PROTECTION OF NATIONAL SECURITY FROM NEW METHODS OF EXTREMISM AND TERRORISM

Selmin Nesimoski[1]
PhD Candidate, Faculty of Philosophy, Institute for Security, Defence and Peace

Abstract: National security in the 21st century faces increasing challenges, making its protection ever more complex, despite the long-standing presence of threats such as terrorism and extremism. This is due to the constant advancement of technology as well as the high adaptability and skill of these non-state actors in exploiting new technologies for their benefit. Recent examples include artificial intelligence-generated propaganda, the creation of fake identities, automated bots moderating group discussions, and the use of voice cloning to spread false information—creating deceptive content that aids in the radicalization of new members. In addition to periodically reformatting their devices, extremists and terrorists commonly use freely available end-to-end encrypted (E2EE) applications, VPNs, the dark web, and cryptographic applications to enhance communication privacy. The metaverse and cryptocurrencies have emerged as new tools for terrorists and extremists, and along with the dark web, they pose a significant challenge to national security and its protection.

Keywords: National security, extremism, new technologies, dark web, cryptocurrencies.

The protection of national security in the contemporary security environment

The protection of national security has never been a simple or easy task for states, but today it is more complex and unpredictable than ever before. Traditional threats to national security may have appeared to be sidelined for a moment; however, the outbreak of conventional wars in Europe has demonstrated that such threats are far from being entirely dormant.

On the other hand, the processes of globalization have created new avenues and opportunities for non-state actors to operate, making the protection of national security significantly more complex. Ensuring the security of the state has become a multifaceted issue that must be addressed beyond the scope of purely conventional threats. In other words, the protection of national security must also focus on the transformed nature of non-state actor activity—specifically, their exploitation of the advantages provided by globalization and their strategic use of digital infrastructure.

National security concepts that focus solely—indeed, predominantly—on military threats and responses are increasingly inadequate for addressing the broad spectrum of modern security risks and threats. In the current environment, such a narrow approach is no longer a viable option (Ungerer, 2008, pp. 1-3).

It can be stated unequivocally that the term national security is used today in a much broader sense than its original meaning. While in the past national security was primarily

[1] Contact address: selmin_nesimoski@hotmail.com

concerned with the military dimension—meaning that states focused on military deterrence (although this dimension remains relevant today)—contemporary national security refers to a desired state of security for the state, which can be achieved only by eliminating threats and risks that may arise from both internal and external sources (Ѓуровски, 2021, стр. 117-118), which may be military, non-military in nature, and/or hybrid.

National security often begins with the protection of national security interests. What constitutes these interests and the extent to which they are threatened varies from one state to another. However, generally speaking, there is broad consensus that territorial integrity and sovereignty represent vital national interests. Nevertheless, national security is also shaped by other vital interests, such as: **economic security**, **environmental security**, and **physical security** (Frans-Paul van der Putten, Minke Meijnders and Jan Rood, 2015), **energy security**, **political security**, **cybersecurity** and **human security** (Holmes, 2015). In this regard, security itself is understood through the prism of a broader social, economic and political context (Pavleski, 2022).

Given that security is inherently a complex concept, it is not possible to provide a single, precise definition. However, what can be distilled from the broad discussions on security is that it is closely associated with the mitigation of threats to vital values—particularly those which, if left unchecked, underestimated, or ignored, may endanger the survival of a particular referent object (of security) in the near future (Вилијамс, 2012, стр. 1-5). In addition, information about security risks and threats can also be formulated in different forms that reflect their complexity and their different assessments as well. It means that the danger, i.e., the threat may be real, but the risk is still in its essence, a social construction (Pavleski, 2023).

The concept of security in the future must shift—from its traditionally exclusive emphasis on national security and the military dimension, toward a greater focus on human security. According to Pavleski, human security is one of the new concepts that are becoming part of the security strategies of many countries, despite still-present dilemmas, especially over its practical significance and usability. However, his assessment in this regard is that the human security concept has a greater chance of being more widely accepted and more effective when based on human rights, and that human rights are more likely to be protected and respected if treated as part of human security (Pavleski, 2023). In other words, it is a transition from achieving security through weapons to enabling security through human development—from territorial concerns to concerns about food, employment, and social security. (Котовчевски, 2011, стр. 27-30).

