

CYBER TERRORISM - MODERN SECURITY THREAT

Drazan Erkić¹, Miroslav Baljak²

¹Ministry of Internal Affairs of the Republic of Srpska, PU Zvornik, St. Sava no.126, Zvornik, Republika Srpska, Bosnia and Herzegovina, Faculty of Security Sciences, University of Banja Luka, drazan.erkic@hotmail.com, ORCID ID [0009-0005-0805-696X](https://orcid.org/0009-0005-0805-696X)

²Ministry of Defense of Bosnia and Herzegovina - Armed Forces of Bosnia and Herzegovina, Serbian Volunteer Guard bb, Bijeljina, Republika Srpska, Bosnia and Herzegovina, baljak.miroslav@gmail.com, ORCID ID [0000-0002-4961-8253](https://orcid.org/0000-0002-4961-8253)

Digital Object Identifier (DOI): [10.70995/RGFI5335](https://doi.org/10.70995/RGFI5335)

Article Category: Scientific paper

Article Type: Review paper

Received: 6th August 2025

Accepted: 5th September 2025

Abstract: *The security threat of terrorism and terrorist acts has been present since ancient times. Today, the world is afraid of cyber terrorism, which is a frequent form of endangering the safety of people and society as a whole. The consequences of this criminal and illegal act are very large and cause great concern for everyone, from citizens, businessmen to state institutions. Attacks by cyber terrorism on the state apparatus and its institutions are of particular concern, creating a feeling of insecurity among citizens, but also mistrust in the institutions and authorities that can protect them. In this paper, the theoretical approach to the phenomenon of cyber terrorism, i.e. its conceptual definition, and the motive for its execution will be pointed out. Also, the targets of the attack will be pointed out, as well as the structure of the terrorists and their training.*

Keywords: *security threat, terrorism, cyber terrorism, cyber space, modern society.*

1. INTRODUCTION

Each period in the development of human society is associated with a certain progress and improvement of the quality of human life. It is natural that man strives to develop and improve in all spheres of socio-political life. All this development of society is directly related to the development of security, because the state of security is a prerequisite for any other development and progress. We have witnessed that throughout the ages, security has been threatened by various forms of threats, from tribal conflicts, fighting for food and territory, through war and other types of conflict, to today's era, which is a product of globalization and the emergence of the Internet. Increasingly, today, due to the rapid development of science and technology, security is threatened by various cyber attacks. Cyber attacks, i.e. criminal activities in cyber space, are on the rise today. This new form of criminal activity is directly related to technological innovations and uses various tools that threaten security. From the aspect of endangering security by cybercriminal activities in cyberspace, there are many different threats, among which cyberterrorism stands out in particular. Cyber terrorism today is a serious security threat and a global problem of modern society. A particular concern of cyber terrorism is reflected in its unpredictability and the selection of attack targets. The targets of attacks are diverse, from individuals and their property to state institutions and the state and its values. In the context of the damage caused by this criminal act, i.e. cybercrime basically, as well as the difficulties in its prosecution, the opinion of Antonovic is valuable. According to this author, "only in the last few years, the economic damage of cybercrime is measured in billions of US dollars. The number of

