Cyber Terrorism as an Object of Modeling

Oleksandr Milov [1], Yevgen Melenti [2], Stanislav Milevskyi [3], Serhii Pohasii [4] and Serhii Yevseiev [5]

[1,3,4,5] *Simon Kuznets Kharkiv National University of Economics, Nauki ave., 9a, Kharkiv, 61166, Ukraine*
[2] *Juridical Personnel Training Institute for the Security Service of Ukraine Yaroslav Mudryi National Law University, Myronosytska str., 71, Kharkiv, 61002, Ukraine*

Abstract

The article examines issues related to the characteristics of cyber terrorism, as well as related concepts of terrorism and cyberspace. The definitions of these concepts are given. The types of cyber threats directly related to cyber terrorism are identified. The differences and similarities of the mentioned cyber threats are described. A structure that reflects the main features of cyber terrorism, which should be included in the model of cyber terrorism is presented.

Keywords

Cyber terrorism, cyber threats, hacktivism, cyber espionage, cyber war

1. Introduction

Advances in computer technology, coupled with the widespread availability of inexpensive, effective development tools and the availability of free knowledge on the Internet, have allowed cyber terrorists to improve their methods and conduct attacks remotely, damaging their intended targets. This opens up new opportunities for individuals and groups willing to engage in illegal activities to advance their shared goals, beliefs and agendas, invisible and often undetected through cyberspace, thereby creating new varieties of criminal threats. Generation of cyber terrorism; use of cyberspace to carry out activities classified as “terrorist”. Cyber terrorists can launch attacks through cyberspace and the virtual world, uniting the physical world and cyberspace [1]. Connectivity has become a central element of government institutions, critical infrastructures (telecommunications networks, finance, transportation and emergency services), culture and education. [2] Many critical private, public, national and military infrastructures can be vulnerable to cyberattacks as they continue to rely on legacy traditional security solutions rather than comprehensive and sophisticated cyber defense [3]. Cybercrime, cyberterrorism, and cyberwarfare are all common topics in the cybersecurity field. Physical terrorism and cyber terrorism have some common elements and a common goal, namely terrorism. However, cyber terrorism remains a vague concept, and there is a lot of controversy around its precise definition, goals, risk factors, characteristics and preventive strategies [4]. Cybercrime and cyberterrorism are often used interchangeably, or the term “cybercrime” can be used to refer to cyberterrorism, thereby blurring the distinction between the two, especially for the general public. Cyberattacks are still considered one of the highest priority risks for national security around the world [5, 6].

2. Characteristics of terrorism and cyberterrorism

Despite the inherent advantages of information

III International Scientific And Practical Conference “Information Security And Information Technologies”, September 13–19, 2021, Odesa, Ukraine

EMAIL: Oleksandr.Milov@hneu.net (A. 1); melenty@ukr.net (A. 2); Stanislav.Milevskiy@hneu.net (A. 3); spogasiy1978@gmail.com (A. 4); Serhii.Yevseiev@hneu.net (A. 5)
ORCID: 0000-0001-6135-2120 (A. 1); 0000-0003-2955-2469 (A. 2); 0000-0001-5087-7036 (A. 3); 0000-0002-4540-3693 (A. 4); 0000-0003-1647-6444 (A. 5)

technology, dependence on information technology has made countries and societies far more vulnerable to cyberattacks such as computer intrusions, program encryption, undetected internal threats in network firewalls, or cyber terrorists. The decentralized nature of the Internet, on the one hand, ensures the relative anonymity of users, and on the other, makes it insecure and ill-suited for tracking intruders or preventing their abuse by the internal openness of cyberspace [7,24-26].

Most researchers agree that a precise definition of cyber terrorism is needed, both for theoretical research and for the implementation of practical applications. At the same time, it is emphasized that this concept is multidisciplinary in nature, and should reflect the legal, economic, technological aspects of the problem. The definition should indicate the main characteristics or principles of the concept, as well as the range of real or potential scenarios to which the term cyber terrorism can be applied [8,27]. Defining cyber terrorism is even more difficult due to its abstract nature associated with understanding how certain incidents occur in cyberspace. Without a clear definition of the basic concepts, researchers cannot analyze the same sentences, therefore conceptualization is a necessary initial stage of research.

