Araştırma Makalesi / Research Article

TESAM Akademi Dergisi

Journal of TESAM Academy

ISSN 2148-2462 / E-ISSN 2458-9217

Integrating Analysis, Cyber Security, and Policy: Securing the Security Intelligence for Effective Counterterrorism in a Complex Digital Age

Analiz, Siber Güvenlik ve Politikanın Entegre Edilmesi: Karmaşık Dijital Çağda Etkili Terörle Mücadele İçin Güvenlik İstihbaratının Güvence Altına Alınması

Muhammet MAĞAT

Doktora Öğrencisi,
Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı.
muhammetmagat34@gmail.com
ORCID: 0000-0003-3237-2995

Bekir PARLAK

Prof. Dr.,
Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı.
bparlak21@gmail.com
ORCID : 0000-0001-8919-6481

Cilt / Issue: 13(1), 375-405
Geliş Tarihi: 09.01.2025
Kabul Tarihi: 25.04.2025

Atıf: Mağat, M. ve Parlak, B. (2026). An analysis on technological innovations, media and other security intelligence factors as new components of intellingece management in counterterroism. *Tesam Akademi Dergisi*, 13(1), 375-405. 10.30626/tesamakademi.1616362.

Abstract*

Intelligence is crucial for shaping both domestic and foreign policy, particularly in volatile regions with pressing security concerns. Objective analysis, free from political bias, is vital for accurate threat assessment and effective counter-terrorism strategies. This is especially important during crises, where understanding the nature of threats– whether from state or non-state actors – is essential for informing decisions on interventions, terrorism escalation, and terrorist profiling. A robust counter-terrorism strategy relies on strong "political security" and necessitates increased information sharing and cooperation on issues like terrorism, smuggling, and threats to national integrity. This strategy must adapt to the "technology factor", acknowledging how terrorist organizations exploit electronic platforms for everything from propaganda to attacks. This study focuses on "security intelligence" and its role in counterterrorism. Using a qualitative, explanatory-descriptive approach, it examines the intelligence analytical culture, the impact of technology, and the specific function of security intelligence in combating terrorism. It argues that prioritizing intelligence efforts targeting state and non-state actors supporting terrorism is crucial for developing effective counter-terrorism policies in today's interconnected world.

Keywords: Counterterrorism, Media, Technology, Security Intelligence, Analytical Culture.

* This study constitutes the expanded and revised version of the paper titled "Intelligence Management in the Fight Against Terrorism: Analysis, Technology, and Security Intelligence Factors," presented orally by Muhammet Mağat at the 19th International Congress of Social Sciences of the Turkic World held in Baku, Azerbaijan, on September 27–29, 2021.

The content of this journal is licensed under a Creative Commons Attribution-NonCommercialNoDerivatives 4.0 International License.

Öz**

İstihbarat, özellikle güvenlik kaygılarının yoğun olduğu istikrarsız bölgelerde hem iç hem de dış politikanın şekillendirilmesinde çok önemli bir rol oynar. Siyasi önyargılardan arındırılmış objektif analizler, doğru tehdit değerlendirmesi ve etkili terörle mücadele stratejileri için hayati önem taşır. Bu, özellikle kriz zamanlarında ister devlet ister devlet dışı aktörlerden kaynaklansın, tehditlerin doğasını anlamanın, müdahaleler, terörizmin tırmanması ve terörist profilleme konusundaki kararları bilgilendirmek için elzem olduğu durumlarda önemlidir. Güçlü bir terörle mücadele stratejisi, güçlü bir "politik güvenliğe" dayanır ve terörizm, kaçakçılık ve ulusal bütünlüğe yönelik tehditler gibi konularda artan bilgi paylaşımı ve iş birliğini gerektirir. Bu strateji, terör örgütlerinin elektronik platformları propagandadan saldırılara kadar her şey için nasıl kullandığını kabul ederek "teknoloji faktörüne" uyum sağlamalıdır. Bu çalışma, "güvenlik istihbaratına" ve terörle mücadeledeki rolüne odaklanmaktadır. Niteliksel, açıklayıcı-betimleyici bir yaklaşım kullanarak, istihbarat analitik kültürünü, teknolojinin etkisini ve güvenlik istihbaratının terörle mücadeledeki özel işlevini incelemektedir. Günümüzün birbirine bağlı dünyasında etkili terörle mücadele politikaları geliştirmek için devleti ve terörizmi destekleyen devlet dışı aktörleri hedef alan istihbarat çabalarına öncelik vermenin çok önemli olduğu savunulmaktadır.

Anahtar Kelimeler: Terörle Mücadele, Medya, Teknoloji, Güvenlik İstihbaratı, Analitik Kültür.

** Bu çalışma, 27–29 Eylül 2021 tarihleri arasındaBakü/Azerbaycan'da düzenlenen 19. UluslararasıTürk Dünyası Sosyal Bilimler Kongresi'ndeMuhammet Mağat tarafından sözlü olarak sunulan "Terörle Mücadelede İstihbarat Yönetimi: Analiz,Teknoloji ve Güvenlik İstihbaratı Faktörleri "başlıklı bildirinin, araştırma makalesi formatındagenişletilmiş ve revize edilmiş hâlini oluşturmaktadır.

Introduction

Terrorism is one of the most serious security threats facing the international community in the twenty-first century. Threatening the borders of states, the security of their citizens, and their way of life, terrorism is a complex and constantly evolving phenomenon. Terrorist organizations aim to create fear and chaos by using acts of violence driven by ideological motivations, political goals, or personal interests. Therefore, combating terrorism requires a multi-faceted approach supported not only by military and security measures but also by intelligence activities. Beyond the immediate physical damage and psychological terror wrought by their actions, terrorist organizations also wage a subtle, insidious war on societal trust, eroding the very fabric of communal resilience. By exploiting vulnerabilities in open societies, they seek to sow discord and suspicion, turning neighbour

against neighbour and fostering a climate where fear dictates daily life. This deliberate fracturing of social cohesion, often amplified by the rapid dissemination of misinformation online, presents a unique challenge to counter-terrorism efforts, demanding a strategic focus on building robust community networks and promoting media literacy alongside traditional security measures.

Intelligence plays a critical role in combating terrorism. Understanding the structure, tactics, funding sources, and targets of terrorist organizations is essential for preventing their actions and bringing terrorists to justice. Traditionally, intelligence was gathered through methods such as human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT). However, in the twenty-first century, technological advancements have fundamentally changed the methods of intelligence gathering and analysis. Tools such as artificial intelligence, big data analytics, social media monitoring, and cyber intelligence have the potential to increase the effectiveness of intelligence in combating terrorism. The proliferation of encrypted communication platforms and the decentralized nature of online radicalization have necessitated a paradigm shift in intelligence practices. Beyond simply collecting data, analysts must now navigate a complex digital landscape, discerning meaningful signals from a deluge of information. The ability to predict and pre-empt terrorist activities hinges on the development of sophisticated algorithms capable of identifying subtle patterns of behaviour, analysing vast datasets of online interactions, and discerning the often-blurred lines between legitimate discourse and the mobilization of violence. This fusion of traditional intelligence craft with cutting-edge computational power represents the frontier of counterterrorism, where the ability to anticipate and disrupt threats relies on the rapid and accurate interpretation of an ever-expanding digital footprint.

This study examines technological innovations, media, and other security intelligence factors as new components of intelligence management in combating terrorism. It focuses on how technology is used by terrorist organizations, how social media is used for terrorist propaganda and recruitment, and the importance of security intelligence. Technological advancements offer new opportunities for terrorist organizations while also creating new challenges. Terrorist organizations effectively use technology in their activities such as communication, propaganda, financing, and operational planning.

