sciendo

The three faces of a digital attack: an analysis of cyber-crime, cyber-terrorism and hacktivism

Jadranka Stojanović

University of Sarajevo - Faculty of Criminology, Criminology and Security Studies
jadrankastojanovic@fkn.unsa.ba

Abstract:

In the modern digital age, the boundaries between crime, terrorism and hacktivism in cyber space are becoming increasingly blurred. Although the usual elements of violence, political motivation, threat and fear provide a line of continuity that runs through the long and complex history of terrorism, it should also be taken into account that technological innovation has created a new form of terrorism. In recent years, the matter of "cyber" terrorism has become very interesting, as a kind of form of computer crime. Cyber terrorism implies the use of information resources in the form of threats or blackmail in order to achieve a specific terrorist goal. In the focus of attention is the abuse of the Internet as the most important global communication network. The use of the Internet by terrorists can be threefold: as a weapon, as a means of communication between activists and as a medium for addressing the public.

Paper type: Non-research article

Received: October 20, 2025
Accepted: December 31, 2025

Citation: Stojanović, J. (2025). The three faces of a digital attack: an analysis of cyber-crime, cyber-terrorism and hacktivism. *Journal of Forensic Accounting Profession, 5*(2), pp 75 – 93

DOI: https://doi.org/10.2478/jfap-2025-0010

Precisely for these reasons, it is necessary to spread the culture of using computer technology, but attention should also be paid to the security culture. After an unsuccessful defense against a cyber attack, Internet forensics allows us to reconstruct the events in order to discover the attackers and their methods of operation. Given that it is an extremely complex matter, in the paper we also looked at the general determinants related to computer crime, computer terrorism and hacktivism.

Keywords: *cyber crime, cyber terrorism, terrorism, criminality, information and communication technology.*

1. Introduction

In the last few decades, the development of information technologies and the Internet has created new opportunities for communication, business and social participation, but at the same time it has opened the door to different types of digital threats. What opened the door to the possibility of computer technology being misused for different purposes is its rapid development, simplification of use, but also its availability to a wide range of users (Matijašević, 2010:852). Today, cyber attacks represent a complex phenomenon, which includes a wide range of activities - from classic cyber crime, through cyber terrorism, to hacktivism. Although these three forms of digital activities are often linked through the means they use, their motives, goals and legal status differ significantly (Brenner, 2010; Wall, 2007). Cyber crime refers to illegal activities that are carried out using computer systems and networks, with the aim of obtaining material benefits, stealing data or damaging systems (Holt & Bossler, 2016). Examples include identity theft, financial fraud, ransomware attacks and intellectual property theft. The field of misuse of information technology for terrorist purposes is very interesting, that is, in recent years, the matter of computer (cyber) terrorism has become very interesting, as a kind of form of computer crime, from which it differs in many respects. Cyber terrorism is defined as the use of information technologies to intimidate, destabilize or cause harm for political, social or military purposes (Arquilla & Ronfeldt, 1993:147). Cyber terrorists often target critical infrastructure, government systems or large corporations to achieve their ideological goals. Hacktivism is a relatively new phenomenon that arose in the 1980s from the meeting of hacker communities and activist technology enthusiasts. Its popularity increased in the late 1990s, it became especially famous with the appearance of the

collective Anonymous. Hacktivism represents the actions of individuals or groups in the digital space with primarily ideological or political motives. Hacktivists use attacks on networks and public systems to draw attention to a particular problem or express protest against certain policies, organizations or countries (Jordan & Taylor, 2004). The line between legitimate hacktivism and cybercrime is often thin, which poses a challenge for legal and security institutions. Abuse of the Internet is a fact that we face every day, and the most dangerous one is certainly that by terrorists. The Internet is primarily used for the purpose of spreading terrorist ideologies and encouraging the commission of a terrorist act, and as a platform for recruiting and training terrorists. They use the Internet both in preparation and during a terrorist attack when it serves as their communication infrastructure. By analyzing the available literature, real cases and international reports, this paper tries to point out the similarities in the attack techniques, but also the differences in the ideological and organizational background. Special emphasis is placed on the question of when hacktivism crosses the line of legitimate digital activism and becomes a threat to information systems and national security. The aim of this work is to contribute to a better understanding of digital threats and the need for a unique approach in the fight against them.