Since cyber terrorism is a combination of the terms “cyberspace” and “terrorism”, it is important to clearly define these terms.

"Cyber" in cyber terrorism refers to cyberspace. It is a prefix that is commonly added to a number of subgroups dealing with issues in the cybersecurity discourse, including, but not limited to, cybercrime, cyberwar, cyber espionage, and of course cyber terrorism. Cyberspace, unlike terrorism, is an accepted term. It refers to the virtual world, including the Internet and other computer communications infrastructure, which consists entirely of computers, algorithms, computer networks and data. According to [9,28], a cyberattack is “a deliberate computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system, or damages or steals the information it contains”. While cyberattacks themselves take place in cyberspace, they can have repercussions in the physical world.

Unlike cyberspace, terrorism is a term for which there is no agreed definition. However, there are a number of similar aspects that are broadly agreed upon. [10,23] contains a definition and criteria for what constitutes terrorism:

«...the deliberate creation and exploitation of fear through violence or threat of violence in the pursuit of political change. All terrorist acts involve violence or the threat of violence. Terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or objects of the terrorist attack. It is meant to instill fear within, and thereby intimidate, a wider “target audience” that might include a rival ethnic or religious group, an entire country, a national government or political party, or public opinion in general. Terrorism is designed to create power where there is none or to consolidate power where there is very little. Through the publicity generated by their violence, terrorists seek to obtain the leverage, influence, and power they otherwise lack to effect political change on either a local or an international scale.»

In this way, terrorism is separated from other types of crime and irregular warfare (see Table 1). For a response, having a criterion to distinguish terrorists from other threats is of particular importance in cyberspace, where attribution can be particularly difficult.

Table 1
Characteristics of Terrorism

Number	**Characteristics**
1	Ineluctably political in aims and motives
2	Violent - or, equally important, threatens violence
3	Designed to have far-reaching psychological repercussions beyond the immediate victim or target
4	Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders;
5	Perpetrated by a subnational group or non-state entity.

Source: [10].

Based on the definition of terrorism, a set of criteria for cyber terrorism can be formed (see Table 2).

Table 2
Characteristics of Cyberterrorism

Number	Characteristic
1	Executed via cyberspace
2	Ineluctably political or ideological in aims and motives
3	Violent or threatens violence
4	Designed to have far-reaching psychological repercussions beyond the immediate victim or target
5	Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders
6	Perpetrated by a subnational group or non-state entity

Source: [10].

The term "cyber terrorism" was introduced in the 1980s. There is still no agreement in the international community as to what kind of cyber activity is cyber terrorism [11]. In [12-15] the following definition of cyber terrorism is given:

«*Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*»

Other definitions of cyber terrorism are rather derivatives of this basic one. For example [16]:

«Cyberterrorism is the convergence of terrorism and cyberspace. ... unlawful attacks and threats of attack against computers, networks, and the information… done to intimidate or coerce a government or its people in furtherance of political or social objectives...to qualify a cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear».

3. Cyberterrorism and other Cyberspace Threats

The authors of the book [17] propose to consider all actions carried out by a terrorist cell or an individual via the Internet as cyber terrorism. The UN Office on Drugs and Crime has classified six ways the Internet is used for terrorist activities: propaganda (recruitment, radicalization and incitement); financing; preparation; planning (through secret communication and information from open sources); execution; and cyberattacks. Depending on the criminals involved and their motivation, cyber attacks can be classified into the types of cyber threats presented and defined in Table 3.

Table 3
Cyberspace Threats

N	Cyber Threats	Definition
1	Hacktivism	the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life. Social movements and popular protest are integral parts of twenty-first-century societies.

