Journal of Infrastructure, Policy and Development 2025, 9(2), 10979.
https://doi.org/10.24294/jipd10979

Article

Hackers in duty of cyberterrorism

Robert Bartko, Roland Kelemen*

Faculty of Law and Political Sciences, University of Győr, 9026 Győr, Hungary
*** Corresponding author:** Roland Kelemen, kelemen.roland@ga.sze.hu

CITATION

Bartko R, Kelemen R. (2025). Hackers in duty of cyberterrorism. Journal of Infrastructure, Policy and Development. 9(2): 10979. https://doi.org/10.24294/jipd10979

ARTICLE INFO

Received: 19 December 2024
Accepted: 20 December 2024
Available online: 18 February 2025

COPYRIGHT

Copyright © 2025 by author(s). *Journal of Infrastructure, Policy and Development* is published by EnPress Publisher, LLC. This work is licensed under the Creative Commons Attribution (CC BY) license. https://creativecommons.org/licenses/by/4.0/

Abstract: The fight against terrorism has been at the heart of the international security policy for decades. The latest forms of terrorism are now being committed in cyberspace, making detection even more difficult. Alongside traditional forms of terrorism cyberterrorism have appeared as an element of the so-called ABC-Terrorism, exploiting the potential of cyberspace. The perpetrators of cyberspace operations, some of whom are hackers, are difficult to detect. Therefore, for an effective investigation it is very important to identify—in a scientific way—hackers and types of hackers who could become perpetrators of a terrorist attack. The opportunities afforded by globalisation and the revolution of the Internet make terrorists able to exploit the possibilities offered by the industrial and internet-based society. It shall be emphasized that the internet has become an integral part of our life, rendering us and the potential terrorist targets more vulnerable. Therefore, the paper aims to identify the concept of cyberterrorism on a scientific bases and to place it in the system of cybercrimes. Furthermore, identifying potential perpetrators by describing the different types of hackers is also an aim of the article. The result of the study may contribute to more effective prevention and response by the authorities. The paper concentrates only on criminal legal perspectives and avoid the political, military legal or ethical approaches.

Keywords: terrorism; cyberspace; ABC-Terrorism; hacker; cybercrime

1. Introduction

Modernisation and globalisation which began in the 60's sought to transform our hitherto bipolar world into a single global space. These processes also had of crucial importance in the history of terrorism because their interaction has made terrorism an integral part of our postmodern age. This has led to the emergence of transnational and virtual forms of terrorism (Choi et al., 2018). The new forms of this phenomenon have been able to take advantage of the opportunities offered by the industrial and information-based society. The development of information technology, the emergence of the new technological achievements and the globalisation of the internet have played a significant role in this transformation and have clearly opened new horizons for terrorist warfare.

The new way of information flow and the advent of the Internet has precipitated a radical transformation in how information is disseminated, thereby exerting a profound influence on the nature of security challenges and the responses to them including the legal ones (Farkas, 2018). Furthermore, it has also reinforced one of the main characteristics of international terrorism, invisibility. Terrorism in its "old and traditional form" always responded directly to the tensions of the society, and its nature has not changed with technological progress. Technology is a social construct through which the traditional social sphere is intertwined with cyberspace (Kelemen,

2023). Furthermore, the traditional social conflicts have appeared also in the system of cyberspace giving opportunity and space for expansion of extremism.

Like other criminality, innovations in technology, the development of Internet, smart devices, the information and social networks and the increasingly diverse channels of digital communication have created new ways of committing terrorism and have widened the range of offences need to be handled by the criminal law (Allahrakha, 2024). This complex nature of international terrorism has created new challenges for democratic states, not only relating to the military and security policy, but also concerning the criminal legal responses. Combating terrorism in the cyberspace is also justified by the irregular migratory pressure and related terrorist attacks and the online spread of terrorist propaganda. The possibilities offered by cyberspace and the Internet creates significant network development opportunities for terrorists' organisations.

Therefore, in the first part of our research, we dealt with the dogmatic and systemic analysis of cyberterrorism as a new form of terrorism and then we focused on the perpetrators. Our research questions are the following. First, how can the concept of cyberterrorism be defined, and how can this phenomenon be placed in the system of the cybercrimes. Second, in which way can hackers link to a concrete terrorist attack, and which hackers can get perpetrators of a terrorist act. This study is structured as follows: Section 2 provides a short overview on scientific concepts of cybercrimes and tries to place—after defining it – the cyberterrorism in this system, and then presents the main forms of hackers and detects those which can be considered relevant relating to committing a cyber-terrorist attack. Section 3 presents the main results of the research, highlighting key findings in the topic chosen. Finally, Section 4 discusses the possibilities of application these findings in the field of criminal law.