2. Cyber crime

It is impossible to define a computer (cyber) criminal with a unique and precise definition. It is "a general form through which various forms of criminal activity are manifested, a form that will become dominant in the future" (Parker, 1983:70). Namely, the difficulties in defining computer crime arise from the fact that it is a relatively new form of criminal behavior, but also from the fact that there is a great phenomenological diversity of this phenomenon, which can hardly be encompassed by a single definition. Therefore, it is necessary to have a very broad approach when defining this type of criminal behavior. The first definition of computer crime originates from 1979, given in the Criminal Justice Resource Manual on Computer Crime, and reads "computer crime is any illegal act for which successful prosecution requires good knowledge of computer technology". This point of view was widely adopted, it was immediately accepted, and even a few years later it was included in the Study on International Legal Aspects of Computer Crime in 1983 (Schjolberg, 1986). However, the most complete definition of cyber crime is given in the document "Crime related to the computer network" (Report of Committee II, Workshop on crimes related to the computer network) from the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, held in

Vienna from April 10 to 17, 2000 (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Vienna, April 10-17, 2000). The working group of experts in the content of the report by cybercrime means "crime that refers to any form of crime that can be committed with computer systems and networks, in computer systems and networks or against computer systems and networks" (Porobić & Bajraktarević, 2012:15). At the Tenth UN Congress on Crime Prevention and Dealing with Criminals, which was held in 2000, it was concluded that cybercrime appears in a narrower and broader sense. In a narrower sense, cybercrime can be seen as illegal behavior that is motivated by the electronic performance of the security of computer systems, as well as the data that is processed, while cyber crime in a broader sense is seen as illegal behavior that is connected to the network and computer system, and includes the illegal giving and sharing of information over the network and computer systems. Cyber crime is a form of crime where computer networks are used as a means of committing a criminal act. This type of criminal behavior is mostly carried out by individuals, while it is not uncommon for criminal organizations themselves to be involved in this type of crime, which results in unauthorized access to confidential information, as well as its publication. Cyber crime changes computer data, contains a wide range of illegal activities, including unauthorized access to a computer network as well as juvenile pornography, misuse of payment cards, but also criminal acts that threaten the safety of Internet users.

2.1. Definition of cyber crime

In today's world, the term "cyber" is used more and more, without actually knowing what it means. The term "cyber" first appeared in military terminology, in the sense of predicting future forms of warfare. "Cyber war" represents warfare with knowledge, that is, information. It is a high-tech war, which refers to the collection of confidential information (Gligorević, 2014:164). Cyber war is an event that takes place in cyber space and has elements of conventional war. Some theoreticians believe that the Orchard operation, which Israel used by activating components built into the information system so that Syrian radars would not be able to detect Israeli aircraft on Syrian territory, was a cyber war. Proponents of increased budget allocations for training the US military to conduct operations in cyberspace often try to convince the public that the cyber war has already begun, using the "cyber Pearl Harbor" metaphor. However, while there is no doubt about who, when, where and how carried out the actual attack on Pearl Harbor, nor about the immediate and long-term consequences that this attack had on the course and outcome of World War II, there is no agreement about who and

when carried out the “cyber Pearl Harbor”, or whether it even happened. The credibility of this metaphor, which was put into circulation in the 1990s, was significantly reduced by the terrorist attacks on New York and the Pentagon on September 11, 2001. Everyone saw those attacks and the number of their victims is measured in the thousands. There are no visible devastating consequences and human victims of cyber-attacks, and therefore it is difficult to convince the public that a cyber-war has already begun (Kovačević, 2013:92). The word cybernetics does not have the same meaning as the word cyber. Cyber in the dictionary of foreign words denotes the basic matter that is connected to the world of imaginary reality created via computers. Cybernetics can be defined as "the systematic study of communication and management in organizations of all kinds" (Deutsch, 1966:76). It is a very difficult path to track down criminal perpetrators who use a specific method, as well as a means of committing a criminal act of cybercrime using a computer. The persons who engage in these illegal activities are, for the most part, students, IT experts, former inspectors of criminal services and many others who are well versed in modern technology (Gligorević, 2014:166).

The term cyber crime can be defined as a form of criminal behavior for the execution of which computer equipment is used. Cyber crime is committed by a person who illegally enters someone else's information base and enters, modifies, hides, copies, uses, publishes, disables the use of the user's program and enters some data or virus. Cyber crime as a modern threat is experiencing its expansion, and the types of this threat are mainly mentioned in the literature: state-sponsored cyber attacks; ideological and political extremism; organized cybercrime and cybercrime at the level of individuals (Cornish, Hughes, Livingstone, 2009). The main characteristics of cybercrime include: digital means of execution - attacks are carried out using computers, mobile devices and online services, anonymity - use of hidden identities, VPNs and difficult tracking of perpetrators, and financial motive - the majority of cybercrimes aim to obtain financial benefits. In cyber crime, the target of the attack is the services, functions and contents located on the computer network, that is, the theft of data or identity, the destruction or damage of parts or entire networks and computer systems. The perpetrators' goal is a network into which viruses are inserted, websites are taken down, hackers invade and "denial of services" is carried out.