N	Cyber Threats	Definition
		Hacktivism is activism gone electronic [18].
2	Cyberwarfare	actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption [19]
3	Cybercrime	use of computers or other electronic devices via information systems to facilitate illegal behaviours [20]
4	Cyber-espionage	cyber espionage involves obtaining secret or classified information without permission from individuals, companies or governments for economic, political or military advantage using illicit means through the Internet, networks and/or computers, and can involve cracking or malicious software such as Trojan horses and spyware [21]
5	Chaotic Actors, Vigilantes	agents that have operated in cyberspace, such as criminals, hacktivists, industrial spies, nation states, terrorists, and insiders, there are also new challenging threats, such as chaotic actors, vigilantes, and regulators [22]

As shown in Table 4, there are a number of overlaps between cyberattacks that create a cyber threat, demonstrating confusion from the media and other actors who mislabel cyberattacks. For example, the distinction between hacktivism and other forms of cyber activity is especially important because acts of hacktivism have been flagged as cyber terrorism in a number of publications. While there is a definite difference between cyber terrorism and hacktivism, the purpose of the latter is not to maim, kill or intimidate; although the means to achieve the desired results may be similar. Consequently, "hacktivism does highlight the threat of cyber terrorism, the potential for people without moral constraints to use methods similar to those developed by hackers to wreak havoc."

Table 4
Other Cyber Threats v. Cyberterrorism

Cyberterrorism Criteria	Hacktivism	Cyberwarfare	Cybercrime	Cyberespionage	Chaotic Actors	Vigilantes	Cyberterrorism
Executed via cyberspace							
Ineluctably political or ideological in aims and motives	✓	✓	X	-	-	✓	✓
Violent or threatens violence	X	-	X	X	-	-	✓
Designed to have far- reaching psychological repercussions beyond the immediate victim or target	X	-	X	X	-	X	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	-	X	-	-	X	--	✓
Perpetrated by a subnational group or non-state entity.	✓	X	-	-	✓	✓	✓

Likewise, although cyber terrorism and cyber warfare are different, they have similarities; to attack computers, networks and information stored in them and cause damage in pursuit of political or ideological goals. In the case of cyber terrorism, its very nature must be violent and must be designed to be terrifying. While cyber war can lead to violence and have psychological consequences that go beyond the immediate victim or purpose, it can be argued that such effects are accidental and not necessary, as in the case of cyber terrorism. Consequently, cyber attacks by nation states cannot be considered acts of cyber terrorism. These distinctions between different cyber threats are important as they enable smarter countermeasures.

The structure reflecting the main objects and processes of cyber terrorism to be modeled is shown in Fig. 1. It consists of three main sections: Operating Forces, Techniques и Objectives.

Five forces are considered: characteristics, purpose / focus, types, capabilities and social factors. Each workforce, in turn, has a number of related subclauses. Operational forces provide the context in which cyber terrorism operates. Various high-level techniques are presented. These high-level techniques are supported by a variety of information gathering and computer and network security techniques. The objectives are similar to the motivation for standard terrorist activities, although there are some differences to show more pronounced intent.

4. Framework of Cyberterrorism

Operating Forces	**Characteristics** Cheap Anonymous Varied Enormous Remote Direct Effect Automated Replicated Fast	**Target/Focus** Transportation Utilities Financial sector Telecomms Emergency Services Government Manufacturing	**Types of Terrorism** Religious New Age Ethnonationalist Separatist Revolutional Far Right Extremist
	Capabilities Education Training Skill Expertise Financial support Resources Intelligence Insider knowledge		**Social Factors** Culture Beliefs Political Views Upbringing Personality Traits
Techniques	**Practices** Deface web sites Distribute disinformation Spread propaganda DOS using worms and viruses Disrupt crucial systems Corrupt essential data Steal credit card info for funds	**Attack Levels** Simply Unstructured Advanced Structured Complex Co-ordinated	**Modes of Operation** Perception Management & Propoganda Disruptive Attacks Destructive Attacks

Objectives	**Malicious Goals**	**Support Functions**
	Protest Disrupt Kill/Maim	Recruitment
	Terrify Intimidate	Training
	Meet demands	Intelligence
	Sensitive Info	Reconnaissance
	Affect crucial services	Planning
	Publicity Solicit money	Logistics
		Finance
		Propaganda
		Social Services

Figure 1: Framework of Cyberterrorism (Source: [23])

The framework's contribution is to organize the area of cyber terrorism and provide its context for analytical review and in-depth modeling. The operational forces describe the various benefits of using cyberterrorism, the intended systems to be attacked, and the terrorist's mindset. The "Techniques" section discusses the classification of attack tactics. The "Objectives" section discusses the immediate objectives of the attacker and also distinguishes between cyberterror activities and helper functions that can be used by computers and networks (which are often confused with cyberterrorism). This discussion helps to clarify important details regarding the functional thinking of cyber terrorists, as well as clarify which aspects of cybercrime and hacking will be used.