For example, encrypted messaging applications allow terrorists to communicate securely, while social media platforms are used for propaganda and recruitment. Additionally, cryptocurrencies enable terrorist organizations to diversify their funding sources and evade international sanctions.

The use of technology by terrorist organizations creates new challenges for intelligence agencies. Monitoring the encrypted communication channels used by terrorists, detecting propaganda activities on social media platforms, and tracking financial transactions made with cryptocurrencies require advanced technological tools and expertise. Therefore, intelligence agencies must closely follow technological developments and adapt to new technologies. Social media platforms have become a powerful tool for terrorist organizations for propaganda and recruitment. Terrorist organizations use social media platforms to spread their ideology, justify their actions, and recruit new members. Young people are exposed to the propaganda of terrorist organizations through social media platforms and face the risk of radicalization. The insidious nature of online radicalization lies not just in the overt dissemination of violent ideologies, but also in the subtle manipulation of algorithms and the creation of echo chambers. Terrorist groups exploit the personalized nature of social media, tailoring content to exploit existing vulnerabilities and biases within vulnerable individuals. By carefully curating their online presence, they create a sense of belonging and purpose, drawing in susceptible individuals who may feel marginalized or disenfranchised. This digital grooming process, often masked as innocuous online interaction, allows for the gradual indoctrination and radicalization of individuals, making it increasingly difficult for intelligence agencies to identify and intervene before a potential act of violence occurs. Therefore, counter-terrorism strategies must extend beyond simple content removal, focusing on disrupting the very mechanisms that facilitate this online radicalization process and fostering digital literacy among at-risk populations.

The use of social media platforms by terrorist organizations poses a significant challenge for intelligence agencies. Monitoring the activities of terrorists on social media platforms, detecting propaganda content, and identifying individuals at risk of radicalization require advanced social media monitoring tools and expertise. Therefore, intelligence agencies must cooperate with social media platforms and develop effective strategies against the propaganda activities of terrorist

organizations. Security intelligence plays a critical role in combating terrorism (Tiryaki & Özdal, 2020). Understanding the structure, tactics, funding sources, and targets of terrorist organizations is essential for preventing their actions and bringing terrorists to justice. Security intelligence is obtained through the analysis and evaluation of information gathered from various sources such as human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and open-source intelligence (OSINT).

The effectiveness of security intelligence depends on the analytical capacity of intelligence agencies. Intelligence agencies must accurately analyse the information gathered, anticipate the actions of terrorist organizations, and provide timely and actionable intelligence to decision-makers (Miller, 2022). Therefore, intelligence agencies need to strengthen their analytical capabilities and train qualified intelligence analysts. Technological advancements offer new opportunities for terrorist organizations while also creating new challenges. Therefore, the importance of intelligence activities in combating terrorism is increasing. To play an effective role in combating terrorism, intelligence agencies must closely follow technological developments, adapt to new technologies, and strengthen their analytical capabilities (Davis, 2021). Additionally, they should cooperate with social media platforms to develop effective strategies against the propaganda activities of terrorist organizations.

Beyond the sheer volume of data, the crucial challenge lies in discerning the signal from the noise, a task demanding not just technological prowess but also a deep understanding of cultural nuances, linguistic subtleties, and the evolving tactics of terrorist networks. This necessitates a shift from reactive data collection to proactive, predictive analysis, where intelligence agencies cultivate a holistic understanding of the threat landscape. The development of "cognitive security", which incorporates behavioural science and psychological profiling, becomes paramount in anticipating the intent behind seemingly innocuous online activities. This requires a new breed of intelligence analyst, one who can not only navigate the complexities of digital forensics and data science but also possess the critical thinking skills to connect disparate pieces of information, forming a coherent and actionable intelligence picture. This fusion of human expertise and advanced computational power is vital to pre-emptively disrupting terrorist plots before they materialize (Huang & Zhu, 2023).

Security intelligence plays a crucial role in counterterrorism. Intelligence agencies must accurately analyse gathered information, anticipate terrorist organizations' actions, and provide timely and actionable intelligence to decision-makers. Combating terrorism requires a multi-faceted approach supported not only by military and security measures but also by intelligence activities. By closely following technological advancements, strengthening their analytical capabilities, and effectively utilizing security intelligence, intelligence agencies can play a significant role in combating terrorism. However, the ethical dimensions of enhanced intelligence gathering cannot be overlooked. The delicate balance between security imperatives and the preservation of civil liberties presents a persistent challenge. The use of sophisticated surveillance technologies, predictive policing algorithms, and the collection of vast troves of personal data raises profound questions about privacy, due process, and the potential for abuse. Ensuring transparency, accountability, and robust legal frameworks are essential to maintain public trust and prevent the erosion of democratic values in the pursuit of counterterrorism. This necessitates a continuous dialogue between intelligence agencies, policymakers, and civil society to navigate the complex ethical terrain and establish clear guidelines for the responsible use of these powerful tools.

Challenges and Complexities in Modern Intelligence: Analysis, Policy and National Security

Intelligence has diverged significantly from its initially perceived meaning, particularly in Türkiye. As a crucial component in policy formulation for both domestic and foreign affairs of states, intelligence can encompass more diverse meanings in risky geographies. Security concerns have existed since the dawn of humanity. These concerns have been accompanied by the drive for freedom and the desire for prosperity. The nature of intelligence and the conduct of intelligence officers should not be predisposed or aligned with the statements that decision-makers wish to convey to the public. This same principle applies to crisis situations such as hot conflicts on the front lines or any proxy engagements. Specifically, in counterterrorism, intelligence is a "forecasting" element. In this regard, support can be drawn from the conceptual scope of "cultural intelligence". A threat assessment regarding whether threats to homeland security are under the patronage of another state or a non-state actor can be conducted in

this way. Evaluations regarding foreign interventions, the escalation of terrorism, and the neuro-political and psycho-political state of the terrorist can be obtained through this information.

Establishing a state of "unconcern" in counterterrorism, which is an irregular and complex conflict environment, is only possible with an effective "national security management philosophy" (Şengöz, 2019). In the historical transformation of security, the possibilities of comparing the profile of a group of bandits with that of terrorist organizations systematically supported by state or non-state actors are quite evident. In this context, fully identifying the external political and economic support of terrorism and combating it in the eyes of the international public through "hard diplomacy" or, if necessary, an "antagonist approach" can be considered the first step in counterterrorism. For this, intelligence activity against states or organizations that openly or covertly provide patronage to terrorism should primarily be strengthened at the "analysis level". The fact that these parties, especially when the end of a terrorist organization is near, bring up expressions such as "peace/resolution process" or "humanitarian situation" must be carefully monitored by security intelligence analysts. In this sense, along with expecting the effective role of foreign representations, centralizing counter-terrorism intelligence in a single centre, establishing specialized counter-terrorism analysis units at the "institute" level, and conducting effective threat assessments are crucial for achieving effective results by technological advances (Wall, 2025).

The foremost intelligence task is to collect intelligence—whether through technical intelligence (TECHINT) or human intelligence (HUMINT)—then analyse its meaning and bring human understanding to the collected data. At the beginning of each administration, senior officials work with national intelligence management to prepare a "threat assessment," a prioritized list of the most dangerous situations facing the country. Good analysis depends on bringing together the best possible minds to assess global events, drawing on a mixture of public information and stolen secrets (Johnson, 2007, p. 9). Additionally, the demand for timely, original, and even entertaining intelligence products is so great that the constant drumbeat of intelligence alerts and analytical output can take on a life of its own and create an impression of unwarranted certainty, threat, and urgency (Johnson, 2007, p. 32).