When it comes to the tools, the means that modern criminals use, it is important to emphasize that they do not "dirty" their hands by using a network in committing crimes. Sometimes this use of the network represents a completely new tool, while on other occasions it is so perfected that it is difficult to even recognize it (Radnović, Ilić & Radović, 2012:131). According to literature and international research, cybercrime can be divided into several main

categories (Holt & Bossler, 2016; Wall, 2007): financial crime - identity theft, online fraud, phishing, ransomware attacks, theft and misuse of data - unauthorized access to databases, leakage of confidential information, cyberattacks on infrastructure - attacks on power networks, banking systems, transport or health systems, distribution of malicious software - viruses, Trojans, spyware and other forms malicious code, sexual crime and abuse of children - online grooming, distribution of child pornography.

2.2. Cyber crime in the international framework

Criminal law is an indispensable element in the fight against crime. The timely adoption of legal regulations in order to provide a mechanism for dealing with cyber crime, as well as the successful use of such regulations should represent the legal basis for building a criminal policy when it comes to repressive measures. It is possible to detect the computer to which the program sends the collected data by performing a dynamic analysis using a program for analyzing the behavior of malicious programs and by simulating malicious programs in a controlled environment. The data obtained in this way can be used to automatically detect the computer to dump the data collected by the program for monitoring the input of characters from the keyboard. The use of this technique is very successful (Porobić & Bajraktarević, 2012:112).

The first complete document related to the problems of cyber crime is the Convention on Cyber crime of the Council of Europe, which was signed on November 23, 2001, and entered into force on July 1, 2004. The Convention on Cyber crime of the Council of Europe has the form of an international agreement, it was signed by thirty-eight countries, while Bosnia and Herzegovina ratified it on March 25, 2006. The provisions of the Convention are not directly applicable. "Rapid protection of stored computer data (Article 16) is a measure that members of the convention should prescribe in order to enable their bodies to issue orders or otherwise impose rapid (emergency) protection of electronic data stored in a computer system" (Selimović, 2015:74). On January 28, 2003, the Council of Europe adopted an additional protocol to the Convention on Cybercrime on the criminalization of acts of racism and xenophobia that have been committed.

Criminal organizations have so far moved extremely efficiently into the digital sphere, they have even developed new business models that resemble the most advanced legitimate companies. Just as some companies offer "security as a service" and build the cyber security capacities of interested customers, criminal organizations also offer "crime as a service" in the

cyber crime market. Another reason for concern is the possible cooperation between different malicious parties, that is, cybercriminals can offer their services to terrorist groups to commit crimes in cyberspace supported by states, solely for financial gain. In other words, the digital sphere offers criminal organizations new channels and opportunities to carry out illegal activities that might not otherwise be available. Trends and responses to crime enabled by cyber means is on the rise in both developed and developing countries. By its nature, cyber crime is international and transcends national borders so that the perpetrators do not have to be in the same country as the victims or the police pursuing them. This represents one of the key challenges in the fight against cyber crime, differences in the legal systems and practices of the various countries involved can affect the efficiency and possibility of cooperation, as well as the exchange of operational knowledge and evidence. Furthermore, very few police forces in the world have the capacity to fight cyber crime independently, although many have special units to fight cyber or "high-tech" crime. As with other types of malicious activity in cyberspace, there is an obvious asymmetry in the associated costs. As a result, the traditional approach to crime policing has been modified to some extent in the cyber sphere. Instead of immediately arresting the perpetrators, police cyber crime units focus on suppressing ongoing crimes and overcoming security weaknesses that have already been abused. Due to the equally present challenge of attribution across the cyber spectrum and lengthy and investigative procedures, including data forensics, reaching final convictions also takes longer than in the case of traditional crimes. The private sector is the most common target of cyber criminals and its experiences and interests should be taken into account when planning cyber crime strategies. At the international level, progress was achieved with the adoption of the Council of Europe Convention on High-Technological Crime, which is also called the Budapest Convention and which is the only binding international instrument on cyber crime to date and prescribes guidelines for countries to work on developing comprehensive national legal frameworks to combat cybercrime and establish a framework for international cooperation between signatory states. However, with sixty-one signatories and ten more expected to join, the Budapest Convention is still not a universal global document. Regardless, cases of international cooperation can be seen in recent years. The best examples of cyber crime where organizations for international police cooperation, especially Europol and Interpol, have joined the frameworks for strengthening international capacities and facilitating cross-border cooperation between police services are:

1. **WannaCry ransomware attack (2017)** – a global attack that affected more than 200,000 computers in 150 countries, paralyzing hospitals, companies and government institutions,
2. **Phishing campaigns against banks** – attacks that target user data through fake emails and websites,
3. **Theft of data from social networks** – for example, incidents in which millions of user data from Facebook or LinkedIn ended up in darknet sales (Holt & Bossler, 2016).