cyberattacks on critical infrastructure has increased dramatically. Almost five billion Internet users are potential victims of cybercriminal attacks. The development of information technologies and the increasing dependence of society on new forms of communication based on the Internet increase the danger of cybercrime. Most cyberattacks remain undetected or unreported, which further complicates the prosecution of perpetrators" (Antonovic, 2023: 7-8). Attacks in cyberspace today are the subject of interest for many, especially the security services. In the focus of interest today is especially cyber terrorism, as a phenomenon that is still not sufficiently researched and defined. Today, special emphasis is placed on terrorist activities in cyberspace. Regarding the above, Putnik is of the opinion that "after the terrorist attack on the Twin Towers in 2001, security analyzes put special emphasis on terrorists and issues related to the transmission of terrorism into cyberspace, i.e. its misuse for terrorist communication, propaganda and psychological warfare, financing of terrorist activities and other purposes" (Putnik, 2009: 12). The very development of society, and therefore of new technologies, should be mutually connected with the security system, that is, new technologies, as well as new threats to security resulting from the development of new technologies and the Internet itself, must be the starting point for building a security strategy and defense. In the context of the above, the view of Sanja Klisarić is valuable, who states the following "namely, it is logical to consider that the development of technologies must also follow the development of security systems and defense against threats that threaten the Internet. The task of security systems and security services is not only to monitor the development of new technologies, but also to implement adequate defense" (Klisarić, 2021: 248). When talking about the very outcome of cyber terrorism as a serious security threat, many agree that the outcome is disastrous and disturbing. Thus, speaking about the very scenario of cyber terrorism, Votel believes that "scenarios with threats of cyber terrorism include paralyzing large urban areas, the health system or disrupting the financial sector "by changing a few units and zeros"" (Votel, in Klopfer et al., 2000:15).

2. CYBER TERRORISM - TERMINAL DISCOURSE

Cyber terrorism is a form of terrorism that is more recent and belongs to a new security threat about which little is known and which, at least for now, has not been sufficiently investigated. With the process of globalization, and especially with the emergence of the Internet and new technologies in use, the issue of cyber terrorism is becoming more and more topical and is receiving more and more attention, both from the professional public and from the public in general. According to Luknar, "cyber terrorism is a specific form of terrorism, not only because of the means used by cyber terrorists, but also because it takes place in a specific environment - a virtual one, where there are online means and principles, where events and dangers in cyberspace remain imperceptible in the real physical world, and its consequences and the damage caused can directly affect people's daily lives, the media, public opinion, infrastructure and security" (Luknar, 2022: 47). With the emergence of cyber terrorism, new questions about security itself appear. According to Antonovic, "cyber terrorism was first mentioned at the end of the 20th century. The cyber revolution has raised the issue of cyber warfare and information security. This is where the idea that terrorists can use the cyber environment for their activities came from. Already in 1991, the American National Research Council warned that future terrorists could do more damage with a keyboard than with a bomb. The security services singled out cyber terrorism as a threat to national security and defined it as a planned, deliberate, politically motivated attack on information, computer systems and data with the aim of causing fear and the threat of violence to civilians" (Antonovic, 2023: 44). Like security itself, cyber terrorism is very difficult to define, and the difficulty is whether it can be brought under a separate phenomenon or whether it can be linked to information and the war for it. The fact that with

the passage of time the definition of cyber terrorism is being expanded and supplemented, but it should be emphasized that there is still no single and unified definition. Nevertheless, regardless of its non-unification, it is worth seeing its determination from the point of view of individual authors. Thus, according to Wilson, cyber terrorism is "the use of computers, as a weapon and as a target, by groups, international or subnational perpetrators or perpetrators with political motivation, who threaten violence or commit violence and cause fear with the aim of influencing the public or imposing a policy change on a particular government" (Wilson, 2005:7). A somewhat different definition of cyber terrorism is given by Antonovic, who believes that "cyber terrorism implies cyber attacks on critical systems and their control systems, with the aim of causing damage and spreading fear among people. Cyber terrorism aims to create both at the national and international level and represents a new form of terrorist opportunities that are available through the use of new technology and networks. This, among other things, allows terrorists to carry out attacks almost without any physical risk to themselves" (Antonovic, 2023: 44-45). A more extensive definition of cyber terrorism was offered by Dorothy Denning, according to which cyber terrorism is linked to cyber space. According to her view, cyber terrorism means "attacks or threats of attacks against computers, networks or information stored in them, in order to intimidate and force governments and society to fulfill political, religious or ideological demands" (Denning, 2001). In the context of a terrorist goal, the definition of cyber terrorism is somewhat different. Thus, according to Petrovic, cyber "an act of computer (cyber) terrorism could be defined as the use of information resources in the form of a threat or blackmail in order to achieve a certain terrorist goal. What is missing from the act defined in this way is one element of terrorism: the use or threat of use of physical violence, so the mentioned definition is based on the assumption that in the information environment, putting the public in a state of fear is no longer necessary, nor is it necessary to destroy property and use violence against people in order to achieve certain terrorist goals. therefore, the main goal is disruption instead of destruction, although it is not excluded either, because in societies highly dependent on information technology, disruption of information systems can cause short-term problems of varying scope and intensity, but also much more significant, long-term loss of confidence in the ability and reliability of these systems" (Petrovic, 2001:345). It is evident that cyber terrorism is closely related to cyberspace. According to Tepsic and Tanjga, "cyberspace is understood as either a type of "community" made up of a network of computers in which elements of traditional society are found in the form of bytes or bits, or "the space created by computer networks"" (Tepsic, Tanjga, 2011: 268-269).

