CONTENTS

PUBLIC LAW

INTERNATIONAL LAW

PRIVATE LAW

PUBLIC LAW

Cyberterrorism Defining the Threat and Evaluating EU Legal Countermeasures

Tal PAVEL[1]
Adriana Iulian STANCU[2]

Abstract: Cybercrime is a criminal activity directed at or using a computer, computer network, or networked device. Cybercriminals or hackers commit most cybercrimes after a quick and undeserved gain. However, there are also cases where cybercrime aims to damage computers or networks for reasons other than profit, such as political or personal reasons. The Internet creates considerable development potential in all areas of social life, its applications being practically unfailing. The current technology, however, opens new horizons for committing crimes. Ease of use, low cost, speed, and anonymity make the Internet an environment conducive and accessible to crimes. Due to the global feature of the network and its vast complexity, the perpetrator's "hidden" possibilities are practically unlimited, thus encouraging the commission of crimes. International law is the most practical means of deterring cyberterrorism due to the inherent realities of cyberspace. Universal jurisdiction is likely the most practical means of prosecution and deterrence. The threat of cyberterrorism can be significantly decreased with a multilayered strategy of deterrence and mitigation.

Keywords: Cyberterrorism; EU; Legislation; Cyber; Counterterrorism

1. Introduction

The research analyses cyberterrorism, its definition generally and especially in the EU and the member states, and examines their current legal measures and initiatives to counter the threat of cyberterrorism, including legislation and cooperation, mainly due to the growing threat both in terrorism and the ability of terrorist

[1] Assistant Professor, PhD, The Academic College of Tel Aviv Yaffo, Address: Rabenu Yeruham St 2, Tel Aviv-Yafo, Israel, Corresponding author: Talpv@mta.ac.il.
[2] Senior Lecturer, PhD, Faculty of Law and Administrative Sciences, "Dunarea de Jos" University of Galati, Romania, Address: 111 Domneasca Str., Galati 800201, Romania, E-mail: Adriana.tudorache@ugal.ro.

ALS, Vol.6, no.2, pp. 7-17

individuals and organizations to take advantage of the Internet and cyberspace to perform terrorism.

Over the years, the literature has tried identifying cyberterrorism and concluding specific definitions for this phenomenon. In addition, the literature analyzed the EU countermeasures for cyber threats. Most of it refers to cybercrime, not cyberterrorism, while those that refer to cyberterrorism are not updated.

Argomaniz J examined the "European Union responses to terrorist use of the Internet" in 2014, asserting that "the EU response has concentrated on raising critical communication infrastructure resilience standards to prevent potential cyber-attacks"[1]. Saulawa J and Marshal M analyzed in 2015 the legal perspective of cyberterrorism as part of the cybercrime convention in Europe, compared to the Economic Community for West African States (ECOWAS)[2]. Foggetti N researched 2009 the tangent lines between cyber terrorism and the right to privacy in EU legislation[3]. Bucaj E expressed the need in 2017 to regulate cyberterrorism in line with principles of international law[4]. Tehrani et al., in a paper from 2013, also expressed the need for "a global response to a multi-jurisdictional crime" by cyberterrorism[5]. Others analyze cyberterrorism legal challenges and their implications from a local perspective[6].

Our research analyses the threat and its countermeasures in the EU member states. Therefore, we examine the current definitions of "Cyberterrorism", mainly in the EU member states as in their strategic publications. In addition, the research will analyze the different legal initiatives by the EU and the member states to counter cyberterrorism's ongoing and evolving threat.

---

[1] Javier Argomaniz, 'European Union Responses to Terrorist Use of the Internet' (2014) 50 http://dx.doi.org/10.1177/0010836714545690 250 <https://journals.sagepub.com/doi/abs/10.1177/0010836714545690> accessed 5 November 2023.

[2] Mu'azu Abdullahi Saulawa and Junaidu Bello Marshal, 'Cyberterrorism: A Comparative Legal Perspective' (2015) 33 Journal of Law, Policy and Globalization <https://heinonline.org/HOL/Page?handle=hein.journals/jawpglob33&id=1&div=&collection=> accessed 5 November 2023.

[3] Nadina Foggetti, 'Cyber-Terrorism and the Right to Privacy in The Third Pillar Perspective' (2009) 3 Masaryk University Journal of Law and Technology 365.

[4] Enver Bucaj, 'The Need for Regulation of Cyber Terrorism Phenomena in Line with Principles of International Criminal Law' (2017) 13 Acta Universitatis Danubius. Juridica 141.

[5] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap and Hossein Taji, 'Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime' (2013) 29 Computer Law & Security Review 207.

[6] Clive Walker, 'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' (2005) 110 Penn State Law Review <https://heinonline.org/HOL/Page?handle=hein.journals/dlr110&id=635&div=&collection=> accessed 5 November 2023.

The research aims to analyze the following research questions: (RQ1) Is there a standard and unified EU definition for cyberterrorism? (RQ2) Is there a standard definition for cyberterrorism among the EU member states? (RQ3) What are the measures and initiatives of the EU and the member states to counter cyberterrorism?