2. Materials and methods

2.1. The concept of cybercrimes and cyberterrorism

It shall be underlined that we use the terminology of "cybercrime" in this paper, but we shall point out that there are several approaches to describe this phenomenon in the international literature. Therefore, the problems of defining cybercrimes begin with the terminology itself (Philips et al., 2022). Having been overviewed, it shall be emphasized that the variety of terminologies is almost endless, the most frequent of these are the following: cybercrimes, cyberspace crimes, computer crimes, computer-related crimes, electronic crimes, e-crimes, technology-enabled crimes, and high-tech crimes. Researchers have provided both simpler and more complex classification-based definition of the concept. The simple definition means that the authors try to describe the phenomenon with one complex sentence. For example, Wall (2001) defines cybercrimes as acts that cause harm in a way connected to computer. According to Gordon and Ford's (2006) concept any crime committed by using computer or hardware device can be considered as cybercrime. As for the Hungarian literature, we mention Kuno's concept. According to this conception cybercrimes are such crimes which are committed by using information technology tools and system (Kunos, 1999). Although their truthfulness is generally not disputed, these definitions are very reductive. Therefore, their usefulness is questionable, and they are unfit for

providing a global picture of the phenomenon. Concepts which operate with grouping the relevant offences are more popular in literature.

These concepts mentioned above are commonly characterised by the emphasis on using the term "cybercrime" as a "working definition", with a focus on grouping and classifying the relevant offences having common characteristics. As for this approach, the literature makes distinctions between dichotomous and trichotomous classification (Bartko et al., 2023). The most popular and accepted dichotomous approach makes difference between cyber-dependent crimes and cyber-enabled crimes. The first way of distinctions includes so-called "real cybercrimes" which have emerged with the rise of info-communications technology and do not exist outside the digital world (for example: hacking). The second category covers traditional offences which have moved into cyberspace, but they can also be committed outside it. In this group, the information system can be considered as the means of the commission of the place (for example cyberterrorism) where the crime is committed (Brenner, 2007).

The most frequently cited trichotom classifications in foreign literature comes from Wall (2007), who distinguishes between the following categories: (a) crimes against machines which are also known as crimes against the information system (for example: hacking, cracking, etc.); (b) crimes using the machine which use the information system as a mean of committing the offence (for example: computer piracy); (c) crimes in the machine which are also known as crimes involving computer content (for example: online harassment or online child pornography). Another trichotom approach is the Sarre et al.'s (2018) concept which emphasis the role and recent development in technology and creates the following groups: (a) type 1 cybercrimes which are technical ones like hacking; (b) type 2 cybercrimes which involve human-to-human contact, such as cyberbullying and (c) type 3 cybercrimes, which include acts committed by artificial intelligences, robots, and self-adaptive technologies. According to our opinion, the trichotom classification of cybercrime based on the role of modern technologies is preferable to the dichotom one, because it reflects better the future of these crimes.

However, it shall be emphasized that not only in the legal literature, but also in the international legal sources a classification of cybercrimes can be found. At this point, we refer to the Budapest Convention on Cybercrimes and its Additional Protocol from 23 November 2001. The Budapest Convention creates 5 groups for 14 criminalities. The first group includes the offences against the integrity and confidentiality of computer systems and computer data (for example: unauthorized access, illegal interception, etc.). The second group contents the computer-related crimes, for example the online fraud. The third includes the offenses relating to the content of computer data, which are regulated in accordance with the online child pornography. The fourth deals with offences relating to infringement of copyrights and related rights. Finally, the fifth category, based on the Additional Protocol, covers offences of a racist and xenophobic nature committed through computer system (for example uploading racist and xenophobic contents by using computer system or harassment with racist or xenophobic intent).

Accepting the literature's view, the emergence of terrorism in cyberspace can be interpreted in two different ways. On the one hand, in the narrower sense of cyberterrorism which refers terrorist acts committed in cyberspace and using it. On the

other hand, cyberterrorism means the other internet activities and aims of the terrorists and terrorist organisations which focuses partly on criminal acts qualified as crime by the legislation and partly on other activities which cannot be considered as crimes, but they can link and help the existence and operation of a terrorist group or terrorist organisation. These aims mentioned above are summarized by Gillespie (2016) as following: ensuring the spread of terrorist propaganda, fundraising, information spreading, secure communication between the members of a terrorist group or an organisation, and intelligence. Considering the above-mentioned approaches, cyberterrorism is not the same as committing a cybercrime with terrorist intent, it is a much broader category. A different interpretation would significantly narrow the scope of the act of terrorism and its elements of crime. In other words, in case of committing an act of cyberterrorism, the perpetrator may not only commit a hacking attack against an information system for terrorist purposes, but also use it to carry out another form of an act of terrorism. In this way, the computer and the information system can be considered as means of committing the offence. In this sense, therefore, the criminalisation of terrorism is a uniform category, whenever it is committed by using cyberspace. This position is confirmed by the mainstream literature as well, which makes basic difference between cyberterrorism in its forms of mass destruction, mass disruption and destabilization of social order (Brenner, 2006). The first category may typically include terrorist attacks against critical infrastructures using computer systems, while the second and the third one is essentially aimed at creating panic, intimidating the population, and making the social life dysfunctional (e.g., attacks against public facilities).