3. MOTIVATING FACTORS FOR THE EXECUTION AND TARGET OF THE ATTACK

There are many reasons why individuals and groups decide to commit cyber terrorism in order to achieve certain goals. Some of the most common and common motives are primarily of a political, ideological, religious and financial nature. The process of globalization and the emergence of the Internet gave birth to other motives related to the virtual space. There are certain factors that influence individuals or groups to decide to commit cyber terrorism, but there are also factors that can deter individuals and groups from committing it. Thus, according to Putnik, and as indicated by the analysis of the Center for the Study of Terrorism and Unconventional Warfare, "it identifies four determining factors for the motives for which a terrorist group may opt for a strategy of cyber terrorism:

- Global networking increases the number of goals that can be reached through cyberspace.

- The dependence of a developed society on information technologies, on the one hand, brings new vulnerabilities, and on the other, it maximizes the possible effects of cyber terrorist actions.

- Insufficient cooperation at the international level and inconsistency of national codes in the field of cybercrime give potential aggressors immunity. In cases where it is possible to identify the perpetrators, the issue of jurisdiction over the tort remains open - whether the jurisdiction is the state from which the attack was committed or the state where the consequences of the attack manifested themselves.

- Expenditures for the preparation and execution of a cyber terrorist attack, compared to other strategies, are significantly lower" (Putnik, 2009:156-157).

Unlike the motivational factors that make individuals or groups opt for cyber terrorism, there are factors that dissuade them from the idea. According to the same author, and according to the Center of the same name, there are "arguments that can dissuade terrorists from the strategy of cyber terrorism:

- Terrorists have many strategic options at their disposal. Seen from that perspective, the usefulness of cyber terrorism might be marginal.

- Cyber attacks can cause interruptions of certain services, but they do not have the ability to cause destruction on a wider, global level.

- The main consequences of cyber attacks can be financial losses, losses of confidential or private information, losses of reputation and trust, but in most cases the consequences of attacks do not endanger human life. Of course, one can imagine a scenario in which a general interruption of vital services indirectly leads to human casualties. However, even in that case, the question remains open to what extent the physical and psychological damage caused by cyber terrorism attacks is comparable to the effects of traditional terrorist methods.

- Growing awareness of the vulnerability of cyber infrastructure leads users of information and communication technologies to continuously improve their own defense systems. This means that the potential victim's readiness for attacks and his ability to defend himself in the future require greater expenditures for the aggressor.

- The effects of a cyber terrorist attack are difficult to predict, not only in terms of physical damage but also in terms of its impact on public opinion. The idea that one can put pressure on an opponent just by threatening to break serve seems, at least in most conceivable scenarios, frivolous. Interruption of services seems an inadequate alternative to destruction. Given such circumstances, terrorist organizations, especially those with limited resources in terms of knowledge and finances, would probably not choose a strategy of cyber terrorism" (Ibidem, pp. 157-158).