3. Cyber terrorism

In recent years, developed information technology has become a very effective tool in the hands of terrorist organizations to achieve their destructive goals. Namely, the new sophisticated techniques provided not only good opportunities for the realization of new attacks, but also for the protection of one's own channels of communication, as well as the promotion of fundamentalist ideas. Terrorists are no longer geographically limited within a certain territory, nor are they politically or financially dependent on individual countries. Today, they rely on modern communication capacities in which the Internet plays a very important role. Bearing in mind that a large number of highly skilled personnel from the IT field are available to terrorist organizations, we are aware of the danger of misuse of high-tech capacities by terrorists in the coming periods. An act of cyber terrorism is defined as the use of information resources in the form of a threat or blackmail to achieve a specific 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. 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 (Petrović, 1994:345).

The main advantages of the Internet are: easy access, availability (minimal or absent language barriers, time limitlessness, e-mail, chat rooms, discussion groups, blogs, sound, image, open or coded communication), non-regulation, absence of censorship and government control, potentially large audience worldwide, anonymity of communication and

decentralization, fast flow of information, low costs of setting up Internet presentations, constant movement and evasion (creation and deletion of addresses), a wide range of weapons (viruses, worms, backdoor bombs), critical infrastructure as potential targets (Kešetović, 2008:38).

Use of the Internet by terrorists can be threefold: as a weapon (cyber terrorism), as a means of communication between activists and as a medium for addressing the public. Cyber terrorism, as the first way of using the Internet by terrorists, refers to deliberate, politically motivated attacks on computer systems, programs and data that result in violence and fear against civilian targets (Zirojević, 2008:5). The first terrorist attack on computers was recorded back in 1969 in the American state of Michigan, where members of an anti-war organization called "Beaver 55" attacked the center for electronic data processing of the well-known chemical concern "Dow Chemical", which was claimed to produce war poisons, napalm and other chemical weapons. Another way of using the Internet is as a means of communication between activists, it is known that Osama Bin Laden communicated with members of Al Qaeda via mobile computers and wireless networks via encrypted messages (Zirojević, 2008:5). The third way of using the Internet by terrorists refers to addressing the public via a global computer network. Numerous organizations have entered the Internet space and created their Internet websites. "Terrorist attacks are often very carefully orchestrated to attract the attention of the broadcast media and the international press. The taking and holding of hostages only heightens the drama. The hostages themselves mean nothing to the terrorists. Their target group is spectators, not actual victims" (Jenkins, 1975). The regular content of the websites of terrorist organizations consists of information related to the history of the organization and important events during its development, political and social determination, biographical data of the leaders and prominent members of the organization, their speeches and texts, selective descriptions of significant activities in the past, information about political and ideological goals, as well as news containing information about current events, also selectively presented, avoiding the violent aspect of their activities. Due to its numerous advantages, the Internet is a suitable medium for presenting a terrorist organization in the light it wants and with goals that can be presented and achieved very effectively. One of the goals is to secure the support of as many supporters as possible, as well as the use of skilfully made and quite substantial presentations and texts in order to justify their activities, there is often a denial of any use of violence when carrying out the organization's activities. Today, active terrorist groups have at least one form of presence on the Internet, some groups have more than one Internet site - one main (so-called home page) and a larger number of unofficial ones (Kešetović, 2008:39). On

the other hand, "computers sometimes became the target of terrorist organizations. At one time, the IRA (Irish Republican Army) and the RAF (Red Army Faction) carried out several attacks on computer centers in England, Ireland and Germany, where information about terrorist activity was based" (Aleksić, Škulić, 2007:391).

We are aware of the fact that information technology is a valuable tool in the hands of a terrorist organization, but we must not lose sight of the fact that the results of technological progress are available to all people and state structures, in this sense, using the same advantages of information technology, we can track down every negative phenomenon, as well as the activities of terrorist organizations. When it comes to terrorist activities on the territory of Bosnia and Herzegovina, the percentage of computer and Internet use is relatively small compared to developed countries. According to data published in 2022, that percentage is around 24%. The most important areas of use of the Internet by terrorists are: planning and coordination, management of operations (physical contact between those who manage operations and those who directly carry out actions is practically no longer necessary), propaganda, fundraising, publicity, psychological warfare, data collection, recruitment and mobilization, networking, information sharing, money laundering, cyberwar, fraudulent purchases of sophisticated equipment, bioterrorism (advertising of falsified and fake medicines) (Kešetović, 2008:38).