This necessity arises precisely from the fact that terrorism is a symptom of a diseased society—a manifestation of inequality among people and historical injustice between states and nations in international relations. In such circumstances, where individuals feel disenfranchised, they are often drawn to groups that promise to "help" them take justice into their own hands. Rather than contributing to the development of society (and thereby enhancing the level of security within the state), they resort to using all available means—material and technical-technological—to inflict harm on the state and undermine national security.

From this, it can be unequivocally concluded that establishing and maintaining national security—and indeed, our very survival—does not depend solely on military balance, but rather requires global cooperation focused on a sustainable biological environment and the creation of a world in which the allocation and distribution of essential and capital resources is equitable.

In today's modern world, there is no state that is not somewhat threatened by certain forms of threats, which can often be generated from within or from outside, or even be a combination of both. There are many classifications for the types of threats to national security, but one classification based on the location of the emergence of threats or activities is particularly significant. According to this classification, there are external threats (organized, directed, controlled, and carried out from outside the state) and internal threats. Another important classification concerns how these threats are carried out, that is, whether armed force is used to achieve the set goals or whether the threats are unarmed. However, it is crucial to note that with the development of technology, there are hardly any pure forms of threats (only external or only internal, armed or unarmed); instead, it is most often a third category – combined threats (Котовчевски, 2011, стр. 164-166).

These two phenomena represent a serious challenge at the national, regional, and global levels; consequently, a significant portion of the traditional tools applied for the prevention and countering of these phenomena are becoming insufficient. Policymakers, as well as professionals in this field, must understand the specific nature of these ideologies, many of which aim at the destruction of the existing society and its order, rather than its reconstruction or transformation in accordance with their doctrines (Tanja Miloshevska, Sofija Georgievska, 2025, стр. 5).

If the GAO (Government Accountability Office) report is examined in relation to the threats that are feared to potentially jeopardize U.S. national security in the near or long term, violent extremism and terrorism occupy the fifth and sixth positions on the threat ranking list. Out of the 210 threats analyzed, which were gathered from surveys of officials from various security and intelligence agencies in the U.S., the report consolidates them into 26 groups of threats with the highest tendency to jeopardize national security. In addition to the already well-known fear of the development of nuclear, chemical, and biological weapons by a certain terrorist organization, today, as noted in the GAO report itself, uncertainty and unpredictability regarding national security are increasing due to the opportunities that terrorist and extremist organizations have in the digital age, especially with the use of sophisticated communication technologies aimed at recruiting new members or disseminating propaganda, which could further trigger suicide attacks by sympathizers (Office, 2018, pp. 1-2).

Digital Battlefield: How Terrorists and Extremists Operate in Cyberspace

The actions of terrorists and extremists in cyberspace were noted as early as the end of 2004 by the OSCE, specifically through its decision emphasizing that the OSCE expresses great concern regarding the threat to the security of states posed by terrorist and extremist organizations that use the internet to (OSCE, 2004):

- To target and recruit new members;
- To collect financial resources and engage in trade;
- To plan, organize, and coordinate terrorist acts; and
- To incite terrorist violence, most often through the dissemination of propaganda.

This list represents a good indicator of the fact that terrorist organizations have long recognized the importance of the internet and its use. Meanwhile, states and their security agencies have remained one step behind in understanding these two phenomena.

Before proceeding to the analysis of their operations, it is necessary to highlight the most widely used approach to studying the phenomenon of violent extremism, namely the classification of its underlying causes and driving factors into two main categories (Miloshevska, 2022, p. 369):

1. **"Push" factors** or structural conditions (e.g., poverty, grievances, lack of access to political processes or justice, and protracted conflict);
2. **"Pull" factors** or direct drivers, such as ideological appeal or the financial and social benefits associated with joining a violent group.