It is evident that cyber terrorists have both motivational factors and factors that deter them from committing cyber terrorism. From the aspect of preventing and detecting cyber terrorism, it is necessary to point out the targets of cyber terrorist attacks. According to Antonovic, "targets of cyber terrorists can be:

- the integrity of information, for example, unauthorized deletion, unauthorized data changes and the like, resulting in a loss of trust in information and communication technologies and state institutions.

- targets can be databases that are critical to society, such as personal records, vehicle registration, property ownership and financial statements and accounts.

- confidentiality of information, breaches of privacy and theft of confidential information on a large scale can create disruptions in the provision of services. For example, the release of health records of people infected with HIV could trigger a series of harassment and suicides. The government's response may further violate citizens' privacy and result in increased fear and mistrust of citizens in state institutions.

- availability of services based on information and communication technologies. For example, a long-term attack, an unauthorized interruption of systems and networks, or a physical or electromagnetic attack on databases and critical components of information and communication systems can slow down or disable the delivery of services to the population" (Antonovic, 2023: 45-46).

Comparing the targets of standard and cyber terrorism attacks, there are evidently certain differences. Thus, according to Nelson et al. "the number of potential targets is much higher than in standard terrorism, and thus the audience is larger. The financial and time costs are much lower, and the possibility of controlling and spreading ideology is much more widespread. Second, there is an increasing dependence on computer technology. Terrorists can find or acquire their financial support to a greater extent than ever before, and the consequences of attacks are more widespread. Although there are conventions on cyber terrorism, the lack of legal consensus allows attackers a safe haven. Also, complications arise when the identity of the attacker in cyberspace needs to be determined space, which contributes to the turn to cyber terrorism" (Nelson et al., 1999: 24-30).

4. STRUCTURE AND QUALIFICATIONS OF TERRORISTS

From the aspect of the fight against cyber terrorism, it is necessary to know the structure and their perpetrators. Perpetrators of cyber terrorism can be individuals as well as groups. In cyberspace there are several structures, that is, organizational forms, most often we talk about some four forms. According to Putnik, "in the first place, we are talking about individual cyber terrorists. Many of the known viruses spread in cyberspace were created by individuals. Individuals who create malicious programs usually do so for the sake of adventure and intellectual challenge, and not for the purpose of causing physical violence. However, it is redundant to assume that there can be a combination of hacking abilities and psychopathological traits in one person. In destructive individuals, there is a pathological desire to cause death, material damage and fear among population. The combination of knowledge and pathology would, metaphorically speaking, correspond to the psychological profile of a terrorist like McVeigh. The threat of an individual terrorist attack cannot be assessed as extremely high, since there is a lack of empirical evidence to support it. Theoretical considerations of cyber terrorism pay special attention to information terrorist groups composed of technical well trained members.

By grouping together, pooling knowledge and skills, extremists would be able to carry out well-coordinated cyber terrorist organizations. Such groups can be considered a more serious threat compared to individual cyber terrorists, because they have proven their capacity to carry out criminal actions. The ability of small terrorist groups to independently develop software applications causes fear in security circles that these groups could move on to more destructive goals. Large terrorist organizations such as Al Qaeda, with a documented history of physical aggression, represent the third category of potential actors on the cyber terrorist track. As we have shown before, most of them are present in cyberspace, where they carry out various activities. In the last category we can classify groups that are sponsored or supported by governments to conduct information warfare against enemy states. A distinction can be made between these groups on the basis of their origin and competence. Certain countries are forming, at the official level, units for cyber warfare, with the aim of

