BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Implications of the jihadist terrorism in cyberspace

Bianca Brandea, Ph.D. Candidate*

* University of Bucharest, Faculty of Foreign Languages and Literatures
"Languages and Cultural Identities" Doctoral School, Romania
e-mail: bianca.brandea@drd.unibuc.ro

Abstract

The terrorist attack on the 11th of September, 2001, marked the change in the West's perception of the Middle East and vice versa. Followed by the US military presence in the Middle East, this event contributed to the development of the means of terrorist actions around the world and the popularization of jihad. The hostile attitude of the West thus succeeded in maintaining the state of tension between the two spaces. Over time, jihadist and terrorist groups have been joined by members originating from the West who were convinced by the importance of the "missions" they later undertook. In the present paper, we will focus on the transposition and continuation of hostilities in both geographic and cyber spaces, with reference even to the current Israeli-Palestinian conflict.

Keywords:
terrorism; jihad; security; conflict; hacktivism; propaganda; defense; cyberterrorism.

Article info
Received: 12 February 2024; Revised: 28 February 2024; Accepted: 13 March 2024; Available online: 5 April 2024

Citation: Brandea, B. 2024. "Implications of the jihadist terrorism in cyberspace". *Bulletin of "Carol I" National Defence University*, 13(1): 157-165. https://doi.org/10.53477/2284-9378-24-10

The beginning of the 21st century brought major changes in the West's perception of the Middle East, a fact that contributed to the delimitation and segregation of the two spaces. Perpetual Western technological progress goes hand in hand with the evolution of Eastern attitudes and measures regarding Western supremacy. In this paper, we will analyze situations in which the interference of the two spaces was necessary for the performance of offensive and combative actions, from the physical environment to the virtual environment.

The international armed conflicts of the last decade – especially those in Eastern Europe and the Middle East[1] – have strengthened the rivalry between the US and Russia and reinstated negotiations on the positions of each other's allies. The conflict between Israel and Palestine is the most important one that we will consider, for which we will note some of its most important implications throughout history.

[1] The focus of our discourse herein pertains to the geographical domain commonly referred to by historians as the Near East, a constituent component encompassed within the broader expanse recognized as the Middle East.

In general, during international military tensions, the phenomenon of radicalization is becoming more common among civilians interested in actively supporting the cause of their belief. The unfettered access to the internet facilitates the circulation of materials designed to attract new followers who either already share the beliefs publicized or become interested or attracted to them. In the case of the radicalization of cyberspace attackers, the propaganda they are exposed to is intended to form invisible "troops" to contribute to hostilities from an invisible "front". It is notable that such "troops" are not only created through propaganda that is accessible on the internet, but they also include members who have extremist views gained from other sources, especially of a political nature.

The cyber environment is constantly exposed to threats both psychological and with repercussions in the physical environment. Therefore, in the context of the current armed conflicts in the proximity of Romania, the EU, and NATO, a high degree of alertness in cyberspace is necessary for attempting to meet and counter threats, attacks of various types, propaganda, and disinformation, taking into account the fact that such events have already taken place under the justification of contesting Romania's position.

Cyber-jihad or cyberterrorism?

Jihadist propaganda spread online by terrorist organizations such as Al-Qaida or ISIS is a manner of intimidating Westerners, but also a way of recruiting Muslims from both areas, namely encouraging non-Muslims to convert to Islam in order to join the jihad. It is important to state that, in such a context, Islam is used as a tool for manipulation and radicalization,

encouraging values that are not found in authentic Islam or that are even opposed to it, thus promoting an incomplete and incorrect image of religion (Toma 2013, 72).