Although it is very difficult to conduct a complete analysis and provide data on the extent of extremist content present in cyberspace, the data concerning the followers of right-wing extremists can help us shape the evolutionary depiction of extremism in the digital era. According to the report by J.M. Berger, from April to June 2018, "the presence of right-wing extremists on the social network Twitter alone was of significant importance, covering more than 100,000 accounts" (Maura Conway, Ryan Scrivens and Logan Macnair, 2019, pp. 5-7).

On the other hand, the use of live streaming during the terrorist attack by Brenton Tarrant in Christchurch placed Facebook in the spotlight as a platform to broadcast messages to a wide audience. During the execution of the attack and the live broadcast, none of the individuals who were watching the terrorist attack reported it to the social network. From the moment the video was removed from the platform, Facebook immediately prevented the posting of 1.2 million videos, and over 300,000 were removed after being published. However, social media and video-sharing platforms faced a significant challenge in dealing with the innovative ways in which violent right-wing extremists distributed this violent content.

Neil Mohan, Chief Product Officer at YouTube, stated that his team worked overnight in a race to intercept and remove this content, highlighting several issues his team faced. Just one hour after the live stream ended, there was an attempt to post a video nearly every second. Furthermore, a significant challenge emerged with bypassing the algorithms designed to detect violent content, such as cutting short segments of the original video, adding logos, stickers, and captions, and recording the footage while it was being played on another device, thus altering it in ways that "outsmarted the company's detection systems" (Maura Conway, Ryan Scrivens and Logan Macnair, 2019, стр. 5-9).

When discussing non-state actors, the focus is often on tracking their organizational structure, movements, and actions in physical space—where they go, where they meet, and what their headquarters are. However, today, national security protection must advance to the next level. The internet, gaming platforms, and social media have enabled terrorists and extremists to establish and maintain close connections even in the absence of creating formal organizational structures or any formal group. The main goal and dedication of these groups is ideological, not organizational. This type of community can also be viewed from a marketing perspective, as Hughes points out, where they are ideologically based networks functioning as brand communities, filled with racism and misogyny as fundamental values of that brand. In these brand communities, a terrorist attack is legitimized and perceived as a noble action

by heroes who have decided to sacrifice their lives for the common cause (Shirley Leitch and Paul Pickering, 2022, pp. 5-9).

In addition to these activities, terrorists and extremists have advanced their methods, starting to apply technical and technological advancements in their operational activities, including reconnaissance, planning, coordination, and execution of terrorist acts.

In the terrorist attack in New Orleans on January 1, 2025, we can observe two key moments in which new technology and the internet are playing an increasingly prominent role in carrying out terrorist acts, with these technologies gaining more influence in operational actions. First, the attacker was a former U.S. active soldier who served in Middle East missions but was responsible for human resources and information technology (not directly involved in combat). What is significant here is the moment when he used the internet, specifically needing a vehicle that would have enough capacity to accommodate improvised explosives, good power, and dimensions to carry out this terrorist act. For this purpose, he used the "Turo" app, which provided him with the opportunity to meet his logistical needs by renting a Ford F-150 Lightning pickup truck, with which he crashed into a police barricade and carried out the terrorist attack, exiting the vehicle and firing at the police officers.

Second, during the planning of the attack, the attacker used Meta's smart glasses. Using these glasses, the attacker conducted surveillance of the area a month before the attack. Thanks to the technology embedded in these glasses, he collected information about the surroundings, took photographs, and filmed videos (Pierre Thomas, Josh Margolin, Aaron Katersky, Luke Barr, Bill Hutchinson, Meredith Deliso, 2025). Thanks to the artificial intelligence embedded in the glasses themselves, he was able to gather information about the surrounding environment in its entirety, even translating texts and broadcasting the attack live on social media.

Before carrying out the attack, Jabar posted videos on social media where he pledged his allegiance to the terrorist organization ISIS. Just one week later, ISIS published an article in its weekly magazine "Al-Naba," in which the attack was praised, highlighting that the attacker had used American technology during the reconnaissance process before carrying out the attack and threatening the security of the city of New Orleans. What is very important is that in the article, ISIS also called on other sympathizers to carry out similar attacks in Europe and the U.S., emphasizing that one attack could be enough to inspire other attacks and trigger a series of "voluntary cycles of attacks." This attack was carried out according to the instructions published by ISIS in the magazine "Rumiyah" in 2016, providing guidelines on how to achieve the maximum effect in terms of casualties when conducting terrorist attacks (Aaron Y. Zelin, Levy Senior Fellow, 2025, pp. 1-7).