3.1. Areas of cyber terrorism attacks

The development of information and communication technologies in recent decades has led to profound changes in the functioning of society. Today, digital infrastructure is an integral part of almost all aspects of human life - from banking transactions, energy supply and healthcare, to education and state administration. However, this comprehensive digitization has also created a new dimension of vulnerability: cyberspace has become a scene of conflict in which the activities of criminal groups, espionage networks, and even terrorist organizations take place. Unlike traditional forms of terrorism, which use physical violence, cyber terrorism operates in an invisible but extremely powerful space - the virtual environment. In this context, an attack does not have to directly cause human casualties to produce serious consequences; it is enough to disrupt the functioning of key systems and thereby cause panic or loss of public confidence. The key areas of attack are:

1. **Critical infrastructure** - includes power grids, water supply systems, fuel distribution systems, telecommunications and transport networks. Attacks on these sectors can

cause long-term disruptions in the way of life, threaten public health and safety, and have wide-ranging economic consequences.

2. **Health and medical systems** - hospitals, patient management systems and medical devices are increasingly networked. Disruptions in the work of hospitals (preventing access to electronic records) directly endanger lives and are therefore an attractive target for actors who want to produce shock or political influence.
3. **The financial sector** - banks, payment processors and stock exchanges represent targets that enable real economic consequences. Attacks that disrupt financial operations or undermine trust can have swift and far-reaching implications for markets and the public.
4. **Government and state institutions** - government networks, election systems, databases and communications of institutions are targets due to their symbolic and practical value. A successful attack can undermine trust in the state or hinder crisis management.
5. **Media and information ecosystem** - control of information - compromising media services, spreading misinformation or interrupting communication channels - enables terrorists to influence public perception, cause panic or demoralize opponents.
6. **Industrial control systems (ICS/SCADA)** - systems that manage industrial processes (eg refineries, power plants, water treatment plants) are particularly vulnerable because their disruption can cause physical damage or danger to human life.

A particular danger is the fact that cyber terrorism knows no borders - attackers can operate from any part of the world, often hidden behind complex anonymization networks. Attacks are most often aimed at destabilizing the state, endangering national security or sending an ideological message. The Organization for European Security Cooperation (OSCE) defines cyber terrorism as "cyber-related terrorism and more specifically, as terrorist attacks on cyber infrastructure, especially on control systems of non-nuclear critical energy infrastructure". Scenarios with cyber terrorism threats include paralyzing large urban areas, the health system or disrupting the financial sector "by changing a few ones and zeros" (Votel, 2015:4). Acts of cyber terrorism that can have a real physical effect of destruction are considered less likely and therefore less of a challenge for states due to the enormous amount of resources needed to carry out such an act (Weimann, 2004). Many terrorist organizations use the Internet to commit traditional crimes such as fraud, illegal access and hacking into computer systems. This leads to an overlap between cyber crime, cyber attacks and cyber terrorism, making it difficult to

differentiate between the two in the end. The rise of the Internet of Things represents another important threat that can easily be used by terrorist organizations to commit acts of cyber terrorism. Acts of cyber terrorism that can have a real physical effect of destruction are considered less likely and therefore less of a challenge for states due to the enormous amount of resources needed to carry out such an act (Weimann, 2004). Many terrorist organizations use the Internet to commit traditional crimes such as fraud, illegal access and hacking into computer systems. This leads to an overlap between cyber crime, cyber attacks and cyber terrorism, ultimately making it difficult to differentiate between them.

United Nations Security Council Resolution 1566 offers certain instructions on this issue, as it emphasizes the politically motivated element, identifying "terrorist acts" as: "criminal acts, including acts against civilians, committed with the intention of causing death or grievous bodily harm, or taking hostages, with the aim of causing a state of terror, intimidating the population or forcing a government or an international organization to perform or refrain from performing an act, which constitutes a criminal offense within and according to definitions of international conventions and protocols on terrorism." In addition, terrorist organizations use the Internet on a daily basis for various activities, such as propaganda (including radicalization, incitement to terrorism, recruitment), financing, training and planning (including through secret communications and information from open sources), as well as to carry out cyber attacks. While the use of the Internet for propaganda purposes has become a very important topic in the international community, accompanied by calls for the creation of strong partnerships, including those with the IT industry, the problem of using the Internet for financing purposes is quite often neglected. Meanwhile, the general transition to the use of technology in international trade has turned the Internet into a tool for terrorist organizations to launder money, collect and transfer funds (Jacobson, 2017:18).

The main motive of cyber terrorism is to achieve a political, religious or ideological goal, rather than personal or financial gain. The goal may be to instill fear among the population, destabilize the government, or attract international attention (Arquilla & Ronfeldt, 1993). Examples of cyber terrorism that have characterized the last decade are:

1. **Attacks on nuclear and energy systems** - the attack on the Iranian nuclear program (Stuxnet, 2010), which demonstrated the potential of cyber weapons for political purposes,
2. **Al-Qaeda and ISIS online activities** - use of the Internet for propaganda, recruitment and coordination of attacks,

3. **DDoS attacks on government websites** - during political protests or conflicts, often accompanied by propaganda messages.