For some jihadists, radicalization has meant adopting a new way of life, in which goals such as establishing a new Caliphate, killing those who do not follow the rules and values they consider to be Islamic, destroying or reshaping the West and especially the great powers, etc. (Leiken 2012, 142-144). Although all jihadist groups are divided by goals and ideologies, supporting the Palestinian cause represents a common ideal. For example, Al-Qaida's online approach is not only focused on insulting Israel but also involves incriminating Arab states that support Western perspectives on the conflict in Palestine. In addition, based on Europol's analysis of Al-Qaida's online propaganda in 2021, they claimed that jihad involves engaging every Muslim in support of the Palestinian cause while encouraging attacks against Israel, "Crusaders" and "Zionist" Arab states (Europol 2022, 39). By maintaining such beliefs, the information published by ISIS is intended to convince the audience that the jihadists are in fact the real Muslims (Frampton, Fisher and Prucha 2017, 24).

In another study published by Europol in 2017, cyber-jihad is described as "the global exploitation of the Internet by the Islamic State, which identifies itself as the Cyber Caliphate, through the specific discourse aimed at attracting hackers from around the world to engage in the media war against the "Crusaders" and join the United Cyber Caliphate" (Antinori 2017, 6).
These are just some of the concepts that underlie threats in the real world, but in the following lines, we will focus on the situation on the cyber "battlefield" and the common motivations identified at both levels.

Notably, jihad and terrorism are two distinct concepts. According to the *Dictionary of International Security*, jihad, although often translated as "holy war", is described as a central element in Islam, representing struggle, striving, or effort. Jihad can be offensive in order to spread Islam or defensive in situations where Islam is under attack (Robinson 2010, 119). Terrorism has not been given a precise definition, being described as a phenomenon that "consists of the illegal use of force by non-state actors with the aim of spreading terror among civilian populations and forcing governments to political concessions. The use of illegal violence is what distinguishes terrorism from normal political activity, legal/judicial violence, and conventional warfare" (Robinson 2010, 227).

As for the differentiation between cyber-jihad and cyberterrorism, it should be stated that information disseminated on behalf of a terrorist organization or a jihadist acting alone belongs to the cyber-jihad category. In contrast, cyberterrorism aims to carry out attacks with the aim of contributing to economic, political, and psychological conflicts (Babanoury 2014), and, in a strict sense, the usage of cyberspace as a tool for causing physical harm to individuals and objects (Torres 2016, 109).
Hence, placing the two concepts in the field of cyber security, we observe that jihadist

propaganda uses the religious pretext to attract followers, while Islam is actually the appearance of intentional political actions, while terrorism represents the tense state and attacks motivated by similar pretexts.

Terrorism abreast with cyber progress

In his study on the radicalization phenomenon of the second generation of Asian and African immigrants in Europe, Robert S. Leiken mentions the attraction of young extremists to the chosen identity, at the expense of the inherited one. Such an identity is shaped as a result of the failure of integration both among European natives and the lack of identification with the extended family and community of origin of the immigrant parents. Consequently, the justificatory discourse provided by terrorist groups together with the sense of belonging in a united community represents the ideal context for channeling their lifelong anger (Leiken 2012, 410).

Various specialists argue that terrorism associated with Islamist extremism is not technologically advanced enough to pose a major threat. Hunker (2010) notes that disruptive cyberattacks by terrorists are likely and possible, rather than serving to annoy the masses, cyber itself not being a weapon of terror (Hunker 2010, 12). Torres (2016) suggests that jihadists do not have the necessary technical training for cyber warfare, being rather prone to propaganda and hacktivism (Torres 2016, 108-9).

Interest in continuous technological progress and exposure to social networks where propagandistic materials and news of interest can be disseminated, along with the principle expounded by Leiken (2012) can establish a risk factor even for Romania's general and cyber security. According to the National Defense Strategy for 2020-2024, one of the listed risks includes "the intensification of global Islamist-jihadist propaganda that feeds the risks of radicalization on the national territory, including among Romanian citizens, conferring perspectives that are difficult to anticipate and counter" (Presidential Administration, 27).

From a general point of view, the attention of the Islamist terrorist organizations is mainly directed towards the states that support the US in the actions carried out in the Middle East. From this point of view, Romania could constitute a "legitimate" target, a fact that is also motivated by Romania's permanent involvement in international security councils and committees (Andreescu and Radu 2015, 273). "Indirectly exposed, through association with NATO, the EU, the USA, and the European states involved articulately in combating the scourge, our country remains a target of opportunity" (Presidential Administration, 25).