5. Conclusion

Cybercrime, regardless of how it is defined or classified, can have devastating consequences for computerized networks. Until a universally effective solution to this universal problem is found, the strength of a cybersecurity governance regime will depend on an information security management system that emphasizes a comprehensive cyber risk assessment that takes into account all possible threats to an organization's business, including internal and external threats. Modeling the technologies and processes for conducting cyberattacks, and not least the behavior of attackers, should lead to the construction of effective systems for ensuring the cybersecurity of critical infrastructures. The classification of cyber threats given in the article, the definition of cyber terrorism and its characteristics should focus the attention of the model developer on the processes and entities that should be reflected in the models of cyber terrorism in the first place.

6. References

[1] D. A. Simanjuntak, H. P. Ipung and C. lim, "Text Classification Techniques Used to Facilitate Cyber Terrorism Investigation," in Proceeding of Second International Conference on Advances in Computing, Control, and Tele-communication Technologies (ACT 2010), Jakarta, 2010

[2] Lord Jopling UK NATO General Rapporteur, "171 CDS 11 E rev. 1 final InformationS And National Security General Report," NATO Par l iamentary Assembly International Secretariat, Brussles, 2011

[3] M. A. A. &. C. E. Dogrul, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.," Tallinn, 2011

[4] DCSINT, "Handbook No. 1.02, Critical Infrastructure Threats and Terrorism," US Army Training and Doctrine Command, Fort Leavenworth, Kansas, 2006

[5] NATO, "173 DSCFC 09 E bis - NATO and Cyber Defence," NATO, Brussles, Belgium, 2009

[6] L. Jarvis and S. Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers," Terrorism and Political Violence, vol. 27, no. 4, pp. 657-678, (2015)

[7] Michael Kenney, “Cyber-Terrorism in a Post-Stuxnet World,” *Orbis* 59, no. 1 (2015): 112

[8] Bruce Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2017), 40-41

[9] NATO, "171 CDS 11 E rev. 1 final - Information and National Security," 09 11 2011. [Online]. Available: http://www.nato-pa.int/default.asp?SHORTCUT=2589.

[10] Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of

control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

[11] Oleksandr Laptiev, Oleh Stefurak, Igor Polovinkin, Oleg Barabash, Savchenko Vitalii, Olena Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.172 –176.

[12] Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

[13] O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021.

[14] Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021. pp.62-71, DOI: 10.5815/ijcnis.2021.03.06.

[15] Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

[16] Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

[17] D. Denning, "- Cyberterrorism‖, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives," 23 05 2000. [Online]. Available: https://pdfs.semanticscholar.org/7fdd/ae586b6d2167919 abba17eb90e5219b7835b.pdf

[18] Dorothy Denning, 2001. “Is Cyber Terror Next?” New York: U.S. Social Science Research Council, at http://www.ssrc.org/sept11/essays/denning.htm.

[19] Dorothy Denning, 2000b. “Cyberterrorism,” *Global Dialogue* (Autumn), at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

[20] Dorothy Denning, 1999. “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” Washington D.C.: Nautilus, at http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[21] Gordon, S. & Ford, R. (2002) Cyberterrorism? *Computers & Security*, **21**(7): 636-647.

[22] UNoDC, "The Use Of The Internet For Terrorist Purposes," United Nations Office On Drugs And Crime, Vienna, 2012

[23] Paul Taylor and Tim Jordan, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004), 1, papers3://publication/uuid/50380B27-672A-4D1A-89C0-6FC517868773.

[24] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It, Terrorism and Political Violence*, vol. 23 (New York: HarperCollins Publishers, 2012), 6.

[25] Samuel C. McQuade, *Understanding and Managing Cybercrime* (Boston: Pearson Education, 2006), 2.

[26] Khan, “States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis,” 93.

[27] Tyson Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things* (Cambridge: Morgan Kaufmann, 2016), 228.

[28] Salih Tutun, Mohammad T. Khasawneh, Jun Zhuang. New framework that uses patterns and relations to understand terrorist behaviors // Expert Systems With Applications 78 (2017) 358–375.