In an era of information overload, the critical challenge for intelligence agencies extends beyond simply acquiring data to effectively synthesizing and contextualizing it. The relentless pursuit of "actionable intelligence" can lead to a focus on immediate threats, potentially obscuring long-term strategic vulnerabilities. This necessitates a shift towards fostering a culture of "strategic foresight," where intelligence analysts are encouraged to explore alternative scenarios, challenge prevailing assumptions, and cultivate a deeper understanding of the complex interplay between geopolitical, economic, and social forces. Furthermore, the inherent subjectivity of human interpretation, coupled with the pressure to deliver rapid assessments, can lead to the amplification of biases and the creation of self-reinforcing narratives. Therefore, intelligence agencies must prioritize the development of rigorous analytical methodologies, promote intellectual diversity, and cultivate a culture of critical self-reflection to mitigate the risks of groupthink and ensure the production of objective and insightful intelligence products (Şeşen & Kuzucuoğlu, 2021, pp. 93-110).

Researchers have also turned to organizational behaviour for insights into the production of finished intelligence. For example, parochialism is endemic in intelligence production because the "need-to-know" principle governs individual analysts' access to information. However, organizations are jealous guardians of information, and bureaucratic rivalries or differences in standard operating procedures can impede, to some degree, the flow of information within organizations or across the intelligence community as a whole. Bureaucratic competition can also take on a life of its own; the pursuit of outmanoeuvring analysts from other organizations may take precedence over efforts to serve the needs of policymakers. Small group dynamics can also shape intelligence estimates: the well-known phenomenon of "groupthink" can occur among small teams of analysts and intelligence managers. Organizational affiliation also tends to complicate one's perceptions, and rare is the analyst or manager who advances a position that contradicts the interests of their own organization or career interests. Bureaucracy itself—hierarchy, specialization, centralization, routine, and secrecy—and the constant need to justify budgets and priorities, which creates an endless reporting requirement and innovative "metrics," all conspire to inhibit creative thinking and effective analysis (Johnson, 2007, p. 33).

The digital age has introduced a new layer of complexity to these

organizational challenges. The increasing reliance on automated data analysis and artificial intelligence, while promising greater efficiency, risks exacerbating existing biases and creating opaque decision-making processes. The "black box" nature of some algorithms can obscure the underlying assumptions and methodologies, making it difficult to challenge or scrutinize intelligence assessments. Moreover, the rapid proliferation of open-source intelligence (OSINT) and the blurring lines between public and classified information demand a re-evaluation of traditional "need-to-know" principles. The need for agile, interdisciplinary teams capable of navigating the dynamic information landscape necessitates breaking down traditional bureaucratic silos and fostering a culture of collaboration and information sharing. This requires not only technological adaptation but also a fundamental shift in organizational culture, prioritizing transparency, intellectual humility, and a commitment to continuous learning in the face of evolving threats.

An important level of analysis, the intelligence-policy nexus, focuses on how the relationships between intelligence professionals and policymakers shape dissemination and the response to finished intelligence and warning. Various problems can arise to disrupt the relationships between the intelligence and policymaking communities. The best-known pathology, politicization, occurs when policymakers exert overt or covert pressure on intelligence analysts and managers to produce intelligence estimates that support existing political preferences or policies. Although there is no consensus on what constitutes best practices when it comes to intelligence-policy interaction, two schools of thought compete as a guide to the relationships between policymakers and the intelligence community. One school of thought, most closely associated with the work of Sherman Kent, focuses on ensuring the independence of intelligence analysts. Kent's thinking, which shaped the evolution of the U.S. intelligence community, identifies the importance of political and policy neutrality in producing finished intelligence. The other school, most closely associated with reforms initiated by then-Director of Central Intelligence Robert M. Gates in the mid-1980s, focuses on producing "actionable" intelligence, information that can be used immediately and directly by policymakers. To produce actionable intelligence, analysts must maintain close working relationships with policymakers, literally looking into policymakers' inboxes, and

ensuring that finished intelligence addresses the important policy issues of the day (Wirtz, 2007).

With the growth of the modern "national security state," coupled with technological advancements in intelligence gathering and analysis for national security purposes, traditional legal criteria such as the harm test and the public interest test are becoming less effective in limiting the scope of national security for the protection of state secrets. These changes are also diminishing the role that the judiciary or independent public oversight bodies can play, even in liberal democracies where an ideological commitment to the protection of individual liberties is supposed to underpin political and legal systems (Nashu, 2015). The expanding digital frontier, with its inherent challenges to jurisdictional boundaries and the anonymity it affords, further complicates the application of traditional legal safeguards. The very nature of cyber threats, often originating from non-state actors operating across international borders, necessitates a re-evaluation of sovereignty and the scope of state authority. This creates a tension where the urgency to protect critical infrastructure and national security interests can lead to an expansion of surveillance powers and a blurring of the lines between domestic and foreign intelligence gathering. Consequently, the erosion of traditional legal constraints, coupled with the opacity of advanced technological capabilities, risks creating a "surveillance state" where individual liberties are increasingly subordinated to the perceived imperatives of national security, demanding a renewed focus on international legal frameworks and ethical guidelines to ensure accountability and prevent unchecked expansion of state power (Miller & Bossomaier, 2024, pp. 55-95).

Securing the Digital Frontier: Cyber Warfare and Effective Countermeasures

One of the important issues in the context of counter-terrorism intelligence is the "technology factor" in the actions of terrorist organizations. In an age where borders are becoming electronic, terrorist organizations will not be slow to take advantage of this opportunity. Developing an extremely complex combat concept, from propaganda activities on social media to drone technology-based attacks, necessitates a policy system. Especially the social media factor plays a critical role in the realization of conditions such as propaganda, communication, recruitment, and financial support

(Darıcılı, 2020). Political and diplomatic engagement can also be carried out in these channels by acting with the "integrated society" sign. Ultimately, the common impact that terrorist organizations want to leave on their targets is the formation of a profile of pain, disrepute, and unreliability. The technology falling into the wrong hands, as mentioned above, necessitates the increase of policy options and the use of the incremental public policy model. Incremental public policy is a method of reproduction by formulating new policies by performing policy analysis for the current situation, taking into account past practices in a policy area (Demir, 2020).

The rapid convergence of emerging technologies, such as artificial intelligence, autonomous weapons systems, and synthetic biology, introduces an unprecedented level of complexity to the counter-terrorism landscape. Terrorist organizations, adept at exploiting technological vulnerabilities, are increasingly capable of developing and deploying sophisticated, asymmetric attack vectors. This necessitates a proactive, anticipatory approach to intelligence, one that goes beyond simply reacting to current threats and instead focuses on predicting and mitigating future technological risks. The incremental public policy model, while valuable for adapting to known challenges, may prove insufficient in addressing the disruptive potential of these emerging technologies. Therefore, a more dynamic and adaptive policy framework, incorporating elements of horizon scanning, scenario planning, and collaborative risk assessment, is essential to ensure that counter-terrorism strategies remain relevant and effective in the face of rapidly evolving technological threats (Poyraz, 2024, pp. 887-894).

Relating the rapid technological evolution and its impact on terrorism directly to intelligence necessitates a fundamental re-evaluation of intelligence methodologies. The "technology factor" doesn't just demand new tools for intelligence gathering, but also a complete overhaul of analytical frameworks. Intelligence agencies must develop the capacity to anticipate the misuse of emerging technologies by terrorist groups, requiring a shift from reactive to predictive intelligence. This includes cultivating expertise in fields like AI ethics, cyber warfare, and biosecurity, to understand the potential attack vectors. Furthermore, the sheer volume of data generated by these technologies requires AI-driven analysis, but with careful oversight to prevent algorithmic bias. Intelligence analysts must also become adept at understanding the "digital battlespace", comprehending the

psychological and sociological impacts of online radicalization and the use of social media as a weapon. The incremental public policy model, when applied to intelligence, means continuously adapting intelligence operations to the changing technological landscape, incorporating lessons learned from past failures, and proactively addressing new threats. This requires a collaborative approach, sharing intelligence across agencies and international partners, to build a comprehensive understanding of the evolving threat landscape and develop effective countermeasures (Lahmann, 2022).