Romania has already been the target of DDoS attacks claimed by the pro-Russian hacker group Killnet and occasioned by the military and social support given to Ukraine as a result of the war started by Russia (Oancea 2022). The states that assist

Ukraine are still eligible as future targets for this type of attack, at least until the armed conflict has been finished (SRI 2022).

Hacking and hacktivism: the weapons of volunteers during armed conflict

Between hacktivism and cyber terrorism, there are similarities, but especially differences. Hacktivism involves a low level of disruption to the functionality of targets, with the main objectives being to humiliate them and gain visibility. In terms of cyber terrorism, perpetrators aim to remain undetected and the main goals are to undermine institutional security and public trust by attacking critical infrastructure and emergency services. Common features of the two concepts are the spread of propaganda, recruitment and fundraising intentions, and similar attack tools and techniques. In cases where hacktivists and cyber-terrorists have opposing visions, it is not out of the question that there will be cyber-attacks between the two types of groups (Baldi, Gelbstein and Kurbalija 2003, 18-19).

The involvement of the Killnet group in the conflict between Palestine and Israel does not represent the intention to support Palestine or the Hamas group with certainty, being rather an opportunity to launch cyberattacks against Israel. Their actions benefit the interests of other compatible groups around the world, as evidenced by their cooperation with Anonymous Sudan in the campaign against the "Israeli regime" (Hollingworth 2023). Although there is no accurate evidence that the members of the aforementioned groups belong to terrorist or jihadist organizations, we can identify two important elements that are part of the pattern of terrorist threats.

The first element is outlined by the choice of high-level targets. Successfully carrying out attacks on a government symbolizes the interaction between the attacker and the victim. In this way, the attacker has the certainty of delivering hostile messages and gains recognition of their destructive potential. Gaining control of government cyberspace means, as a result, the ability to control the security of the entire targeted state.

The second element is represented by the voluntary involvement of foreigners in supporting relevant causes and/or carrying out attacks. Analogous to non-Arabs and non-Muslims joining jihadist groups, we observe the motivation of pro-Russian and Sudanese groups to contribute to harming the Israeli government cyberspace.

On the other hand, radicalization is a key principle in the behavior and mentality of jihadists and terrorists. For hacktivists, radicalization is not necessarily a defining element, given that most high-profile attacks are carried out during periods of political tensions. Nevertheless, the extremist character is rather common to both hacktivists, hackers, and jihadists.

In addition, images of Palestinian civilians injured during the conflict – especially children – have over time contributed to the rise of jihadists and their desire to act against Israel in particular, but also against the Western states that support it. *Ways of cyberterrorism* cites the example of Nizar Trabelsi, a jihadist accused of planting a bomb in a military base in Belgium, who testified that images of a girl killed in the Gaza Strip encouraged him to become a member of Al-Qaeda in 2001 (Topor 2019, 87).

For better clarity on the current international tensions, it is relevant to recall some important aspects of the history of the last decades. In his study published in 1990 about the Arab-Israeli political tensions and the Cold War, Jerome Slater presents the conflict as caught up in the rivalry between the US and the Soviet Union, where the USSR would have pursued its expansionist ideology over the Middle East, eliminating US and NATO influences from the area and especially the energy independence of the West, Japan and the USA (Slater 1990, 557-9). In addition, Slater mentions the active support provided by the USSR for the establishment of the state of Israel, including the diplomatic recognition offered to Israel in 1948 within the UN council; certain historians justify the USSR's position during the named period as having the purpose of diminishing the British influence in the Middle East (Slater 1990, 562).