Cyber terrorism has wider social, political and economic consequences than classic cyber crime. In addition to financial losses, it can cause panic, undermine trust in state institutions and potentially destabilize entire sectors of critical infrastructure (Rid, 2012). Defense against these threats requires sophisticated technical measures, international cooperation and legal frameworks adapted to the digital age.

4. Hacktivism

By definition, hacktivism is a combination of hacking and traditional activism. The word itself was not appropriated by the "hacktivists" themselves, but was appropriated by researchers, journalists and cyber security experts in an attempt to differentiate between the different actors in the cyber space. Hacktivism gives new forms of mobilization to activists online in their struggle for a certain value, that is, a goal, thus hacktivism enables remote activity and large-scale mobilization with one click of the mouse. Hacktivism represents the use of digital tools and hacking methods for the purpose of expressing political, social or ideological views. Unlike cyber crime, the primary motive of hacktivists is not financial gain, and unlike cyber terrorism, the goal is not to create fear or violence, but public attention and policy change (Jordan & Taylor, 2004). The main characteristics of hacktivism include: ideological or social motivation - attacks are aimed at policy change, awareness-raising or protest, collective action - often involving groups or networks of individuals, such as Anonymous or LulzSec, transparency and symbolic attacks - the goal is often public attention, not material damage. In terms of consequences, ordinary hacktivism generally causes less harm, which is why very few cases end up being prosecuted, especially because of the additional challenge of attribution that is as present here as in all other types of cyberspace activity. Motives of hacktivists and the difference from cyber crime and cyber terrorism is in essence hacktivism is considered disruptive, not destructive. This distinguishes it from other forms of malicious activity in the cyber space, such as cyber crime and cyber terrorism.

Hacktivists mainly use the tactics of spreading worms and viruses, distributed denial of service (DDoS) attacks, manipulation of websites and the like. The extent to which hacktivists are generally considered a minor threat can be illustrated by the characterization that their DDoS attacks are the equivalent of peaceful protests from the 1960s. However, hacktivists also engage in activities of taking over user accounts on Twitter and Facebook, and steal and/or

reveal sensitive and personal information from and on the systems they penetrate. There is a very fine line between hacktivism and cyber attacks. In some cases, hacktivists may collaborate with cybercriminals. In addition, direct public threats made by some hacktivist groups against various governments, companies and individuals can potentially cause panic and fear in the civilian population, which is one of the basic elements of the definition of terrorism. Finally, recent discussions have highlighted the growing allegations of state sponsorship of hacktivism, which is virtually impossible to prove even though reasonable assumptions can be made about its existence. Hacktivists use different methods to achieve their goals (Coleman, 2014; Jordan & Taylor, 2004): DDoS attacks - temporarily disabling websites to point out a problem or express protest, Website Defacement - changing the content of government, corporate or media websites to send a message, Leaks - breaking into systems and publishing confidential data for political or social criticism, Digital campaign and propaganda attacks - use of social networks and the Internet to spread ideological messages. While some hacktivists act out of the belief that they are "serving the public interest", their actions can cause legal consequences or damage to third parties (Coleman, 2014), as shown by the following examples:

1 **Anonymous** – an international group that carried out attacks on government and corporate websites to protest censorship, corruption or abuse.
2 **LulzSec** – a group that published user data of large companies in order to highlight system vulnerabilities and criticize security policies.
3 **WikiLeaks** – publication of confidential documents and information to reveal corruption or human rights violations.

Although many hacktivist attacks are symbolic, they have real consequences: temporarily disabling systems, damage to reputation, loss of data or financial damages. Hacktivism also raises the question of legal regulation and ethics in the digital space, as it often conflicts with regulations against unauthorized access and digital vandalism (Jordan & Taylor, 2004).

5. Legal framework for cyber terrorism, cyber crime and hacktivism in Bosnia and Herzegovina

Phenomena such as cybercrime, cyberterrorism and hacktivism represent different forms of abuse of digital space, which require an adequate legal framework and institutional response. In Bosnia and Herzegovina, although there is still no special law that would specifically regulate each of these areas, the existing criminal law and security regulations enable their sanctioning within the existing regulations.

Cyber crime in Bosnia and Herzegovina - the basic legal framework for combating these crimes consists of the Criminal Code of Bosnia and Herzegovina and entity criminal laws. In the Criminal Code of BiH, articles 300-303. regulate acts that fall under computer crime, such as unauthorized access to systems, interfering with the operation of computers network, data theft and damage, and computer fraud. This includes attacks aimed at financial gain, sabotage or breach of information security. At the entity level, the Criminal Codes of the Federation of BiH and Republika Srpska contain almost identical provisions. It is particularly significant that these provisions are harmonized with the Budapest Convention on Cyber crime (2001), to which BiH is a signatory, which ensures international cooperation and a single standard in the fight against digital crime. In practice, the prosecution of cyber crime requires cooperation between the Prosecutor's Office of BiH, State Investigation and Protection Agency (SIPA), the Ministry of Internal Affairs of the entities, and the National CERT of BiH, which has a technical role in detecting and preventing attacks. Although the legal framework exists, the main challenge remains the lack of professional staff and technical capacities for digital forensics, which makes it difficult to effectively prove these crimes.