The symbiotic relationship between combating terrorism and intelligence has been fundamentally reshaped by the digital frontier and cyberspace. The traditional intelligence cycle, focused on physical surveillance and human sources, must now contend with the ephemeral and decentralized nature of online radicalization, encrypted communications, and the weaponization of social media. Analytical capabilities must evolve to parse vast datasets, identifying subtle patterns of radicalization and predicting potential attack vectors within the digital domain. This demands a nuanced understanding of online subcultures, the psychology of digital manipulation, and the evolving tactics of cyber-enabled terrorism. Intelligence agencies must not only collect data but also develop sophisticated algorithms to discern signal from noise, anticipate emerging threats, and provide actionable intelligence to policymakers in near real-time. Moreover, the inherent anonymity and transnational nature of cyberspace necessitate enhanced international cooperation and intelligence sharing, alongside the development of robust legal frameworks to govern surveillance and counter-terrorism operations in the digital age (Martin, 2016).

The image of a state or government has been a matter of importance since the very inception of politics. Having a good image and prestige is crucial for the continuity of power. Honest and transparent communication regarding the reasons, processes, and consequences of implemented policies is a fundamental requirement for the desired support and prestige. Today, every commercial, political, national, and international actor, from civil society organizations to companies, from Haiti to China, is striving to improve in this regard. Recognizing that every step taken in politics cannot be flawless and entirely well-intentioned, all actors in the game are at least obligated to explain the reasons behind their actions and convince the public. Accordingly, radio, TV, newspapers, the internet, and, more recently, the rising social

media, are fundamental avenues for the relevant actors to explain all their actions, whether justified or not, to the public. This situation, in parallel with developing technology, has led to the transfer of conflicts of interest to cyberspace and the reflection of coordinated perception management efforts onto digital platforms and, recently, onto social media (Bural, 2021).

The digital frontier, particularly cyberspace and social media, has fundamentally altered the relationship between combating terrorism and intelligence by transforming the battleground from physical space to the realm of perception and information warfare (Prier, 2017). Intelligence agencies must now grapple with the weaponization of a state or government's image, recognizing that terrorist organizations and state actors alike leverage digital platforms to manipulate public opinion, recruit followers, and undermine trust in legitimate institutions. The ability to conduct effective counter-terrorism operations hinges not only on gathering actionable intelligence about physical threats but also on understanding and countering the coordinated perception management efforts that proliferate online. This requires a shift from traditional intelligence analysis to a multidisciplinary approach incorporating social psychology, media studies, and computational propaganda analysis. Intelligence agencies must develop the capability to detect and disrupt the spread of disinformation and extremist narratives, while simultaneously fostering transparent communication and building resilience against digital manipulation. The challenge lies in navigating the complex interplay between security imperatives and the preservation of free speech, ensuring that counter-terrorism efforts do not inadvertently erode the very democratic values they seek to protect.

The 1999 NATO intervention in Kosovo, including the bombing of specific targets in Serbia, has gone down in history as one of the first international events where internet propaganda was utilized. The massacres perpetrated by the aggressive Serbian forces under Milošević were communicated to all interested parties through various propaganda activities by Western media outlets such as CNN, official national channels, and civil society organizations to influence international public opinion. It is possible to speak of a multifaceted flow of information and provocative content here. Accordingly, many television and internet sources, primarily in the US and the EU, made efforts to inform the Serbian people about the racist and brutal regime's

crimes against humanity, while many Kosovars strove to make their hardships known to the world. The bombing of the Television Tower, the official propaganda tool, being among the primary targets of NATO in Serbia, yet the fact that public internet access was not prevented in Belgrade and surrounding areas, was a step taken to inform the ordinary people and, presumably, to reveal the justified reasons for the intervention and highlight the correct narrative. Because, within the framework of the Responsibility to Protect (R2P) principle, transparency is vital for ensuring that the intervention will bring more benefit than harm, that there was no other solution that could be implemented (last resort), and most importantly, that it is conducted within the common view of multiple parties, in accordance with the just war doctrine. The Kosovo War emerges as a new arena and battleground where ideas, accurate or misleading news, and evidence clashed in cyberspace. In the following years, both the technological developments in cyber-attacks and cyber security systems, and the entry of social media, have gradually increased the importance of cyberspace in politics. Especially after the advent of social media into our lives, political activity in the cyber domain has intensified.

In this context, with Denning's (2001) expression, the phenomena of hacktivism and cyberterrorism have emerged, with hacktivism referring to the application of certain illegal techniques on the internet for the purpose of activism. Firstly, if we need to delve deeper into the definition of activism, what is meant here involves organizing various promotion and support campaigns on the internet within a specific political agenda, without engaging in any harmful activity. Secondly, if we focus on the term hacktivism, which is formed by the combination of activism and hack: it refers to the use of various hacking techniques to disrupt the normal online activities of the targeted state, NGO, institution, organization, or company. The activities in question include virtual sit-ins and blockades, email bombing, intrusion attempts, computer viruses, and worm applications. The main target of those other than intrusion attempts is to disrupt the system's operation by creating congestion on the internet network. To give an example: On December 21, 1995, in France, a group calling themselves the Strano Network carried out a one-hour cyber sit-in on the state websites of relevant government institutions to protest the government's agenda regarding social policies and nuclear energy. Again, in 1998, a group calling themselves The Electronic Disturbance Theater (EDT), in

collaboration with the Mexican Zappatistas group, organized cyber sit-ins and blockades against a series of sites, such as the personal website of the then-Mexican President Zedillo, the official website of the then-US President Clinton, the Pentagon's website, and the official website of the Frankfurt Stock Exchange (Ronfeldt; Arquilla; Fuller, 1998).

Similarly, the group's FoodNet software was made available to some animal rights activists, and in January 1999, cyber sit-ins involving approximately 800 protesters from more than 12 countries were carried out, targeting the websites of various institutions in Sweden (ECD, 1998). Furthermore, with some intrusion attempts, relevant groups can attract the necessary audience and get what they want. For example, on October 16, 1989, an anti-nuclear power group, using a computer worm called WANK, infiltrated NASA's (National Aeronautics and Space Administration) SPAN network and damaged the Galileo spacecraft, which was being prepared to go to Jupiter and was filled with radioactive plutonium. John McMahon, NASA's chief of protocol, stated that this action cost them approximately half a million dollars and a great deal of time (Bridis, 1999). Also, in September 1998, a Portuguese hacker group accessed forty internet servers in Indonesia and published the slogan "Free East Timor" in large and bold black letters on the relevant sites, also sharing links to websites that allegedly contained evidence of human rights abuses in the country at that time. To give an example from closer geographies, in the 1990s, a 14-year-old Israeli citizen named Nir Zigdon, after government officials "hesitated" to assassinate Saddam Hussein, thinking that he could at least "destroy" his personal website, infiltrated an internet server of a Gulf country through special software. From there, he sent an email to Saddam Hussein, posing as a young Palestinian who was a big fan of him, offering to erase websites in Israel with a new computer virus he had developed, thus crashing government computers (Gross, 1999).

Finally, regarding the issue of cyberterrorism, unlike the other two categories, it refers to various cyberattacks that directly target loss of life and injuries, as well as economic losses. For example, the possibility of hacking an aircraft system or an air traffic controller's computer and causing two planes to collide falls within the scope of cyberterrorism. On the other hand, the line between internet activism, hacktivism, and cyberterrorism is quite thin. As in the case of the NASA Galileo spacecraft hacking incident, the distinguishing factor of physical and economic damage can also be possible with the other options.