At the formal level, the evolution of the conflict broadly depends on the attitude of the "great powers" and the "superpower", respectively on the definition of the latter. According to Sarcinschi's study, the "superpower" status could be attributed to the United States of America, but during the latest decades, the decline of the power of the USA is taken into account, followed by the potential assignment of this rank to another state. As for the current "great powers", the states internationally recognized as having this status are the USA, Great Britain, China, France, Russia, Japan, and Germany (Sarcinschi 2010, 20-21). In the context where Israel plays the leading role in the conflict that started in 1948 and intensified in 2023, there are theories according to which Israel intends to become a superpower in the Middle East (Khashan 2020), at the global level (Kor 2021), in the field of technology (Forbes 2015), respectively of artificial intelligence for warfare (Williams 2023).

On the cyber "front", two defining aspects thus emerge for the perspectives of extremists on each of the opposing sides: the side allied to Israel seeks to achieve cyber and especially informational supremacy, while the side allied to Palestine opposes these operations, acting rather in response to Israel's continued offensives. In general, cyberattacks of a terrorist nature are classified as disruptive attacks by state and non-state actors, and cyber warfare is named as a special form of disruptive attack. A cyber war includes a disruptive attack on the space of one state by another state, which can be classified as an act of use of force (Hunker 2010, 2-4).

In an article on the cyber perspective of the conflict in the Gaza Strip, published by the Singaporean company Cyfirma, cyber security is particularly important not only

for the states involved, but also for their allies. This conclusion is based primarily on the conduct of cyber-attacks by hacktivist groups and threats from other types of actors in various regions that have targeted government websites, the education and media sectors, billboards, power plants, warning systems, and even sensitive military information. The article also mentions the possibility of Iran and its allies conducting "preemptive" actions in the near future as a result of Israeli attacks against Palestine (Cyfirma 2023).

In another Cyfirma article on hacker and hacktivist attacks in conflictual contexts of international relations, diplomatic intervention by governments is recommended in order to reduce geopolitical tensions. In such an approach, it is envisaged hacktivist activities can be prevented by eliminating their actual motivations (Cyfirma 2024).

Conclusions

The international conflicts in which the West and the Middle East are involved attract the engagement of civilians from both areas who, for this purpose, can carry out their offensive actions in the cyber environment. The conflict between Palestine and Israel is an opportunity for the intensification of jihadist and terrorist propaganda, which is joined by followers from both the Western and Eastern space.

The arguments applied to justify the hatred and the possible offensive position against the West are currently amplified as a result of the support provided by the West to Israel, a fact that may imply the increase in the number of terrorist threats in the cyber environment and outside it. Disagreement with the positions adopted by Western governments is also expressed among certain civilians originating in the West who, motivated by empathy and the belief that they can contribute to changing the international political landscape, adhere to an interpreted form of religion that gives the appearance of concordance with the ideologies that they generally guide themselves. Thus, an important part of the threats in conflict contexts is realized by exploiting the psychological factor both of the attackers who have the opportunity to satisfy their need for validation and of the targets among whom the state of terror is installed.

Romania is a potential target due to its presence in the EU and in treaties such as NATO, but precisely these memberships are crucial for maintaining and increasing the level of security, as well as cooperation in order to achieve these goals. In conclusion, complementary to military and logistical involvement in conflict zones, the resilience and defensive dimension of Romania's cyber environment remain extremely important regardless of the evolution of events.

References

Andreescu, Anghel and Nicolae Radu. 2015. *Jihadul islamic. De la „înfrângerea terorii" și „războiul sfânt" la „speranța libertății" [The Islamic Jihad. From "defeating terror" and "holy war" to "hope for freedom"].* București: RAO.

Antinori, Arije. 2017. *The "Jihadi Wolf" threat the evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization "ego-system".* Hague: Europol Public Information.

Babanoury, Julien. 2014. *Cyber Jihad: The Internet's contribution to Jihad.* https://incyber.org/en/cyber-jihad-the-internets-contribution-to-jihad-par-julien-babanoury-ceis/.

Baldi, Stefano, Eduardo Gelbstein and Jovan Kurbalija. 2003. *Hacktivism, cyber-terrorism and cyberwar. The activities of the uncivil society in cyberspace.* Msida: DiploFoundation.

Cyfirma. 2023. *Israel Gaza conflict: the cyber perspective.* 18 October. https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/.