In this context, hackers can be perpetrators of some attacks, as they can defeat the security elements of computer systems and can give support for terrorist groups and organizations. Cyberterrorism is a good option for terrorists, because it's cheaper and more anonymous than the traditional methods. It is guaranteed by the development of technology. Terrorists use certain technologies for communicating, networking, training, financing, and recruiting. AI has been embraced by supporters of terrorism, hackers have integrated the use of generative AI and LLMs into the propaganda toolbox. They can accelerate the spread of disinformation and hate speech online with help of AI (TE-SAT 2024). The Center for Strategic & International Studies (CSIS) regularly summarizes the main cyber incidents and the list and the events on it clearly show in which way the hackers can support a concrete terrorist attack (CSIS Significant Cyber Incidents since 2006). However, to see which hackers may be involved as perpetrators relating to an act of cyberterrorism, it is important to analyse hackers in comprehensive way. This is what we aimed to do in the next session.

2.2. Type of the hackers and perpetrator model

A crucial approach to preparing for challenges in national and cybersecurity is the development of scenarios that map potential future attacks. These scenarios can reveal current vulnerabilities by highlighting potential threats. In the context of terrorism, they may identify infrastructures that are not yet critical at the given moment but could become so through foreseeable processes. This can also support advancements in the security aspects of tools, while the resulting documents may

provide insights into regulatory directions. However, these scenarios suffer from a significant shortfall: they are heavily technology-focused and give insufficient attention to cultural, societal, and psychological factors, thereby neglecting the human element. This is particularly noteworthy as the individual remains the central component in the attack chain (Kigler, 2015)

The FBI's reports on cybercrime consider cyberterrorism only in a restrictive sense and fail to address cases where it intersects with traditional terrorism, such as financing, planning, and operational support (FBI Internet Crime Report 2021). This approach is incomplete and undermines the accuracy of preparation and mapping as outlined by Kigler. Terrorist organizations exploit digital platforms for financing, recruitment, and planning attacks. The increased financing, often facilitated by digital tools, is closely linked to the rise in terrorist activities. This financial support is critical for the execution of attacks and is complemented by recruitment efforts conducted through online platforms. Furthermore, cyberterrorism represents an extension of traditional terrorism—manifesting traditional objectives within a digital environment. This digital presence can independently cause significant harm, instill fear, and influence political decisions, or it may amplify the impact of physical acts of terrorism (Smith et al., 2023). Due to its complex nature, cyberterrorism constitutes a significant security threat that affects political, economic, and social stability worldwide. The digital realm provides a new arena for terrorist activities, complicating the effectiveness of traditional security measures (Lobach, 2022).

The FBI's 2023 report on cybercrime reinforces this perspective, revealing that cybercrime caused $12.5 billion in damages in 2023, accompanied by 880,418 reported incidents. Analyzing the FBI report highlights the significant risks these actions pose to individuals' lives and the functioning of states. In 2023, the FBI received 1193 complaints related to ransomware attacks targeting institutions within critical infrastructure sectors, with 14 out of 16 sectors being affected. The sectors most impacted by ransomware attacks included energy, water and wastewater systems, chemical industries, government institutions, financial services, food and agriculture, and, most notably, healthcare (FBI Internet Crime Report 2023). The Australian government similarly classifies cybercrimes intended to finance terrorism as high-impact crimes (Australia National Risk Assessment, 2024).

The criminal law approach to cyberterrorism encompasses these forms of conduct as well. Thus, individual hackers can engage with the phenomenon of terrorism in vastly different roles and with varying motivations. Perpetrators of cybercrimes in the digital space do not form a homogeneous group. Cyberterrorism, as a distinct category of crime, requires specialized technical expertise and targeted motivations, which distinguish certain types of hackers. The following section will analyze these groups in detail to explore the knowledge, skills, and intentions that render hackers potential cyberterrorist actors.

The study of cybercriminals, particularly hackers, is crucial for law enforcement agencies (FBI, Interpol, MI5) to effectively combat cybercrime. While the FBI does not independently classify hackers, based on its annual reports, four categories can be distinguished according to their goals: financial motivation, state and non-state actor solicitation or commissioning, hacktivism, and cyberstalkers (FBI Internet Crime Report 2023). The MI5 Director's annual threat report, being national security-

focused, uses categories aligned with this perspective. MI5 classifies hackers into the following categories: state-sponsored actors, terrorist cybercriminals and independent criminals. Terrorist cybercriminals are hackers allied with terrorist organizations, often exploiting cyber capabilities for funding, recruitment, and operational planning (MI5 Director annual threat update, 2024). However, these categories only partially, if at all, highlight the specific skills and motivations of individual hackers. It is no coincidence that law enforcement agencies themselves employ profiling to better identify hackers and understand their capabilities and motivations.

The term "hacker" originates from the 1950s, when graduate students and professionals programming mainframe computers at MIT began applying this term to themselves. It was because, confronted with the limitations of the machines at the time (which had very little memory), they attempted to "compress" programs and operating systems as much as possible by modifying and rewriting them, essentially manipulating the systems and their codes (Kazári, 2003). The narrowly defined category of hackers can be further classified, as hackers do not constitute a homogeneous group and can be typified based on their level of knowledge. According to some authors, hackers can be categorized into four groups based on their skills: 1) guru hacker, 2) casual hacker, 3) learning hacker, and 4) novice hacker. Beginner and learning hackers, while attempting to view cyberspace at a systemic level, lack the actual knowledge to make changes to its fundamental processes. Instead, they focus on identifying patterns and targeting a few well-known vulnerabilities or weak points. Casual hackers, on the other hand, are already capable of writing programs; the defining feature of this group is their ability to manoeuvre invisibly in cyberspace using circumvention tools and to communicate with other computers. The guru hacker is the most knowledgeable type of hacker, capable of writing their own programs (such as viruses or worms), which they often share with less skilled peers. They elevate their activities to an exceptionally high, almost artistic level. A guru not only comprehends cyberspace processes on a systemic level but actively intervenes in and manipulates those processes (Zhang et al., 2015).