Another challenge in this area remains the dark side of the internet, which, together with the deep web, constitutes about 96% of the internet. In 2023, the dark web had an average of 2.5 million users daily through the TOR browser. This year, the most users joined from Germany, replacing the United States. Finland, India, and Russia are the other countries with the highest number of visitors to the dark web (Awasthi, 2024, pp. 1-15).

The dark side of the internet is used for many of the activities that terrorists and extremists also carry out on the surface web. However, in this context, the list of activities is extended with a number of other services and activities provided by the dark web. They use it for sharing information, recruitment, radicalization, distributing propaganda, generating money, coordinating attacks, obtaining fake documents and travel IDs, as well as ordering

cyberattacks and acquiring necessary elements for making explosives, weapons, and similar items. Although many of these activities were carried out on the surface web, now, with the secrecy provided by the dark side, especially in preparing terrorist attacks and issuing instructions both for carrying out the attacks and for crafting explosive devices, it is also used to encourage attacks by lone wolves.

Mark Sageman argues that the dark web creates a habitat for interaction and uses chat rooms to facilitate the development of ideological relationships. In this way, the dark side of the internet has become a vital tool for the radicalization of young people. Terrorist activities on the dark web primarily cover the following categories (Awasthi, 2024, стр. 6-8):

- **Internal communication and external propaganda.** The dark web provides secure channels for communication, facilitating the secret exchange of information and wide connectivity for planning, organizing, coordinating, deploying, and executing terrorist operations.

- **Recruitment and training.** Due to increasing efforts to combat radicalization, recruitment, and propaganda on the internet, terrorists and extremists are migrating to more secure platforms, one of which is the dark side of the internet. After attracting and radicalizing individuals from large social networks, they move to the dark web where they provide training to their followers worldwide, as well as offer courses on making explosives and carrying out terrorist attacks. The anonymity offered by the dark web complicates the efforts of counterterrorism agencies in their battle to identify and prevent radicalized individuals from becoming so-called "lone wolves."

- **Fundraising and financial transactions.** In addition to conventional methods of raising funds used by terrorists, such as oil sales, kidnapping, and smuggling, they are increasingly using digital cryptocurrencies and the dark web to secure additional financial resources. This includes: donations in Bitcoin, online extortion, human trafficking, and trade in human organs. For example, one website called "Fund the Islamic Struggle Without Leaving a Trace" uses an app called Dark Wallet to receive donations in Bitcoin. Another example is the Islamic State – Khorasan Province, which, through its magazine "Voice of Khorasan" urged its followers and sympathizers to make donations in cryptocurrencies like **Monero (XMR).**

- **Acquisition of weapons.** The dark web serves as a marketplace for acquiring weapons and ammunition, where illegal trading platforms such as Silk Road facilitate the execution of such transactions. Furthermore, EuroGuns is an online platform that sells weapons. Additionally, on the AlphaBay website, terrorists and violent extremists can purchase books such as: The Terrorist Handbook and The Explosives Guide.

Future Challenges of Emerging Technology on Terrorist and Extremist Tactics, Techniques, and Procedures

Today, the most common response to protect national security by governments is the banning of extremist groups. This strategy has proven to be ineffective in combating modern, loosely, but emotionally intensely connected extremist networks. Thus, the primary priority of every state is to protect its vital and national interests, as well as to ensure a secure environment. In order to ensure national security, or in other words, to minimize the opportunities for the expansion of terrorist and extremist networks, it is essential to engage in the digital battlefield.