executing offensive and defensive data. Strictly speaking, they should not be classified as cyber-terrorist groups, but they are extremely similar on the scale of gradation of potential damage. It can be stated that, in the field circumstances, the activities of these military units are implicitly hindered by the publicity brought about by frequent international discussions about this phenomenon. Thanks to this, attacks on the opponent's systems are not carried out, at least not publicly" (Putnik, 2009:159-161). The very success of the terrorist action against the chosen target depends on the training and competence of the persons who carry out cyber attacks. In addition to individual, personal characteristics and skills, cyber terrorists must master new techniques and technologies in cyber space, as well as have an obligation to constantly monitor innovations in this area. On the other hand, the way to detect cyber terrorists and their activities in cyber space, depends on the training and special knowledge and skills of members of the security system, who deal with this problem. Also, the success of the security service in preventing cyber terrorism as a modern threat to security depends to a significant extent on international connectivity, data exchange, education, and compliance with legal regulations in this area.

5. CONCLUSION

Today, cyberspace has become a place where everyone works, both individuals and legal entities, as well as state and governmental institutions, so the possibility of threats is becoming more certain and more frequent. Frequent threats to individuals, legal entities and institutions also come from cyber terrorism. The targets of cyber terrorism are diverse and very often unpredictable. Cyber terrorists are constantly improving and showing their creativity in cyberspace. The vulnerability of cyberspace is evident, which is especially contributed to by a kind of irresponsible attitude of modern man towards this security threat. What particularly favors cyber terrorists is the lack of clear rules and procedures related to information security, but equally, no less important is the lack of awareness among citizens about the threat of cyber terrorists, insufficient and inadequate training of citizens, as well as the lack of digital hygiene in cyberspace. The fight against cyber terrorism should be reflected in the very risk assessment and the very threat to citizens, society and its values. Based on the assessment, look at the shortcomings in the security system itself, and based on that, adopt preventive and proactive measures. Successful activity in preventing cyber terrorism implies active international cooperation of specialized bodies and organizations, as well as high-quality cooperation and coordination of the state and private sectors. Investment in cyber security is a need of today's society, especially investment in human resources and means of work. Constant monitoring and analysis of cyber terrorism should serve the purpose of training professional staff in the fight against this security threat, as well as be the basis for building an adequate cyber protection program. Attacks in cyber space, especially on state institutions and authorities, create special concern among citizens, fear and mistrust. The process of globalization, as well as the accompanying activities related to globalization, are also reflected in threats to cyberspace. Protecting cyber space from various forms of threat, including cyber terrorism, is everyone's obligation, but also a condition on which the functioning of today's modern society depends. The time ahead of us will continue to be marked by the accelerated development of science and technology, the emergence of new sophisticated methods and tools for working in cyber space, and the logical conclusion is that some new forms of threats will appear in cyber space, above all innovations in the execution and realization of cyber terrorist activities. In step with the development of technology and society in general, it is necessary to develop the security sector itself, contributing to the needs of modern man.

LITERATURE

Antonovic, R. (2023). Cybercrime as the crime of today. Center for Strategic Analysis, Belgrade.

Denning, D. (2001). Is Cyber Terror Next? <http://www.ssrc.org/sept11/essays/denning.htm>

Klisaric, S. (2021). Cyber terrorism as a trigger for the ever-increasing need for system security from the dangers that come from the Internet. Belgrade, Megatrend University, Megatrend Review, Vol. 18, No. 2, 2021, p. 247-256.

Klopfer, F. and others. (2000). Introduction to Cyber Security Management - A Handbook for Members of Parliament. DCAF, Geneva Center for Security Sector Governance.

Luknar, I. (2022). Cyber terrorism - Measures for suppression and prevention. Institute for Political Studies, Belgrade.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyberterror Prospects and Implications.

Petrovic, S. (2001). Computer crime. Security, Ministry of Internal Affairs of the RS, Belgrade.

Putnik, N. (2009). Cyber space and security challenges. Faculty of Security, University of Belgrade, Belgrade.

Tepsic, M., Tanjga, R. (2011). Protection of information systems. College and BESJEDA, Banja Luka.

Wilson, C. (2005). Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service – The Library of Congress, <http://fpc.state.gov>