On the other hand, as the use of social media has become a routine part of our lives, many parties, from civil elements and organizations pursuing various public interest goals ranging from environmental issues to gender equality, to radical Islamist terrorists, are increasing their effectiveness by taking advantage of the cross-border, fast, cheap, and even anonymous usability features of this technology. With the widespread global use of applications such as Facebook, X(Twitter), Instagram, TikTok, YouTube, and even WhatsApp, cyberspace and the physical world have become virtually intertwined, and a parallelism has emerged between individuals' behaviours in both planes. Osama Bin Laden was the first to utilize the internet for terrorist purposes. In 2005, Ayman al-Zawahiri, the leader of the organization, declared that they were in a war more than half of which continued in the media, and that they were fighting within a race that continued in the hearts and minds of the Ummah (Liang, 2015). Today, many activities, from agendas for social benefit to terrorist recruitment, are carried out online.

Terrorist organizations aim to attract attention, gain legitimacy by acquiring supporters, spread fear and anxiety throughout society, cause emotional collapse, and ultimately destabilize the state, thus achieving military and political gains (Kartal, 2014, p.58). Many active terrorist organizations, such as ISIS, Boko Haram, and PKK/YPG, have various public relations, press and media, and, more recently, propaganda strategies focused on social media and digital platforms developed in this vein. In essence, although various media propaganda efforts have been carried out since the 1980s for the spread of the concept of Jihad based on radical Islam, it is possible to say that the use of social media and the internet has elevated the situation to a higher level. For example, ISIS began its clear and concrete propaganda activities with the magazine Dabiq, published in 2014 and aimed at international followers. Here, the "martyrdom" of the killed terrorists, the aid provided to the women and children left behind, and the richness of the schools and other social opportunities built are described (Choi, 2018).

On the cover of the second issue of the same magazine, in an Armageddon-themed issue featuring Noah's Ark, the "ISIS Caliphate" was portrayed as the ship that would save humanity from the apocalypse. In the third issue, an appeal was made to sympathizers living in Western countries to "migrate" to the regions captured by

ISIS "before the doors close". In this way, it tries to attract more people by publicizing its social opportunities and state-like perspective, thereby increasing its prestige. ISIS also has a media wing called The Zora Foundation to gain female supporters (Liang, 2015).

In the following period, ISIS and Al-Qaeda shifted the intensity of their activities to cyberspace. From this point of departure, more propaganda activities were undertaken, especially through digital platforms such as YouTube and social media applications such as X(Twitter). The online activities of these groups are based on recruiting supporters, increasing their financial resources through donations, and putting pressure on governments by making publications that will increase fear and instability in society, rather than cyberattacks. While ISIS actively uses YouTube and X(Twitter), Al-Qaeda's cyberterrorism activities are primarily focused on X(Twitter) propaganda. For example, ISIS has an official X(Twitter) page called Al-Furqan and many auxiliary pages that retweet the content published here, allowing more people to see it. At this point, the fact that the relevant accounts can operate separately and as if they were real individuals is again realized by taking advantage of the loopholes in the X(Twitter) algorithm. According to 2014 data, the Al-Furqan page has 284 million followers, and 500 million daily tweets published in 35 languages. In addition, there is the Al-Battar media group, with around 32,000 followers, and the Al-Hayat Media Center, which are affiliated with the organization. These also ensure that the organization's content is translated into various world languages and accessed through traditional media channels. To elaborate, Al-Hayat Media has content in the form of "mujahedeen tweets" describing the daily lives of the organization's members in the "battlefield" (Liang, 2015).

On connected social media accounts, content aimed at female users, such as childcare and elderly care advice, recipes, suggestions on how to please their "jihadi" husbands, videos of kittens and happy family settings, and even educational materials on the use of weapons are also shared. On the other hand, in addition to the goal of increasing the organic follower count of the relevant pages, the goal of reaching more people with the relevant posts is also pursued by preparing specific special hashtags. To elaborate, during the 2014 FIFA World Cup finals held in Brazil, they created hashtags using trending topics such as "#Brazil_2014" and increased the viewership of their posts. In addition, additional hashtags such as "#AllEyesOnISIS" and

"#CalamityWillBefallUS" were also used in these posts. These shares and tweets were retweeted so frequently that these "Twitter bombs" brought the organization's shares to the list of the most talked about topics in the world.

By taking advantage of the somewhat anonymous structure of social media and the weak links in the algorithms designed by the relevant service providers, terrorist organizations have gained a more effective and easy-to-use way to achieve their goals. For example, while ISIS guaranteed economic sustainability in the territories it seized with the oil reserves it acquired, it also recruited approximately 18,000 people from about 90 countries with its ongoing social media propaganda. Similarly, the Al-Shabaab organization continues to follow the same steps. Again, radical Islamist and separatist terrorist organizations operating in Nigeria use the internet for propaganda at a rate of 42%, for observation at a rate of 26%, for communication aimed at recruiting people (which is also a type of propaganda) at a rate of 17%, for generating additional income at a rate of 10%, and only at a rate of 5% for committing crimes (Ogunlana, 2019).

To give a more recent example from Türkiye, the PKK/YPG, like its Arab counterparts, also attaches great importance to both printed and digital media channels and social media propaganda. For example, it operates websites such as "https://www.rojaciwan.eu" and "http://www.hawarnews.com/" publishing in Turkish, Kurdish, Arabic, and English, and "https://rojnews.news/" publishing in Russian, German, and Spanish. Similar to ISIS's strategy, there is a video sharing site, "http://gerilatv.com/", depicting the supposed daily lives of guerrillas, and a virtual magazine called "http://www.komunar.net/". In addition to these, there are countless terrorist blogs and forum sites, such as "ypgnews.blogspot.com/", which describe themselves as "virtual guerrillas of the media". Furthermore, especially in line with the foreign policy of some Western allied states, instant images of the operations supposedly launched against the spread of ISIS in Syria and Iraq are shared on related YouTube accounts.

Again, during Türkiye's legitimate military operations such as Operation Euphrates Shield (2016), Operation Olive Branch (2018), Operation Peace Spring (2019), and Operation Spring Shield (2020), which it launched in accordance with Article 51 of the UN Charter to ensure its border security, the organization and its sympathizers

carried out various hashtag campaigns to spread lies such as civilians being targeted in the relevant regions and that this was a "genocide" rather than a counter-terrorism operation. In these posts, English hashtags were used together referring to the Armenian Genocide lie and disputes regarding the continental shelf in the Aegean, claiming that Türkiye committed Greek and even Syriac genocides.

With this method, the organization aims to put Türkiye in a difficult position with the manipulation of "they massacred Armenians and Syriacs in the past, now they are massacring us". When we also consider that during Operation Spring Shield, US President Joe Biden, without basing it on any historical data and beyond his authority, recognized the Armenian Genocide lie for political ambitions, the intention of these actions will be better understood. To give another example, during Operation Olive Branch, Julian Röpcke, a reporter for the German newspaper Bild, made explanatory tweets about the disinformation and manipulative posts of the PKK/YPG terrorist organization. To mention a few of these, Röpcke announced the propaganda war is heating up in Syria, 3 photos not belonging to Afrin and on February 7, 2018, that photos of children left among the rubble after Israel's bombardment in Palestine were montaged and false news and posts were made that the civilian population in Syria was targeted (Toktay, 2019).

What Can Be Done Against Cyberterrorism?