Cyber terrorism in Bosnia and Herzegovina is not specifically defined, but it can be qualified through the existing provisions on terrorism. The Criminal Code of Bosnia and Herzegovina, Article 201, defines terrorism as an act that aims to cause serious fear among citizens or force state authorities to take certain actions. If such an act is carried out using digital technologies - for example, an attack on the power grid, information systems of state institutions or the media - it can legally be treated as a terrorist attack through information technologies. In addition to the CC BiH, the Law on the Protection of Secret Data, the Law on Communications of BiH, and strategic documents such as the Cyber Security Strategy of Bosnia and Herzegovina (2023–2027) are also relevant. These acts provide for measures to strengthen institutional capacities and international cooperation. BiH is also a signatory to the Council of Europe Convention on the Prevention of Terrorism (2005), which additionally obliges the state to sanction all forms of digital terrorism. The Prosecutor's Office of BiH and SIPA are responsible for cyber terrorism investigations in BiH, while the Ministry of Security of BiH has a coordinating and preventive role. This division of responsibilities enables a more efficient response to complex threats that take place in the digital space, but requires a high degree of cooperation between judicial, police and security authorities.

Hacktivism in Bosnia and Herzegovina: hacktivist activities do not have a special legal status, but are treated within the same provisions that apply to cyber crime - especially articles 300-303. Criminal Code of Bosnia and Herzegovina. If hacktivist activity causes significant

damage, disrupts public services or threatens security, it can be treated as a serious crime. The legal framework does not distinguish between motivated activism and a classic digital attack, which shows that the line between "digital protest" and crime remains unclear in practice.

6. Conclusion

The modern digital space represents both an opportunity and a threat, cyber crime, cyber terrorism and hacktivism, although they differ in motivation and goals, show a common characteristic - the use of technology as a means of realizing their interests. No person can guarantee that his/her data will be protected from misuse, so the consequences of misuse of personal data of Internet users are enormous. Cyber crime includes criminal acts committed both against individuals and against the state as an organized social community governed by a political system. In order to alleviate the problem of the phenomenon of the modern era of cyber crime, it is necessary to improve the information security of both organizations and individuals who use the Internet. Detecting crimes against electronic data processing systems is becoming more and more complex. The peculiarity of cyber crime requires an appropriate form of education for operatives involved in the fight against cybercrime. Protective measures are reflected in the application of the most modern means to protect data from misuse. Successful opposition to cybercrime requires a complete criminal procedural system of resistance to cybercrime. It is necessary to exchange information at the international level between the authorities for the fight against cybercrime. Although BiH does not yet have a special law on "cyber terrorism", the existing criminal law and security mechanisms enable the qualification and sanctioning of such acts. In practice, the qualification depends on the motive, goal and consequences of the attack. Key challenges remain: the lack of specific provisions, the need to strengthen capacities for digital investigations and the improvement of international cooperation. In Bosnia and Herzegovina, the term cyber terrorism is not explicitly defined as a separate criminal offense. However, the existing legal framework enables its sanctioning through a combination of provisions on terrorism and computer crime. Modern challenges require BiH to continue improving legislation, strengthening the digital capacities of investigative bodies and greater cooperation with international institutions. Only with a combination of legal, technical and educational approaches is it possible to ensure comprehensive protection of the national cyber space and respond to the complex threats of the modern era.

References:

Aleksić, Ž., & Škulić, M. (2007) Kriminalistika (5. izd.). Beograd: Pravni fakultet; Službeni glasnik.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141–165.

Brenner, S.W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Coleman, G. (2014). Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous. Verso Books.

Conway, M. (2007). Terrorism and the internet: New media – new threats? Parliamentary Affairs, 60(2), 288–306.

Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyber space and the national security of the United Kingdom: Threats and responses. London: Chatham House (Royal Institute of International Affairs).

Council of Europe. (2001). Convention on Cybercrime. Council of Europe (COE), 23 November 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy. In J. Arquilla & D. Ronfeldt (Eds.), Networks and Netwars: The Future of Terror, Crime, and Militancy (pp. 239–288). RAND Corporation

Gligorević, R. (2014). Cyber crime. Digital Economics, 163-174.

Deutsch, Karl W. (1966). The Nerves of Government: Principles of Political Communication and Control (2nd ed). New York: Free of Glencoe.