Although some terrorists and violent extremists use low-tech methods, the spread of relatively cheap commercial technology offers great potential for many terrorists and extremists to create and/or adopt far more sophisticated methods for creating propaganda, recruiting, financing, acquiring, communicating between members and supporters, as well as planning and executing attacks. In the next decade, there is a great possibility that terrorists and violent extremist groups will use new technology for:

- **Advancement of the Radicalization Process**

The internet may be seen as an unprecedented "communication revolution," which is, in fact, just the latest manifestation of the deep changes that every new means of communication – from the invention of parchment, through the printing press, to the telegraph – has caused over the centuries. The first technology for instant and global communication – the telegraph, for example, contributed to the establishment of colonial empires by enabling effective and timely administration of distant territories. The telegraph, much like the internet today, was associated with increased social problems, especially as it offered new opportunities for fraud and deceptive behavior. (Archetti, 2015, pp. 49-59). However, unlike previous communication technologies that were introduced, today the internet plays a much greater role due to its accessibility and the high level of possibilities it offers to everyone. The internet has enabled online recruitment, facilitating the process of communication with individuals in different parts of the world. Technological advancements in the future will further expand this ability to reach a larger audience that is of interest to terrorist and extremist groups, allowing recruiters to form, expand, and maintain social connections, spread their influence, and gain public sympathy and support for their cause. The problems will multiply due to the fact that these groups will be granted access to powerful tools such as video manipulation tools and deepfake technology supported by artificial intelligence (AI). These types of tools will enable them to create and disseminate extremist narratives, spread disinformation, call for violence (often through others, or fabricated voices of impactful figures, using AI technology), as well as build and maintain virtual ideological and social communities. For example, in the Kashmir region, Indian authorities reported that militant groups were using fake videos and photos (generated by artificial intelligence) in order to incite violence. Thus, with the combination of augmented and virtual reality (AR/VR), terrorists and extremists will be able to spread their messages through avatars based on real people to incite violence (NCTC, 2022, pp. 1-11).

- **Improving planning, training, and dissemination of propaganda**

Although in recent years, major social platforms (such as Twitter, now known as X, Facebook, and TikTok) have implemented countermeasures to combat propaganda and related profiles, the number of profiles and content supporting ISIS or its activities has significantly decreased on platforms like X and YouTube. However, by focusing exclusively on ISIS propaganda, perceiving it as the biggest threat, they have enabled a shift to other social media platforms that offer greater protection and encryption. Furthermore, these groups often employ a wide range of coordinated strategies and methods within the "larger digital ecosystem." Additionally, this shift has left space for the dissemination of propaganda from other terrorist and extremist organizations, especially from the far-right (Kirdemir, 2020, pp. 1-10).

With the help of new augmented and virtual reality (AR/VR) technology, terrorists could create virtual environments with scenarios of potential targets and other physical structures, allowing their members and sympathizers to be walked through the routes and streets leading to a specific planned target for attack. This would give them the opportunity to coordinate alternative routes, create backup plans in case Plan A doesn't succeed, and practice attack plans and scenarios in a safe virtual environment, enhancing the terrorist act and increasing its effectiveness when it is executed in real life. The development of virtual technology could also enable the creation of virtual training camps, where these training camps could be led by experienced planners located in remote war zones (NCTC, 2022).

- **Application of new methods in carrying out terrorist attacks**

Unmanned Aerial Systems, commonly known as drones, have been identified as one of the key terrorist threats by the United Nations Counter-Terrorism Committee. Today, in addition to states, non-state actors have the ability to acquire drones and use them for their own purposes. There are currently 113 countries with military drone programs, while conservative estimates claim that 65 non-state actors now have the capability to deploy drones, meaning they possess unmanned aerial vehicles (UAVs). Drones are particularly attractive to terrorists because they are widely accessible and require minimal training to operate. While high-tech military-grade armed drones remain largely out of reach for non-state actors, the potential to arm civilian drones (commercial drones) gives terrorists a military capability (Liang, 2023), Although limited, it can still be sufficient for destroying certain military targets, civilian infrastructure, or other vital objects that are of significant interest to states.

The use of self-driving vehicle bombs has not yet been realized, but certain international organizations, including NATO, fear that terrorist or extremist groups could use autonomous cars as bombs in the future. This type of vehicle could be used in such a way that a target (objective/target) is set, and the vehicle, previously loaded with explosives, would explode upon impact, thus replacing the "suicide bomber" method with "autonomous killers. " (Nelu, 2024).