Another widely recognized classification of hackers is the so-called "hat-based" distinction, which categorizes hackers not only by their skill level but also by the intent of their activities. In its original form, this classification identifies three groups: white hat hackers, grey hat hackers, and black hat hackers. The white hat hacker operates entirely within the bounds of legality, as they perform their activities with the authorization of system administrators and point out security vulnerabilities to help improve system defences. The grey hat hacker conducts similar activities without prior authorization, notifying system operators only afterward. The black hat hacker operates illegally, attacking systems, seeking out weaknesses and vulnerabilities, and exploiting them for their own purposes (Long, 2012).

The "hat-based" classification has expanded in recent years to include green, yellow, blue, red, and purple hat hackers. Green hat hackers are most comparable to beginner and learning hackers from earlier categories. Yellow hat hackers, also referred to as social media hackers, specialize in breaching social media accounts and user profiles. Their goals include discrediting brands, spreading malicious software, seeking revenge, or exploiting personal data. Blue hat hackers are closest to white hat hackers, as they search for system vulnerabilities upon request. It is the reason why

Microsoft organizes BlueHat conferences. In another interpretation, blue hat hackers are simply revenge-driven individuals focused solely on achieving their goals. Red hat hackers target Linux systems, aiming to disable black hat hackers. However, unlike white hat hackers, they do not intend to turn black hat hackers over to the authorities; instead, they resort to vigilantism, focusing on fully incapacitating black hat hackers, even by destroying their resources. Purple hat hackers, on the other hand, target their own systems to learn and improve their skills in a controlled environment. In terms of their goals, they can be described as a combination of blue and red hat hackers, but they operate exclusively through legal means (Shea, 2024).

More recently—though not under a "hat-based" classification—three additional categories have been associated with this group: cryptojackers, gaming hackers, and large-scale hackers. The cryptojackers and large-scale hackers share similar characteristics, as both aim to exploit the resources of external computers for their own purposes. However, while cryptojackers use these resources for cryptocurrency mining, as the name suggests, large-scale hackers focus on creating botnets to carry out high-volume cyberattacks. The emergence of gaming hackers is linked to the massive growth of the gaming industry, where many players invest significant amounts of money. These hackers exploit this trend by either disabling opponents through methods such as DDoS attacks or stealing in-game assets—now often carrying tangible financial value—acquired by other players (Panda Mediacenter, 2023). Another classification is based on the activities carried out by hackers, which also incorporates the script kiddies. Although there is some overlap between these groups, given their youthful characteristics, it is increasingly common to encounter highly skilled individuals among them. An example of this was the Russian hacker Ilya Hoffman, who, along with his accomplices, transferred approximately $97,000 to their own bank accounts from 16 American and several Russian banks in the late 1990s (Turovszkij, 2020). The "black hat" hackers can carry out state-sponsored activities, intelligence operations, cyberterrorism, or malicious internal activities within organizations. The latter refers to harmful actions perpetrated by current or former employees within an institution (Okpa et al., 2022).

Atkinson, founder of The SecOps Group and a lecturer at Lancaster University, categorizes hackers based on their malicious intent. His classification identifies script kiddies, malicious insiders, cyber activists, cyber spies, cyber terrorists, and cybercriminal organizations. Regarding cyber terrorists, he notes that they may act as state-sponsored agents, ideological groups, or individuals driven by revenge. Cyber spies may serve corporate or state interests, while cybercriminal organizations are primarily motivated by financial gain and the creation of chaos. Atkinson broadly concludes that all these groups exploit similar circumstances: user ignorance, as many individuals are unaware of risks or choose to ignore them, and inherent human flaws such as negligence, laziness, and naivety. A significant portion of people fail to treat their data as a tangible asset, unable to perceive or safeguard its value as they would with physical possessions. This phenomenon contributes to the high latency of cybercrimes, as many victims do not report incidents to law enforcement or fail to detect them altogether. Additionally, users often exhibit a heightened trust in cyberspace compared to the physical world—an aspect these malicious actors readily

exploit. Dependency on digital systems further opens opportunities for attackers to access sensitive data and, through that, even traditional assets (Atkinson, 2015).