Rather than the technical aspect of cybersecurity, terrorist organizations have focused on the social and provocative side, turning to "social media propaganda". This plan for provocation and disinformation has a structure that spreads quickly and uncontrollably, like wildfire, to very large segments of the population, but will not cause lasting damage if a smart crisis management strategy is implemented. However, in addition to the observation and tracking operations to be undertaken by intelligence agencies, all steps to be taken by institutions and organizations related to public diplomacy, public relations, and foreign policy must be carried out in a credible manner, in accordance with the civil and anonymous structure of social media. Otherwise, all shares made run the risk of being labelled as "partisan" or, as Russia is most often accused of today, "troll" and losing their effectiveness.

If we examine academic sources at this point, according to Cohen

and Felson (1979), 4D and R, with their English abbreviations, are vital for ensuring cybersecurity (Cohen & Felson, 1979). These are: Detention, Deterrence, Defence, Defeat, and Resilience. If we first focus on Detention: If we need to focus on Deterrence, what is important here is predicting hostile behaviour, if necessary, denying the existing damage, hiding the vulnerability from the public, and implementing punishment. The main goal at this point is to instil the belief that the effort spent by the attackers in a similar action will not be worth it, that the desired damage can never be inflicted, so to speak, "the stone thrown will not be worth the frog startled." Exhibiting a strong stance and pursuing a good propaganda program will be beneficial here. The attacks carried out should not set a precedent. On the other hand, just like in the distinction between symmetric and asymmetric warfare, preventing non-state actors and the deterrence methods that can be applied against them are quite problematic. The ambiguity created by cyberspace makes it difficult to perceive who might be behind the attacks and therefore prevents the implementation of a quick and effective counter-attack policy. In this case, the only advantage that states have is that the cyber-attack capabilities of individual or non-state actors are still not at a sufficient level.

A similar situation is the relatively uncontrolled structure of cyberspace, which allows attacks to be carried out from international and foreign internet networks beyond political borders. In this context, international cooperation against cyber-attacks is of vital importance. In ensuring cybersecurity in the international arena, in addition to making legal regulations and information transfer, it would also be beneficial to cooperate with multinational companies in the production of technical devices such as network and operator services, mobile phones, and computers, and to work on a more "transparent production system" for the safety of users. But unfortunately, there is no mutual trust at this point. For example, the Cambridge Analytica scandal occurred on March 17, 2018. According to this, it refers to the modelling of the behaviour style of approximately eighty million users using a method called psychographics, based on the information users gave to Facebook and the results of the personality test created by Aleksandr Kogan, a lecturer at Cambridge University, and its use by those involved in critical events such as BREXIT and the 2016 American Presidential Elections (Hinds, Williams, & Joinson, 2020).

The key here is Facebook's algorithm showing similar posts in the news

feed according to users' past likes, creating a special parallel reality universe for that user, and influencing decision-making processes. After these events, the Federal Trade Commission imposed a record fine of 5 billion dollars on Facebook. However, the spread of fake news continues today on applications such as Facebook and X(Twitter). The tradition of prioritizing news feed and homepage posts according to likes continues. In this way, desired views become more visible, and people are tried to be brought closer to this view. Contrary views are marginalized. There is also no data to suggest that this situation is not or will not be used in line with the foreign policy interests of any country. In fact, following US President Biden's statements, the relevant account was immediately closed by the service provider after the sentence "The Armenian Genocide is an Imperialist lie" was uttered in a broadcast on the YouTube channel of the Youth Branches of the Homeland Party. Again, after MHP leader Devlet Bahçeli tweeted that the so-called Armenian Genocide claims were a lie, his personal account was closed by the service provider. Although it was announced after the 2018 scandal that accounts making violent, sexually explicit, insulting, etc. posts and comments would be closed upon complaint (the phrase "protect our community" is included), the misinformative content that Kim Kardashian made from her Instagram account was not removed from the site and the account was not closed despite the complaints of thousands of Turkish users.

In sum up, the fact that service providers such as both X(Twitter) and WhatsApp have avoided opening representative offices in our country for a long time may also indicate that they want to take advantage of the situation where the law cannot be applied to foreign-based companies. All these examples show us that "some states may want to take advantage of the greyness of social media", that the relevant platforms may turn into a new area of legitimacy war, and that cooperation regarding the solution of the problem is not very possible. In addition to increasing technical competencies, effective crisis management and political communication strategy are essential for every state.

Securing the Security Intelligence in Counterterrorism: Bridging the Gap Between Information Gathering and Effective Policy Formulation

A point to be emphasized in counterterrorism is "security intelligence" and "securing intelligence", which is a specialized intelligence field

exclusive to counterterrorism. In Türkiye, there was a "Security Intelligence Directorate" unit within the National Intelligence Organization (MİT). As stated on the institution's website, this unit was responsible for collecting security intelligence against threats to Türkiye's national power, primarily terrorist organizations and terrorist activities. The intelligence collected by the Directorate at home and abroad is used to take security measures and eliminate the threat. Today, this unit replaced its name as "Counterterrorism" in the context of duty-case (MİT, 2021). Security intelligence can mean more than just an information product. It can also mean a process. While it is easy enough to state the basic purpose of intelligence (providing information to policymakers), the difficulty of collecting, evaluating, and providing useful insights to decision-makers is a complex issue (Johnson, 2018). In these contexts, the Turkish intelligence community is also expected to be in a school/institute format that works with an analytical culture, in addition to its purely operational capabilities. Within this framework, retired professionals should not refrain from transferring their exclusive experience under the pretext of "state discipline" or "state secret". In other words, to put it precisely, intelligence in general is no longer something that needs to be hidden. Almost everything is in open-source format. The concept of state secret seems to mean very little. Today, there are manifestly "national security interests" (Kitler, 2021, p. 41). In such an environment, what is important is to compile and collect information from open sources and "produce analysis". If an operational behaviour needs to be developed, its foundation should be the analyses produced. A sword not based on the pen runs a high risk of bringing oppression or failure. It can be understood from this that the work of analysis does not seem easy either.

The transition from a "Security Intelligence Directorate" to a "Counterterrorism" unit within MİT reflects a broader shift in the intelligence landscape, where the focus has moved from merely gathering information to producing actionable analysis within a rapidly evolving digital environment. This necessitates a paradigm shift from a purely operational model to one that emphasizes analytical rigor and the integration of open-source intelligence. The challenge lies not in hoarding information, which is increasingly accessible, but in developing the capacity to synthesize disparate data points, identify emerging threats, and provide timely, contextually relevant intelligence to policymakers. This requires cultivating a culture of

intellectual curiosity, fostering collaboration between analysts and operators, and creating a framework for knowledge transfer, including the valuable insights of retired professionals. The "pen" of analytical prowess must guide the "sword" of operational action, ensuring that counterterrorism strategies are grounded in sound intelligence assessments, rather than reactive responses to perceived threats. Furthermore, the emphasis must be placed on developing robust analytical methodologies that can discern patterns within the noise of the digital sphere and anticipate the evolving tactics of terrorist organizations in the age of information warfare.

National systems need to be examined in terms of security intelligence networks that include foreign, domestic, and police systems across the public and private sectors. The fact that in many areas, especially the Middle East and Africa, there is no "definitive working unit" for the state's intelligence activities – it could be a tribe, clan, warlord, or gang – adds extra weight to this (Gill, 2007, p. 83). The Intelligence Community is relatively small, highly selective, and largely shielded from public scrutiny. For its practitioners, intelligence work is a cognitively demanding and high-stakes profession that can lead to public policy that either strengthens the nation or puts it at greater risk. Because the consequences of failure are so great, intelligence professionals constantly feel significant internal and external pressure to avoid it. One consequence of this pressure is a long-standing bureaucratic resistance to implementing a systematic program to improve analytical performance (Johnston, 2005).