Conclusion

The emergence of the internet from the very start tested the resilience of national security in states. To be more precise, it showed how prepared national security systems are to provide an adequate response to threats posed by non-state actors, actors who have transformed and aligned themselves with new technology, applying it to their activities.

National security concepts (or systems designed as such), which focus on military threats and responses through military force, are no longer sufficient to deal with the wide range of modern security risks and threats. These threats and risks, which pose a danger of either undermining or ultimately destroying states, now come from both external and internal sources. The internet has enabled extremists and terrorists to operate from all corners of the globe and contribute to executing specific terrorist acts. These attacks are no longer purely military in nature; they have become hybrid, combining military actions with activities that contribute to the growth of their cause (radicalization, spreading propaganda, and recruiting new members).

In the past, national security was dominated by the military dimension. Today, it is clear that national security represents the desired state of a country's security, which can only be achieved by eliminating threats and risks that may come from both internal and external sources, whether they are military or non-military in nature and/or hybrid. In the current environment, this is no longer optional.

From this perspective, states must focus on developing strategies and policies that allow them to intercept terrorist and extremist activities at their inception. Establishing special units within national security agencies that are multidisciplinary and well-trained could serve as a strong foundation for combating the creation of extremist and terrorist online communities, which, unlike in the past, now unite based not on structural organization but rather on their ideological stance.

Terrorist and extremist organizations will continue to use large social platforms to disseminate their propaganda. This is due to their search for a broader audience, which is currently only available through social media. The countermeasures taken by state authorities against extremism and terrorism in the online space will force these non-state actors to migrate to platforms offering greater secrecy in their communications. At present, one of these is the dark web, which primarily facilitates illicit criminal activities and services.

The collection of funds in cryptocurrencies has emerged as a significant challenge for state security agencies. Combined with artificial intelligence, these tools offer terrorists and extremists vast opportunities for content creation, voice alteration, and video falsification. Virtual reality has already begun to be utilized for training and planning terrorist activities, functioning as a type of simulator or "virtual training camp" that allows them to train their sympathizers to carry out terrorist attacks with high precision and efficiency.

National security today faces a major challenge, which, unlike in the past, requires a fast and precise response. Otherwise, national security will face severe consequences in its attempt to safeguard vital national interests.

Bibliography

Frans-Paul van d• er Putten, Minke Meijnders and Jan Rood. (2015). National security and the international context. Clingendael Institute, 10-13.

Aaron Y. Zelin, Levy Senior Fellow. (2025). The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization. The Washington Institute for Near East Policy, 1-7. Retrieved april 10, 2025, from https://www.washingtoninstitute.org/sites/default/files/pdf/ZelinTestimony20250304-v2.pdf

Archetti, C. (2015). Terrorism, Communication and New Media: Explaining Radicaliza• tion in the Digital Age. Terrorism Research Initiative, 49-59. Retrieved april 10, 2025, from https://www.jstor.org/stable/26297326

Awasthi, S. (2024). The Dark Web as Enabler of Terrorist Activities. Observer Resear• ch Foundation, 1-15. Retrieved april 8, 2025, from https://www.orfonline.org/research/the-dark-web-as-enabler-of-terrorist-activities

Holmes, K. R. (2015). What is national security? INDEX OF U.S. MILITARY STRENGTH, 17-20. Retrieved April 08, 2025, from https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf

Kirdemir, B. (2020). EVOLUTION OF VIOLENT EXTREMIST AND TERRORIST THREATS ON SOCIAL WEB. Centre for Economics and Foreign Policy Studies (2020), 1-10. Retrieved April 2, 2025, from https://www.jstor.org/stable/resrep26085

Liang, C. S. (2023). Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies. Geneva Centre for Security Policy. Retrieved april 15, 2025, from https://www-gcsp-ch.translate.goog/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies?_x_tr_sl=en&_x_tr_tl=mk&_x_tr_hl=en&_x_tr_pto=wapp