It is no coincidence that within academic discourse, hacker classifications have moved away from the traditional "hat-based" system, increasingly shifting toward motivations as a primary basis for categorization. A classification by Singaporean authors identifies thirteen distinct types of hackers: script kiddies, learners, cyberpunks, old guards, malicious insiders, petty thieves, professionals, nation-state hackers, hacktivists, cyber predators, digital pirates, crowdsourcers, and cyber enablers. Learners differ from script kiddies in that they have no malicious intent; they are driven by curiosity and a desire to learn. Cyberpunks are low- to mid-skilled hackers whose primary goal is destruction. The old guards are non-malicious hackers motivated by curiosity and the pursuit of recognition; this group overlaps with white and grey hat hackers from the hat-based classification. Malicious insiders are disgruntled employees—current or former—who act out of financial gain, revenge, or ideological motivations. Petty thieves are those who transfer their traditional criminal activities into cyberspace. Professionals represent highly skilled hackers. Nation-state hackers work directly or indirectly for governments, destabilizing other states, creating disruption, or gathering intelligence for their sponsors. It should be added that hackers working directly within state agencies may also be responsible for protecting critical infrastructure and other key systems. Hacktivists act based on political or ideological motivations. Cyber predators are sexual predators, primarily pedophiles. Digital pirates engage in activities that violate intellectual property rights. Crowdsourcers are temporary groups of hackers collaborating to solve a particular problem. Finally, cyber enablers provide tools and resources for others to commit cyber (or cyber-enabled) crimes; they possess specialized expertise in specific areas (Chng et al., 2022).

A more comprehensive understanding can be achieved by examining the possible motivations behind the actions of each hacker group. According to Hutchings' classification, these motivations can include curiosity, self-improvement, entertainment, the desire to feel power or demonstrate it, and seeking challenges. Other factors include striving for social status, ecological or political activism (hacktivism), financial gain, and external pressures exerted by terrorist or criminal organizations (Hutchings, 2013). Barber (2001) expands on this list by adding industrial espionage, cyber warfare, extortion, and fraud.

In his developmental model, van Beveren utilized Csíkszentmihályi's (2008) flow theory to map the motivations of hackers. The flow experience refers to a mental state in which one becomes so immersed in an activity that their attention becomes completely focused, time perception fades, and the activity itself brings a sense of joy and fulfilment. According to Beveren, hackers often enter this state of flow during their activities, which helps them develop a sense of control, enhances focus, and amplifies their curiosity. This, in turn, drives them toward continuous improvement. While Beveren distinguishes between various motivations—such as an internal compulsion to hack, curiosity, a desire for power and control, and the recognition of peers—he also notes that the developmental process fuelled by the flow experience can alter their original intentions and motivations over time (Beveren, 2001). This classification diverges somewhat from reality as it idealizes hackers and overlooks motivations that stem from the traditional world, particularly those of a financial

nature. However, its strength lies in capturing the characteristics of a subculture, as most hackers are indeed driven by these factors, and the flow experience is an undeniable aspect of their environment. For many hackers, hacking is perceived as a kind of game, where the classic elements of gamification—personal, mechanical, and emotional—are present (Xu et al., 2021). The emotional element manifests as the flow experience, generating a sense of happiness reinforced by positive feedback.

The motivations driving hackers can encompass a broad range of activities. These can include breaking into an information system, accessing, modifying, or destroying data, rendering systems inaccessible, leaking obtained information, or misusing personal, economic, research, or innovative data. At the most severe level, such motivations can lead to full-scale attacks on critical infrastructure. Actions carried out in cyberspace by individuals driven by these motives pose significant challenges not only for states but especially for economic organizations. The severity and societal impact of these actions span a wide spectrum: a cyberattack carried out for fun or as a challenge differs substantially in effect from large-scale fraud, financially motivated crimes such as theft, extortion, or espionage, or attacks targeting the disruption of essential state functions. Aligning responses to this scale is crucial for determining appropriate economic, legal, and organizational countermeasures. This includes defining the roles and responses of internal departments, identifying areas of collaboration with law enforcement and national security agencies, and implementing targeted legal and operational steps. It has of paramount importance to address motivations that endanger one or more functions of economic actors—especially those impacting production, administration, customer data, and the integrity of R&D-related data. Ensuring the uninterrupted operation of these networks is critical to maintaining daily economic and operational mechanisms.

Max Kilger, in his so-called MEECES theory, identified six distinct motivations: money, ego, the desire to join a social group (entrance to social group), personal causes (cause), as well as entertainment and status (Kilger, 2015). The Singaporean authors, building on this framework, identified seven distinct motivations: curiosity, financial gain, reputation, revenge, recreation, ideology, and sexual drive (Chng, 2022).

One of the most comprehensive motivational frameworks was developed by a trio of authors at the request of the United Nations Interregional Crime and Justice Research Institute (UNICRI). According to this framework, hackers can be driven by multiple motivations simultaneously, including curiosity, a love of technology, a desire to prove oneself, entertainment, the need to solve problems, and the desire to improve technology or enhance the security of networks and systems. Other motivations include the protection of civil liberties, rendering services inaccessible, privacy protection, anti-system sentiments, rebellion against state authorities or one's environment, a sense of adventure, boredom, the desire to be seen as "cool", media attention, anger and frustration, and political causes (Chiesa et al., 2009). The advantage of this classification is that it also highlights the positive societal aspects of hacker activities, showcasing how some motivations can contribute to constructive or security-enhancing outcomes.