Gligorević, R. (2014). Cyber crime. Economics - innovative and economics research journal, 2(1), pp. 179-189. https://doi.org/10.7251/OIK1301011G

Holt, T. J., & Bossler, A. M. (2016). Cybercrime and digital forensics: An introduction. Routledge.

Jenkins, B. (1975). International Terrorism: A new mode of conflict. Los Angeles: Crescent Publications.

Jordan, T., & Taylor, P. A. (2004). Hacktivism and cyberwars: Rebels with a cause? Routledge.

Kešetović, Ž. (2008). Internet kao oruđe terorista. Revija za bezbednost, 4, pp. 37-41.

Matijašević, J., & Spalević, Z. (2010). Specific characteristics of computer criminal offenses with regard to the law regulations. XLV International Scientific Conference on Information,

Communication and Energy Systems and Technologies – ICEST 2010 CONFERENCE, 23 - 26 June 2010, Faculty of Technical Sciences, University "St. Clement Ohridski", Ohrid, Macedonia.

Kovačević, B. (2013). Cyberwar-American pretext for a new cold war? Polemos, 16(2), pp. 91-110.

Krivični zakon Bosne i Hercegovine. Službeni glasnik Bosne i Hercegovine (3/2003, 32/2003, 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015, 35/2018, 46/2021, 31/2023, 47/2023).

Krivični zakon Federacije Bosne i Hercegovine. Službene novine Federacije Bosne i Hercegovine (36/2003, 21/2004 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017, 31/2023, 58/2025).

Krivični zakonik Republike Srpske. Službeni glasnik Republike Srpske (64/2017, 104/2018, 15/2021, 89/2021, 73/2023, 9/2024, 105/2024, 19/2025, 14/2025, 31/2025).

Krivični zakon Brčko Distrikta BiH. Službeni glasnik BD BiH (19/2020, 3/2024, 14/2024).

Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Springer.

Olson, P. (2013). We are Anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency. Little, Brown and Company.

Parker, D. B. (1983). Fighting computer crime. New York: Scribner.

Petrović, S. R. (1994). Kompjuterski kriminal. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije; Uredništvo časopisa “Bezebednost”.

Porobić, M., & Bajraktarević, M. (2012). Cyber crime, pranje novca i finansijske istrage. Sarajevo: Visoko sudsko i tužilačko vijeće Bosne i Hercegovine; Swiss Agency for Development and Cooperation (SDC)

Rid, T. (2012). Cyber war will not take place. Oxford University Press.

Schjolberg, S. (1986). Computers and Penal Legislation: A Study of the Legal Politics of a new Technology. Universitetsforlaget.

UN Security Council, Security Council resolution 1566 (2004) [concerning threats to international peace and security caused by terrorism], S/RES/1566 (2004), 8 October 2004.

Votel, J. L. (2015). Statement before the Senate Armed Services Committee on the Posture of the U.S. Special Operations Command. Washington, D.C.

Weimann, G. (2004). Cyberterrorism: how real is the threat? Washington, D.C.: United States Institute of Peace.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Zirojević, M. (2008). Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma. Revija za bezbednost, 2(11), pp. 19-21.

Sažetak

U savremenom digitalnom dobu granice između kriminala, terorizma i haktiviuma u sajber prostoru postaju sve nejasnije. Iako uobičajeni elementi nasilja, političke motivacije, prijetnje i straha daju liniju kontinuiteta koji prolaze kroz dugu i složenu povijest terorizma, treba uzeti u obzir i da je tehnološka inovacija stvorila novi oblik terorizma. Posljednjih godina postala je veoma zanimljiva materija "cayber" terorizma, kao svojevrsne forme računarskog kriminaliteta. Sajber terorizam podrazumijeva korištenje informacionih resursa u vidu prijetnje ili ucjene da bi se ostvario određeni teroristički cilj. U fokusu pažnje jeste zloupotreba Interneta kao najznačajnije globalne komunikacione mreže. Korištenje Interneta od strane terorista može biti trojako: kao oružje, kao način komunikacije među aktivistima i kao medij za obraćanje javnosti. Upravo iz tih razloga, potrebno je širiti kulturu korištenja kompjuterske tehnologije, ali pažnju treba posvetiti i sigurnosnoj kulturi. Nakon neuspješne odbrane od sajber napada, internetska forenzika nam omogućava da izvršimo rekonstrukciju događaja kako bi otkrili izvršioce napada i metode njihovog djelovanja. S obzirom da se radi o izuzetno složenoj materiji, u radu smo se osvrnuli i na opšte odrednice vezane za računarski kriminalitet, računarski terorizam i haktivizam.

Ključne riječi: *sajber kriminal, sajber terorizam, terorizam, kriminalitet, informaciono-komunikaciona tehnologija.*