The increasing interconnectedness of global threats, particularly those originating from non-state actors operating in regions with fragmented or non-existent state intelligence structures, necessitates a paradigm shift towards building agile and adaptive security intelligence networks. This demands a move beyond traditional, siloed national systems to foster robust information sharing and collaboration across public and private sectors, as well as with international partners. The challenge lies in establishing trust and interoperability among diverse entities, including those operating in complex and volatile environments where traditional state actors may be marginalized. Furthermore, the inherent pressure to avoid intelligence failures, coupled with bureaucratic inertia, can hinder the adoption of innovative analytical methodologies and the integration of emerging technologies. To mitigate this risk, intelligence agencies must prioritize the cultivation of a culture that

values critical thinking, embraces diverse perspectives, and encourages continuous learning. This includes investing in training programs that equip analysts with the skills necessary to navigate the complexities of the digital age, while also fostering a collaborative environment that promotes open communication and knowledge sharing (Elshimi, 2018).

Intelligence in counterterrorism concerns the national security policy system with an inherent analytical culture. The primary issue that decision-makers or statesmen need to be convinced of is that intelligence is a methodological collection and analysis activity in a separate category from mere espionage (Yılmaz, 2018, p. 29). A well-organized intelligence system working with an integrated public administration approach requires warning intelligence (Grabo, 2010), comprehensive consultation, and an agile government with a swift decision-making mechanism and process within the bureaucracy (Mergel, Ganapati, & Whitford, 2020). In this vein, policy-oriented intelligence production is important. When only military intelligence methods are used in counterterrorism, "the work of analysis" can be forgotten. Counter-terrorism is a matter of state policy, and an action plan is implemented with a selected set of policies.

The imperative for effective counterterrorism intelligence extends beyond mere information gathering to encompass the development of a strategic, policy-driven analytical framework that permeates the entire national security apparatus. This necessitates a fundamental shift away from viewing intelligence as solely a covert, espionage-driven endeavour, and towards recognizing it as a rigorous, methodological process that informs and shapes comprehensive national policy. The creation of a truly integrated public administration approach requires not only robust warning intelligence systems but also the cultivation of a collaborative environment where diverse perspectives and expertise are brought to bear on complex security challenges. Moreover, the agility and responsiveness of governmental decision-making mechanisms are paramount, enabling swift and decisive action in the face of rapidly evolving threats. The tendency to rely solely on military intelligence methods risks neglecting the crucial role of in-depth analysis, which is essential for understanding the root causes of terrorism, anticipating future threats, and developing effective, long-term counterterrorism strategies. The development of a holistic counterterrorism policy, therefore, demands an intelligence system

that is deeply integrated into the policymaking process, providing nuanced insights and strategic guidance to inform a multifaceted and sustainable approach.

Accordingly, the intelligence serving the purpose of these policies can fulfil the function of a "beacon" or "shield" for the state. If effective results are desired in counterterrorism, it is a priority to act in a policy-oriented manner without politicizing the intelligence community and to build a "culture of information sharing". In national security community regimes, "policy analysis" based on these priorities is considered a prerequisite for sustainable development. Ensuring a "political security" environment, which can be considered the most important of the security sectors, is based on an effective counter-terrorism concept. For this, instead of being limited and restricted; problems such as terrorism, international smuggling, and threats to nation-state integrity require strengthening high-level information sharing and cooperation (Mağat, 2020).

Conclusion

Counterterrorism is one of the most complex and challenging security issues of this century. The transnational nature of terrorism, its constantly evolving tactics, and ideological motivations pose a serious threat to the international community. To combat this threat effectively, security forces and intelligence agencies need to adopt a proactive and adaptable approach. Beyond the reactive measures often necessitated by immediate threats, a truly effective counterterrorism strategy must cultivate a deep understanding of the socio-political ecosystems that breed radicalization. This involves nuanced analysis of grievances, power dynamics, and information landscapes within vulnerable communities, coupled with investments in fostering resilience and inclusive governance. Only by pre-empting the seeds of extremism, rather than merely pruning its violent manifestations, can we hope to construct a sustainable framework for global security.

It is a fact that technological advancements have revolutionized intelligence gathering and analysis methods. Tools such as artificial intelligence, big data analytics, social media monitoring, and cyber intelligence offer significant opportunities to understand the structure, tactics, and goals of terrorist organizations, prevent their actions, and bring terrorists to justice. However, it should not be forgotten that

these technologies can also be used by terrorist organizations and can create new challenges. While the allure of technological supremacy in the intelligence domain is undeniable, a critical ethical dimension must temper its application. The very algorithms designed to predict and pre-empt terrorist actions can, if unchecked, perpetuate biases, erode privacy, and create a surveillance state that undermines the very freedoms it purports to protect. Furthermore, the digital battleground necessitates a paradigm shift in security thinking, moving beyond mere data acquisition to cultivating human-machine symbiosis that prioritizes critical thinking and contextual awareness, ensuring that technological tools augment, rather than replace, the essential human element in intelligence work.

For example, encrypted messaging applications make it easier for terrorists to communicate securely, while social media platforms are used for propaganda and recruitment purposes. Cryptocurrencies allow terrorist organizations to diversify their funding sources and evade international sanctions. Therefore, intelligence agencies need to closely follow technological developments, adapt to new technologies, and develop strategies to neutralize the use of technology by terrorist organizations.

Social media has become a powerful propaganda and recruitment tool for terrorist organizations. Terrorist organizations use social media platforms to spread their ideology, legitimize their actions, and gain new members. Young people are exposed to the propaganda of terrorist organizations through social media platforms and face the risk of radicalization. Therefore, intelligence agencies need to cooperate with social media platforms, detect and neutralize the propaganda activities of terrorist organizations, identify individuals at risk of radicalization, and take preventive measures against these individuals. The digital age has fundamentally altered the calculus of counterterrorism, demanding a shift from reactive monitoring to proactive disruption within the very ecosystems terrorist's exploit. Beyond simply tracking encrypted communications and social media posts, intelligence agencies must engage in a form of 'digital anthropology', mapping the online communities, influencers, and narratives that fuel radicalization. This requires not only technical prowess in identifying and removing extremist content, but also strategic partnerships with tech companies to develop early warning systems and counter-narratives that resonate with at-risk populations. Moreover, the focus must extend beyond content removal to understanding the psychological drivers that draw

individuals into these online echo chambers, allowing for targeted interventions that disrupt the radicalization process at its source.

Security intelligence and securing intelligence is critical in the fight against terrorism. Understanding the structure, tactics, funding sources, and goals of terrorist organizations, preventing their actions, and bringing terrorists to justice is essential for security intelligence. Security intelligence is obtained through the analysis and evaluation of information gathered from various sources such as human resources, signal intelligence, imagery intelligence, and open-source intelligence. The effectiveness of security intelligence depends on the analytical capacity of intelligence agencies. Intelligence agencies must accurately analyse the information gathered, predict the actions of terrorist organizations in advance, and provide decision-makers with timely and actionable intelligence. Therefore, intelligence agencies need to strengthen their analytical capabilities, train qualified intelligence analysts, and continuously improve intelligence processes.

However, the pursuit of actionable intelligence must not overshadow the critical imperative of safeguarding its integrity. In an era where disinformation and deepfakes can be weaponized to sow chaos and manipulate perceptions, ensuring the veracity and provenance of intelligence becomes paramount. This necessitates a robust framework for validating information sources, cross-referencing data across multiple modalities, and implementing stringent protocols to prevent the infiltration and manipulation of intelligence streams by hostile actors. Furthermore, fostering a culture of intellectual humility within intelligence agencies is crucial; acknowledging the inherent limitations of any single data point and promoting a collaborative approach that encourages diverse perspectives can mitigate the risks of cognitive biases and groupthink, ultimately bolstering the resilience of the intelligence apparatus against both internal and external threats.