Nevertheless, it is appropriate to combine the classifications into a unified approach that merges overlapping categories. At the same time, it must be noted that certain motivations are not mutually exclusive, meaning that a hacker can be driven

by multiple motives simultaneously. This research distinguishes the following motivations: the desire to learn, curiosity, the pursuit of fame, entertainment, the sense of power, challenge, revenge, sexual drive, social/subcultural status, worldview (including religion, politics, ideology, and anti-system sentiments), financial gain, service to a nation-state, and protection of IT systems (see **Figure 1**) Kelemen (2023).

Hacker type/ motivation	desire to learn	curiosity	desire for fame	fun	sense of power	challenge	revenge	sexual instinct	social status	ideology	profiteering	serving the nation state	IT system protection
script kiddies	-	+	+	+	+	+	-	-	+	-	+	-	-
student	+	+	-	+	-	+		-	+	-	-	+	+
cyberpunk	-	+	+	+	+	+	+	-	+	+	+	-	-
old guard	-	+	+	-	-	+	-	-	+	+	-	+	+
malicious insider	-	-	-	-	+	+	+	-	+	+	+	-	-
petty thief	-	-	-	-	-	-	-	-	-	-	+	-	-
pros	-	+	+	+	+	+	+	-	+	+	+	+	+
hackers of nation states	-	-	-	-	-	-	-	-	-	+	+	+	+
hacktivista	-	-	+	-	-	-	-	-	+	+	-	-	-
cyber predator	-	-	-	+	+	-	-	+	-	-	+	-	-
digital pirates	-	-	-	+	-	-	-	-	+	-	+	-	-
crowsourcere	-	-	-	-	-	-	-	-	-	-	-	+	+
cyber accomplices	-	-	-	-	-	+	-	-	+	-	+	-	

Figure 1. Motivational classification of hacker types (edited by Kelemen).

When comparing hacker motivations with their impacts on cybersecurity and the key characteristics of hybrid conflicts, it becomes clear that hackers can be effectively mobilized to advance geopolitical interests. This is exemplified by the WannaCry and NotPetya attacks linked to North Korean and Russian hackers, respectively, which caused significant economic damage. Hackers also play a prominent role during military confrontations and hybrid scenarios, as seen in the Russia-Ukraine war, where both sides employed freelance hackers, with particular attention given to the establishment of Ukraine's IT Army.

Equally concerning is the threat hackers pose to economic actors (often in connection with geopolitical conflicts) and individuals. Hacktivists, driven by societal and political fault lines, are particularly prone to targeting economic organizations with malicious cyber activities, sometimes even directly (That et al., 2024). Hacktivists primarily aim to represent political, social, or religious ideologies. They are not driven by financial gain but by the desire to draw attention to a specific cause. Certain hacktivist groups, such as Anonymous, openly invite individuals to join their operations. Common methods include DDoS attacks, data leaks, deface attacks, and information warfare. The latter often involves spreading disinformation, which manipulates public opinion or discredits an organization. These actions can effectively serve the objectives of terrorist groups. Hacktivists frequently operate along similar ideological lines and support narratives that align with terrorist propaganda. Additionally, they may provide technological support that facilitates terrorist

activities, such as leaking sensitive information (e.g., revealing government or military targets) or managing digital funds (e.g., cryptocurrencies or other DeFi platforms). Furthermore, their activities can assist in the recruitment efforts of terrorist groups. It is also not uncommon for hacktivists to conduct DDoS attacks or website breaches as distractions, enabling terrorist acts to be carried out without interference (Kwaku, 2022). In 2015, a group sympathetic to the Islamic State, known as the Cyber Caliphate, hacked the Twitter account of the United States Central Command (CENTCOM), posting propaganda videos and threats. Although the attack was not technically significant, it received widespread attention, contributing to the group's recruitment efforts. The "Asrar al-Mujahideen" (Secrets of the Mujahideen) encryption tool used by Al-Qaeda was built from algorithms known in hacktivist circles and aimed to enhance communication security.

The rapid advancement of technology, including artificial intelligence (AI), plays a significant role in enhancing these activities. AI allows for the automation of operations, increasing their efficiency and effectiveness. With the help of AI, data analysis becomes faster and can cover larger datasets. Deepfake technologies have elevated the production of content supporting terrorist propaganda to new levels, enabling the creation of fake videos and audio recordings aimed at political destabilization. Furthermore, AI contributes to greater effectiveness in cryptography. It facilitates the development of complex encryption systems that protect communication between hacktivists and terrorist groups (Esmailzadeh and Motaghi, 2024).

Actors motivated by financial gain may, alongside their "ordinary" criminal activities, contribute to the controlled chaos required by state actors orchestrating hybrid attacks. With external support, they can inflict financial damage ranging from minor to severe, targeting economic organizations or mass numbers of users. It is also possible that controlled chaos itself is exploited to maximize the efficiency of their operations.

Since a malicious actor's toolkit naturally includes the ability to harm the economic environment alongside political objectives, it is a logical strategy to undermine trust in today's heavily digitalized economy and commerce. By eroding consumer and investor confidence, these actors pave the way for further economic disruption and chaos.

Additionally, it is important to note the two-way interaction between cyberspace and the physical world: not only does cyberspace influence traditional environments, but processes in the physical world also manifest within cyberspace. As a result, illegal groups operating in the physical world—such as organized crime syndicates and terrorist organizations—increasingly carry out cyber activities or use cyberspace to support their traditional operations.