—. 2024. *Caught in the Crossfire : How International Relationships Generate Cyber Threats.* https://www.cyfirma.com/outofband/caught-in-the-crossfire-how-international-relationships-generate-cyber-threats/.

Cyware. 2019. *Flame 2.0 spyware found using strong encryption algorithm to avoid detection.* https://cyware.com/news/flame-20-spyware-found-using-strong-encryption-algorithm-to-avoid-detection-36939d76.

Europol. 2022. *Online Jihadist Propaganda 2021 in review.* Luxemburg: Publications Office of the European Union.

Forbes, Steve. 2015. *How The Small State Of Israel Is Becoming A High-Tech Superpower.* https://www.forbes.com/sites/steveforbes/2015/07/22/how-the-small-state-of-israel-is-becoming-a-high-tech-superpower/.

Frampton, Martyn, Ali Fisher and Nico Prucha. 2017. *The New Netwar: Countering Extremism Online.* London: Policy Exchange.

Hollingworth, David. 2023. *Killnet and Anonymous Sudan join forces to target Israel in widespread hacking campaign.* https://www.cyberdaily.au/security/9652-killnet-and-anonymous-sudan-join-forces-to-target-israel-in-widespread-hacking-campaign.

Hunker, Jeffrey. 2010. *Cyber war and cyber power: Issues for NATO doctrine.* Rome: NATO Defense College.

Khashan, Hilal. 2020. *Israel Becomes the Middle East's Superpower.* https://geopoliticalfutures.com/israel-becomes-the-middle-easts-superpower/.

Kor, Moira. 2021. *'I'm going to turn Israel into a world superpower'.* https://www.jns.org/im-going-to-turn-israel-into-a-world-superpower/.

Leiken, Robert S. 2012. *Islamiștii europeni. Revolta tinerei generații.* [*Europe's Angry Muslims. The Revolt of The Second Generation*]. Translated by Sorin Șerb. Bucharest: Corint Books.

Oancea, Dorin. 2022. *Grupul de hackeri pro-rus Killnet a revendicat atacul cibernetic ce a afectat mai multe site-uri ale instituțiilor din România [The pro-Russian hacker group Killnet claimed the cyberattack that affected several websites of Romania institutions].* https://www.mediafax.ro/externe/grupul-de-hackeri-pro-rus-killnet-a-revendicat-atacul-cibernetic-ce-a-afectat-mai-multe-site-uri-ale-institutiilor-din-romania-20782645.

Presidential Administration. 2020. "The Nationl Defence Strategy for 2020-2024." https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf.

Robinson, Paul. 2010. *Dicționar de securitate internațională [The Dictionary of International Security].* Translated by Monica Neamț. Cluj-Napoca: CA Publishing.

Sarcinschi, Alexandra. 2010. *Rolul actorilor statali în configurarea mediului internațional de securitate [The role of state actors in shaping the international security environment].* Bucharest: Editura Universității Naționale de Apărare "Carol I".

Slater, Jerome. 1990. "The Superpowers and an Arab-Israeli Political Settlement: The Cold War Years." *Political Science Quarterly* 105 (4): pp. 557-577.

SRI. 2022. "Buletin Cyberint." II Semester. Accessed November 14, 2023. https://sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf.

Toma, Gabriel. 2013. *Terorismul internațional. Reacții ale actorilor regionali și globali [International terrorism. Reactions of regional and global actors].* Iași: The European Institute.

Topor, Sorin. 2019. "Ways of cyberterrorism." *Bulletin of "Carol I" National Defence University*, September: pp. 82-90.

Torres, Manuel. 2016. "The limits of cyberterrorism." Edited by H. Giusto. *Daesh and the terrorist threat: from the Middle East to Europe* (Foundation for European Progressive Studies -Fondazione Italianieuropei) 108-114.

Williams, Dan. 2023. *Israel aims to be 'AI superpower', advance autonomous warfare.* https://www.reuters.com/world/middle-east/israel-aims-be-ai-superpower-advance-autonomous-warfare-2023-05-22/.