In conclusion, counterterrorism requires a multifaceted approach supported not only by military and security measures but also by intelligence activities. Intelligence agencies can play an important role in the fight against terrorism by closely following technological developments, strengthening their analytical capabilities, and effectively using security intelligence. The convergence of cybersecurity, counterterrorism, and intelligence coherence demands a holistic strategy that transcends traditional silos. Recognizing that modern terrorist operations are deeply intertwined with digital infrastructure;

intelligence agencies must prioritize the integration of cyber threat intelligence into their broader counterterrorism frameworks. This necessitates not only the development of advanced threat detection and attribution capabilities, but also the cultivation of seamless information sharing and collaborative protocols across national and international security partners. Furthermore, the proactive defence of critical infrastructure against cyberattacks—which could be leveraged to fund or facilitate terrorist activities—requires a unified approach that combines robust cybersecurity measures with strategic intelligence gathering, ensuring that the digital domain is not a vulnerability, but a fortified front in the ongoing struggle against terrorism.

The main findings and recommendations of this study are as follows:

Technology is both an opportunity and a threat. Intelligence agencies should closely monitor technological developments and adapt to new technologies. At the same time, they should develop strategies to neutralize the use of technology by terrorist organizations. Social media is an important area in the fight against terrorism. Intelligence agencies should cooperate with social media platforms, detect and neutralize the propaganda activities of terrorist organizations, identify individuals at risk of radicalization, and take preventive measures against these individuals. Security intelligence is the cornerstone of counterterrorism. Intelligence agencies should strengthen their analytical capabilities, train qualified intelligence analysts, and continuously improve intelligence processes. Intelligence should guide policymakers. Intelligence agencies should provide decision-makers with timely and actionable intelligence and help policymakers make informed decisions in the fight against terrorism. The fight against terrorism is a long and challenging process. However, by closely following technological developments, strengthening their analytical capabilities, and effectively using security intelligence, intelligence agencies can play an important role in the fight against terrorism and contribute to the security of the international community.

Declaration

In all processes of the article, TESAM's research and publication ethics principles were followed.

There is no potential conflict of interest in this study.

The authors declared that this study has received no financial support.

The authors contributed equally to the study.

References

Arquilla, J., & Ronfeldt, D. (1998). Preparing for information-age conflict: Part 1 conceptual and organizational dimensions. *Information Communication & Society*, *1*(1), 1-22.

Bridis, T. (1999, July 7). *Hackers Become an Increasing Threat*. Associated Press.

Bural, E. B. (2021). *Sosyal Medya İstihbaratı: Açık Kaynak İstihbaratında Yeni Bir Boyut*. İstanbul: Yeditepe Akademi.

Choi, K. S., Lee, C. S., & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 21-39.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 588-608.

Darıcılı, A. B. (2020*). Güvenlik Teknoloji ve Yeni Tehditler*. Ankara: Nobel Yayınları.

Davis, A. L. (2021). Artificial Intelligence and the Fight Against International Terrorism. *American Intelligence Journal*, *38*(2), 63-73.

Demir, F. (2020). *Kamu Yönetimi ve Politikası*. Ankara: Nobel Yayınları.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239, 288.

ECD. (1998). *Day of Net Attacking Against Vivisection*. ECD Report.

Elshimi, M. (2018*), Thinking about the symbiotic relationship between the Media and Terrorism*, Morocco: OCP Policy Center.

Gill, P. (2007). *"Knowing the self, knowing the the other": The Comparative Analysis of Security Intelligence*. L. K. Johnson içinde, Handbook of Intelligence Studies (s. 82-90). Oxon: Routledge.

Grabo, C. (2010). *Handbook of Warning Intelligence: Assessing the Threat to National Security*. Plymouth: Scarecrow Press.

Gross, T. (1999, February 7). *Israeli Claims to Have Hacked Saddam Off the Net*. London Sunday Telegraph.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy Concerns and Perspectives Following the Cambridge Analytical Scandal. *International Journal of Human-Computer Studies*, 143.

Huang, L. & Zhu Q. (2023). *Cognitive Security: A System-Scientific Approach*. Brooklyn: Springer Cham.

Johnson, L. K. (2007). *Handbook of Intelligence Studies*. Oxon: Routledge.

Johnson, L. K. (2018). *The Oxford Handbook of National Security Intelligence*. Oxon: Oxford University Press.

Johnston, R. (2005). *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. Washington D.C.: Central Intelligence Agency Center for the Study of Intelligence.

Kartal, A. B. (2018). ''Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği'', *Güvenlik Stratejileri Dergisi*, 14 (27), 33- 77 https://dergipark.org.tr/tr/download/article-file/486376, Erişim tarihi: 10. 12.2021

Kitler, W. (2021). *National Security Theory and Practice*. Warsaw: The Publishing House of the Society of the Defence Knowledge.

Lahmann, H. (2022). *The Future Digital Battlefield and Challenges for Humanitarian Protection: A Primer*. The Geneva Academy.

Liang, C. S. (2015). *Cyber Jihad: understanding and countering Islamic State propaganda*. GSCP Policy Paper, *2*(4), 6.

Mağat, M. (2020). *Ulusal Güvenlik Politika Sisteminde Kültür Anlayışı ve Yönetim Yaklaşımı*. İstanbul: Motto Yayınları.

Martin, S. (2016). *Spying in a Transparent World: Ethics and Intelligence in the 21st Century*. Geneva: Geneva Centre for Security Policy.

Mergel, I., Ganapati, S., & Whitford, A. B. (2020). Agile: A New Way of Governing. *Public Administration Review*.

Miller, S. (2022). National security intelligence activity: a Philosophical analysis. *Intelligence and National Security*, *37*(6), 791-808.

Miller, S., & Bossomaier, T. (2024). *Cybersecurity, Ethics, and Collective Responsibility*. New York: Oxford University Press.

MİT. (2021). MİT Başkanlığı Teşkilat Yapılanması: https://www.mit.

gov.tr/teskilat.html adresinden alınmıştır

Nashu, H. (2015). State Secrets Law and National Security. *International and Comparative Law Quarterly*, 64, 365-404.

Ogunlana, S. O. (2019). Halting Boko Haram/Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. *Journal of Strategic Security*, *12*(1), 72-106.

Poyraz, M. (2024). Silahlandırılmış Yapay Zekâ Otonom Silah Sistemleri ve Uluslararası Hukuk. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, *14*(1), 887-894.

Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, *11*(4), 50-85.

Şengöz, M. (2019). *Ulusal Güvenlik Yönetimi Felsefesi: Aksiyolojik Paradigma*. Ankara: Astana Yayınları.

Şeşen, Y., & Kuzucuoğlu, A. H. (2021). Intelligence Activities in the Context of Data and Information Security. *Library, Archive, And Museum Research Journal*, 2(2), 93-110.

Tiryaki, E. & Özdal, B. (2020), Açık Kaynak İstihbaratında Sosyal Medyanin Rolünün Analizi, *Academic Review of Humanities and Social Sciences (ARHUSS)*, (2020), *3*(2), 267-296.

Toktay, Y. (2019). *Sosyal Medyada Dezenformasyon, Manipülasyon ve Propaganda Etkisi: Zeytin Dalı Harekatı Örneği*. Yayınlanmamış Doktora Tezi. İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Wall, C. (2025). The Ghost in the Machine: Counterterrorism in the Ageof Artificial Intelligence. Studies in Conflict and Terrorism.

Wirtz, J. J. (2007). *The American Approach to Intelligence Studies*. L. K. Johnson içinde, Handbook of Intelligence Studies (p. 28-38). Oxon: Routledge.

Yılmaz, S. (2018). *Temel İstihbarat*. Ankara: Kripto Yayınları.