3. Discussion

The result of the research clearly show that the grouping of hackers and the analysis of their motivation is crucial to understand cyberterrorism. Due to the specific nature of this phenomenon, which requires special technical skills and targeted intent, certain types of hackers are primarily link to this criminal offence.

Cyberpunks, who have high-level technical skills to allow attacks against critical infrastructures or other protected systems with the aim to destabilize the public order, may easily turn to become perpetrators of cyberterrorism. These actors may take part in a cyberterrorist attack by using their illegal activities motivated by financial, political motives. "Hacktivists" directed by political or ideological aims may be inclined to commit acts directly linked to cyberterrorism along the lines of social tensions.

The further analysis of the motivations also shows that ideological and political goals, the desire for revenge, often meet the tools of cyberterrorists. Furthermore, financially motivated hackers may also support terrorist organisations indirectly, for example by generating funds or weakening security systems.

The results fit well previous studies, while clearly demonstrating that the skills and motivations of hackers may open new dimensions in the context of cyberterrorism up. The "WannaCry" and "NotPetya" attacks, as well as hacker's activities in geopolitical conflicts such as the Russian-Ukranian War (e.g., creation of the "IT Army") illustrate the mobilisation of hackers for state and non-state terrorist purposes.

Therefore, the hackers' activities constitute a double challenge: on the one hand, their technical skills make them enable to find and attack the vulnerabilities of state and economic systems, and on the other hand, their political, ideological or financial motivations link them to the target system of cyberterrorism. Social disruption, destabilisation of critical infrastructures and incitement to panic are objectives that fit directly into cyberterrorist strategies.

An important focus for further research is to explore the links between hackers and cyberterrorism, in the following areas:

- Technical capacity and perpetrator's profile analysis: how does the hacker's technical knowledge relate to the type and impact of attacks?
- State-sponsored hacking: how can hackers become an integral part of geopolitical conflicts?

These research directions can help to refine cybersecurity strategies and make the fight against cyberterrorism more effective. Mapping the motivations and skills of hackers will not only allow a deeper understanding of the phenomenon itself but will also provide a basis for targeted prevention and countermeasures.

4. Conclusion

The results of the research show that cyberterrorism is intertwined with the activities of different groups of hackers, who may become potential perpetrators based on their technical knowledge and motivations. Their attacks are targeted to exploit vulnerabilities in critical infrastructures and to destabilise the social order for political or ideological purposes. Actors seeking financial profit can indirectly support cyberterrorist organisations by providing them with funds.

The mapping of the links between motivations and activities shows that the technical capabilities and goals of hackers broaden arsenal of cyberterrorism tools. State-sponsored hacking activities and their mobilisation in geopolitical conflicts are particularly challenging, as the example of Russian-Ukranian war shows it. A deeper

analysis of these links and the development of appropriate preventive and defensive strategies can be considered as a crucial task for future research.

Author contributions: Conceptualization, RB and RK; methodology, RB and RK; investigation, RB and RK; resources, RB and RK; writing—original draft preparation, RB and RK; writing—review and editing, RB and RK; supervision, RB and RK. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Allahrakha, Naeem (2024): Global Perspectives on Cybercrime Legislation. Journal of Infrastructure, Policy and Development Vol. 8. Issue 10., 1-20.

Atkinson, Sean (2015): Psychology and the hacker – Psychological Incident Handling. SANS Whitepaper, 2015 4–9.

Barber, Richard (2001): Hackers Profiled – Who are they and what are their motivations? Computer Fraud&Security, Vol. 2 15.

Bartkó, Róbert – SÁNTHA, Ferenc (2023): A kibertér műveletek büntetőjogi értelmezésének lehetőségei. Military and Intelligence Cyber Security Research Paper Vol. 2. 1-30.

Brenner, Susan, W. (2006): Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal Vol. 3. 453-471.

Brenner, Susan, W. (2007): Re-thinking crime control strategies. In. Jewkes, Yvonne (ed.) Crime Online. Willan Publishing: Cullompton, UK 12-28.

Chang, Samuel – HAN YU, Lu – AYUSH, Kumar – DAVID, Yau (2022): Hacker types, motivations, and strategies: A comprehensive framework. Computers in Human Behavior Reports, Vol. 5., 3.

Chiesa, Raoul – DUCCI, Stefania – CIAPPI, Silvio (2009): Profiling Hackers - The Science of Criminal Profiling as Applied to the World of Hacking. Boca Raton, Taylor & Francis Group: London EN

Choi, Kyung-schick; LEE, Claire Seungeun (2018): The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. International Journal of Cybersecurity Intelligence and Cybercrime Vol. 1. Issue 1., 1-4.CSÍKSZENTMIHÁLYI, Mihály (2008): Flow: The Psychology of Optimal Experience. Harper Perennial: New York, London, USA-EN

CSIS Significant Cyber Incidents since 2006 (https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-12/241210_Significant_Cyber_Events.pdf?VersionId=6M4z53qCe64xZ4cFQd7nkkTFPrQmeLPB)

Director General Ken McCallum gives latest threat update (2024) Available online: https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update (accessed on 28 December 2024),

Esmailzadeh, Yaser – MOTAGHI, Ebrahim (2024): International Terrorism and Social Threats of Artificial Intelligence. Journal of Globalization Studies Vol. 15. Issue 1. 168-179.