Maura Conway, Ryan Scrivens and Logan Macnair. (2019). Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. International Centre for Counter-Terrorism, 5-9. Retrieved April 15, 2025, from https://www.jstor.org/stable/resrep19623

Miloshevska, T. (2022). A CONCEPTUAL FRA•MEWORK OF RADICALIZATION AND. Annual, 75(1), 369. Retrieved April 15, 2026, from https://journals.ukim.mk/index.php/godzbo/en/article/view/2229

Miloshevska, T., Georgievska, S. (2025). Capacity building guidebook with moduls for preventing violent extremism. Open Gate/La Strada. Retrieved April 15, 2026, from https://lastrada.org.mk/wp-content/uploads/2025/05/Prirachnik-prevenci-a-na-nasilen ekstremizam_angliski.pdf

NCTC. (2022). Emerging Technologies May Heighten Terrorist Threats. First Responders Tool Box. Retrieved april 9, 2025, from https://www.odni.gov/files/NCTC/docu-

ments/jcat/firstresponderstoolbox/134s__First_Responders_Toolbox__Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf

Nelu, C. (2024). Exploitat• ion of Generative AI by Terrorist Groups. ICCT. Retrieved April 6, 2025, from https://icct.nl/publication/exploitation-generative-ai-terrorist-groups

Office, G. A. (2018). National Security - Long-Range Emerging Threats Facing theUnited States As Identified by Federal Agencies. GAO-19-204SP. Retrieved from https://www.gao.gov/assets/gao-19-204sp-highlights.pdf

OSCE. (2004). DECISION No. 3/04 COMBATING THE USE OF THE INTERNET FOR TERRORIST PURPOSES. Sofia: OSCE. Retrieved April 20, 2025, from https://www.osce.org/files/f/documents/f/d/42647.pdf

Pavleski, A. (2022). Re-thinking security through the prism of the security studies approach. SECURITY HORIZONS Volume III, No. 6, University "St. Kliment Ohridski"-Bitola,Faculty of Security- Skopje. Retrieved from https://fb.uklo.edu.mk/wp-content/uploads/sites/10/2022/10/TOM-1.2022-konecen-1.pdf

Pavleski, A. (2023). Risk perception and risk management – conceptual understandings and dilemmas. SECURITY HORIZONS Volume VIII, No. 1, Univ• ersity "St. Kliment Ohridski"-Bitola,Faculty of Security- Skopje. Retrieved from https://fb.uklo.edu.mk/wp-content/uploads/sites/10/2023/09/TOM-1-konecen.pdf

Pavleski, A. (2023). The nexus between human security and human rights. ROCZNIK ADMINISTRACJI PUBLICZNEJ 2023 (9). Retrieved from https://www.ceeol.com/search/article-detail?id=1224573

Pierre Thomas, Josh Margolin, Aaron Katersky, Luke Barr, Bill Hutchinson, Meredith Deliso. (2025, January 02). New Orleans truck attack suspect: What we know about Shamsud-Din Jabbar. Retrieved april 19, 2025, from ABC News: https://abcnews-go-com.translate.goog/US/suspect-new-orleans-attack-bourbonstreet/story?id=117247072&_x_tr_sl=en&_x_tr_tl=mk&_x_tr_hl=en&_x_tr_pto=wapp

Shirley Leitch and Paul Pickering. (• 2022). Rethinking social media and extremism. (P. P. SHIRLEY LEITCH, Ed.) ANU Press, 5-9. Retrieved april 3, 2025, from https://www.jstor.org/stable/j.ctv2tsxmq6.7

• Ungerer, C. (2008). A new agenda for national security. Australian Strategic Policy Institute. Retrieved April 07, 2025, from http://www.jstor.com/stable/resrep03892

Вилијамс, П. Д. (2012). Студии по безбедност. (П. Д. Вилијамс, Ed.) Скопје: Национална и универзитетска библиотека "Св. Климент Охридски", Скопје.

Ѓуровски, М. (2021). Основи на безбедност - Концепциски безбедносни пристапи. Скопје: Фондација Конрад Аденауер во Република Северна Македонија.

Котовчевски, М. (2011). Национална безбедност. Скопје: Филозофски факултет - Скопје.