teknolojileri ve Yeni Medya, 52, 113.
Kuyucu, M. (2013). Yeni iletişim aracı olarak sosyal medya ve sosyal ağlar üzerine bir güncelleme. Yeni İletişim Teknolojileri ve Yeni Medya, 114-151.
Landow, G. P. (1994). Hypertext: The convergence of contemporary critical theory and technology. Modern Philology, 92(2), 272.
Laqueur, W. (1999). The new terrorism: Fanaticism and the arms of mass destruction. Oxford University Press.
Levitt, M. (2015). How do ISIS terrorists finance their attacks. The Hill, 18.
Schaub, D. (2019). Economic globalization and transnational terrorism. Transnational Terrorism, 151.

Livingstone, S., & Lievrouw, L. A. (2002). Handbook of new media: Social shaping and consequences of ICTs. Handbook of New Media, 1-592.
Liptak, A. (2019). Sri Lanka restricts access to social media sites following terror attack. The Verge, 21.
Lombardi, M. (2015). IS 2.0 and beyond: The caliphate's communication project. In Twitter and Jihad: The communication strategy of ISIS (pp. 83-124). ISPI-Istituto per gli Studi di Politica Internazionale.
Macnair, L., & Frank, R. (2018). Changes and stabilities in the language of Islamic state magazines: A sentiment analysis. Dynamics of Asymmetric Conflict, 11(2), 109-120.
Manovich, L. (2002). The language of new media. MIT Press.
Monaco, L. (2017). Preventing the next attack: A strategy for the war on terrorism. Foreign Affairs, 96, 23.
Nohria, N., & Eccles, R. G. (Eds.). (1992). Networks and organizations: Structure, form, and action. Harvard Business Review Press.
Neumann, P., Winter, C., Meleagrou-Hitchens, A., Ranstorp, M., & Vidino, L. (2018). Die Rolle des Internets und sozialer Medien für Radikalisierung und Deradikalisierung (Vol. 10). DEU.
Neumann, P., & Stevens, T. (2009). Countering online radicalisation: A strategy for action. International Centre for the Study of Radicalization and Political Violence (ICRS).
Okur, M. R. (2013). Web 2.0 ve sonrası. In Yeni iletişim teknolojileri (Ankara: T.C. Anadolu Üniversitesi Yayını No:2925).
Özkök, E. (2019). Türkiye artık yüzde 99'u müslüman olan ülke değil. Hürriyet.
Pandian, S., Gomaa, O., & Ahmad Pazil, N. H. (2020). Socialisation and recruitment in Islamist movements: A comparison between the Muslim Brotherhood and Al-Qaeda. International Journal of Islamic Thought, 18, 110-120.
Plebani, A., & Maggiolini, P. M. L. C. (2015). The centrality of the enemy in al-Baghdadi's caliphate. In Twitter and jihad: The communication strategy of ISIS (pp. 27-48). Epoké.
Perliger, A. (2014). Terrorist networks 'productivity and durability: A comparative multi-level analysis. Perspectives on Terrorism, 8(4), 36-52.
Rauf, A. A. (2021). New moralities for new media? Assessing the role of social media in acts of terror and providing points of deliberation for business ethics. Journal of Business Ethics, 170(2), 229-251.
Schmid, A. P. (1999). Terrorism and the use of weapons of mass destruction: From where the risk? Terrorism and Political Violence, 11(4), 106-132.
Smith, M. L. R., & Jones, D. M. (2018). What Carl might have said about terrorism: How strategic theory can enlighten an essentially contested debate. Infinity Journal, 6(2), 30-35.
Soriano, M. R. T. (2008). Terrorism and the mass media after Al Qaeda: A change of course? Athena Intelligence Journal, 3(1), 1-20.
Speckhard, A., Shajkovci, A., Wooster, C., & Izadi, N. (2018). Engaging English speaking Facebook users in an anti-ISIS awareness campaign. Journal of Strategic Security, 11(3), 52-78.
Splittgerber, A., & Detmering, F. (2017). Germany's new hate speech act in force: What social network providers need to do now. Technology Law Dispatch.
Timisi, N. (2016). Dijital Kavramlar. In Olanaklar, Deneyimler. İstanbul: Kalkedon Yayınları.
Tu, A. T. (2007). Toxicological and chemical aspects of sarin terrorism in Japan in 1994 and 1995. Toxin Reviews, 26(3), 231-274.
Turkle, S. (1997). Life on the screen: Identity in the age of the internet. Literature and History, 6, 117-118.
Uğurlu, E. G. (2013). Tarih ve kavram olarak yeni iletişim teknolojileri. In T. Volkan Yüzer & M. E. Mutlu (Eds.), Yeni İletişim Teknolojileri (pp. 2-22). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
Varış, F., Gürkan, T., Gözütok, D., Gürbüztürk, O., & Babadoğan, C. (1991). Eğitim Bilimine Giriş. In F. Varış (Ed.), Sosyal Bilimler Dergisi. Eskişehir: Ankara Üniversitesi Eğitim Bilimleri Fakültesi.
Vittori, J. (2011). Terrorist financing and resourcing. Springer.
Weiss, C. (2016). Philippines-based jihadist groups pledge allegiance to the Islamic State. FDD, Long War Journal.
Weimann, G. (2004). www.terror.net: How modern terrorism uses the Internet (Vol. 31). United States Institute of Peace.
Williamson, H., Fay, S., & Miles-Johnson, T. (2019). Fear of terrorism: Media exposure and subjective fear of attack. Global Crime, 20(1), 1-25.
Yengin, D. (2014). Yeni medya ve dokunmatik toplum (2. Baskı). İstanbul: Derin Yayınları. PIAR'2022/9 (1).
Zeiger, S., & Gyte, J. (2020). Prevention of radicalization on social media and the internet. International Centre for Counter-Terrorism (ICCT).