Farkas, Ádám (2018): Gondolatok a 21. századi biztonságról, államról, védelemről. Hadtudomány, Special Issue, 241-256.

Federa Bureau of Investigation Internet Crime Report 2021. Internet Crime Complaint Center Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 28 December 2024),

Federa Bureau of Investigation Internet Crime Report 2023. Internet Crime Complaint Center Available online: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf (accessed on 28 December 2024),

Gillespie, Alisdair A. (2016): Cybercrime – Key Issues and Debates. Routledge 107-111. New York NY US

Gordon, Sarah – FORD, Richard (2006): On the Definition and Classification of Cybercrime. Journal of Computer Virology, 2(1) 13-20.

Hutchings, Alice (2013): A Qualitative Analysis of Online Offending and Victimisation, In. Karuppannan Jaishankar – Natti Ronel (ed.): Global Criminology: Crime and Victimization in a Globalized Era, CRC Press: London EN 95.

Kazári, Csaba (2003): Hacker, cracker, warez. A számítógépes alvilág titkai. Panorama: Budapest, HU, 18.

Kelemen, Roland (2023): Hacker – Az egyén mint a kibertér aktív szereplője. In: FARKAS, Ádám & KELEMEN, Roland: Nemzeti biztonság és kibertér. Médiatudományi Intézet. pp. 59-69.

Kelemen, Roland (2023): The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. Connections: The Quarterly Journal Vol. 22. Issue 2., 75-90.

Khalaf, Tahat, MOHAMMED, Habes, AHMED, Mansoori, NOURA, Naqbi, NAIJA, Al Ketbi, IHSAN, Maysari, DINA, Tahat, ABDULAZIZ Altawil (2024): Social media algorithms in countering cyber extremism: A systematic review. Journal of

Infrastructure, Policy, and Development 8(8) 1-12 KILGER, Max (2015): Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios, In. 10th International Conference on Availability, Reliability and Security

Kunos, Imre (1999): A számítógépes bűnözés. Belügyi Szemle, Vol. 11. 28-42.LOBACH, Dmitriy (2022): Cyberterrorism as an Atypical Manifestation (form) of Terrorism in the Modern World. Advances in Law Studies Vol 10. No. 3., 36-40.

Kwaku, Thimothy (2022): Securing Critical National Infrastructure Against Hacktivist. Advances in Multidisciplinary and scientific Research Journal Publication Vol. 10. Issue 4., 33-42.

Long, Larissa April: (2012): Profiling Hackers, Sans Institute Reading Room, 26th January 2012, 4–6.

Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., et al. (2022). Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Sage Open: Nigeria, 12(3). https://doi.org/10.1177/21582440221122739.PHILLIPS, Kirsty – DAVIDSON, Julia, C. – FARR, Ruby, R. – BURKHARDT, Christine – CANEPPELE, Stefano – AIKEN, Mary, P. (2022): Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2) 379-398.

Panda mediacenter. 14 Types of Hackers to Watch Out For. Panda/mediacenter, 2021 (https://www.pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for/)

Sarre, Rick – LAU, Yiu-Chung – CHANG, Lennon, Y. C. (2018): Responding to cybercrime: Current trends. Police Practice and Research, 19(6), 515–518.

Shea, Sharon: Types of hackers: Black hat, white hat, red hat and more, TechTarget, SearchSecurity (https://www.techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking)

Taken Smith, Katherine – SMITH, Lawrence Murphy – BURGER, Marcus – BOYLE, Erik S. (2023): Cyber Terrorism Cases and Stock Market Valuation Effects. Information and Computer Security Vol. 31. Issue 4., 385-403.

Terrorism Financing in Australia – National Risk Assessment. Available (2024) online: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Terrorism%20Financing%20NRA.pdf (accessed on 28 December 2024),

Terrorism Situation and Trend Report 2024 -EUROPOL (https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf)

Turovszkij, Danyil (2020): Orosz hekkerek – Így lettek lázadókból Putyin katonái. Athenaeum: Budapest, HU

Van Beveren, John (2001): A conceptual model of hacker development and motivations. Journal of E-Business, Vol. 2.

Wall, David, S. (2001): Introduction: Cybercrime and the Internet. In. Wall, David, S. (ed.) Crime and the Internet. Routledge: New York, NY, USA, 2.

Xiong, Zhang – ALEX, Tsang – T. WEI, Yue – MICHAEL, Chau (2015): The classification of hackers by knowledge exchange behaviours, Information Systems Frontiers, Vol. 6, 1245.

Xu, Joy – AARON, Lio – HARSHDEEP, Dhaliwal – SORINA, Andrei – SHAKTHIKA, Balakrishnan – UZHMA, Nagani – SUDIPTA, Samadder (2021): Psychological interventions of virtual gamification within academic intrinsic motivation: A systematic review. Journal of Affective Disorders, 21(10)., 444–465.