Further research may analyze the current regional and international measures and initiatives to counter cyberterrorism, examine local implications of such multi-stakeholder initiatives, and analyze the development of the term cyberterrorism globally, mainly due to ongoing technological development such as the AI, Cryptocurrencies, encrypted communications by the hands of the terrorists, and the low entry level of threat actors in this domain.

2. Cyberterrorism

Barry Collin, an analyst for the Institute for Security and Intelligence, coined "cyberterrorism" in the mid-80s of the 20th century. He defined it as "the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action"[1].

Over the years, various popular and official sources from different sectors, states, and perspectives have defined "cybersecurity". We examine five types of sources: (1) online dictionaries, (2) governmental and international agencies, (3) researchers and experts, (4) EU member states and institutions.

(1) Online dictionaries

- **Vocabulary.com** - "An assault on electronic communication networks"[2].
- **Oxford Dictionary of Politics and International Relations** - "The use of cyberspace by organizations with the intentional aim to promote terrorist propaganda, recruitment, incitement, revenue generation, training, and acts of disruption"[3].
- **Merriam-Webster** - "terrorist activities intended to damage or disrupt vital computer systems"[4].
- **Cambridge Dictionary** - "the use of the internet to damage or destroy computer systems for political or other reasons"[5].

---

[1] Kenneth C, White, 'Cyber-Terrorism: Modem Mayhen' (1998) <https://apps.dtic.mil/sti/pdfs/ADA345705.pdf> accessed 5 November 2023.

[2] 'Cyber-Terrorism' (*Vocabulary.com*) <https://www.vocabulary.com/dictionary/cyber-terrorism> accessed 5 November 2023.

[3] Iain McLean and Alistair McMillan, 'The Concise Oxford Dictionary of Politics' [2009] The Concise Oxford Dictionary of Politics.

[4] 'Cyberterrorism' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/cyberterrorism> accessed 5 November 2023.

[5] 'Cyberterrorism' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/cyberterrorism> accessed 5 November 2023.

(2) Governmental and international agencies

- **Federal Bureau of Investigation** (FBI) - "the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population"[1].
- **US Army Training and Doctrine Command** – "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, to influence a government or population to conform to a particular political, social, or ideological agenda"[2].

(3) Researchers and experts

- **Jonalan Brickey** - "the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change"[3].
- **Dorothy E. Denning** - Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack 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, plane crashes, water contamination, 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 are mainly a costly nuisance would not"[4].

(4) EU member states and institutions

[1] 'Dale L. Watson Assistant Director, Counterterrorism/Counterintelligence Division Bureau of Investigation Before the Senate Select Committee on Intelligence' (6 February 2002) accessed 5 November 2023.

[2] 'US Army Training and Doctrine Command' (2005) <https://web.archive.org/web/20121009012948/http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA439217> accessed 7 November 2023.

[3] Jonalan Brickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace' (2012) 5 Combating Terrorism Center at West Point <https://ctc.westpoint.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace/> accessed 6 November 2023.

[4] 'Terrorist Threats to the United States - Statement of Dr. Denning' (23 May 2000) <https://irp.fas.org/congress/2000_hr/00-05-23denning.htm> accessed 6 November 2023.

- **Organization for Security and Co-operation in Europe (OSCE)** – "terrorist attacks on cyber infrastructure particularly on control systems for non-nuclear critical energy infrastructure"[1].
- **Italy** – "ideology motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organization"[2].
- **Romania** –"premeditated activities carried out in cyberspace by individuals, politically motivated groups or organizations, ideological or religious which may cause damage materials or victims, likely to cause panic or terror"[3].
- **Poland** – "an offence of a terrorist nature committed in cyberspace"[4].

The different definitions of "cyberterrorism" demonstrate what experts argued years ago: "few experts agree on a universally acceptable definition" due to several "stumbling blocks to creating a clear and consistent definition of the term "cyberterrorism.""[5].

Even though we can indicate several common characteristics from the different definitions mentioned above:

Topic	5W+1	Descriptions from the different definitions
Purpose	Why	To promote terrorist activities; to coerce or intimidate a government or civilian population; to conform to a particular political, social, or ideological agenda; the pursuit of political change; furtherance of political or social objectives; ideology influencing a state or an international organization; politically motivated groups or organizations, ideological or religious.
Means	What	To create and exploit fear through violence or the threat of violence; to intimidate or coerce a government or its people;

[1] 'Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace' (2013) <https://www.osce.org/files/f/documents/4/b/103500.pdf> accessed 7 November 2023.

[2] 'National Strategic Framework for Cyberspace Security' (2013) <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> accessed 7 November 2023.

[3] 'Cyber Security Strategy of Romania' (2013) <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania/@@download_version/1b41c7f470b14b52be67866e84007f87/file_en> accessed 7 November 2023.

[4] 'Cyberspace Protection Policy of the Republic of Poland' (2013) <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf> accessed 7 November 2023.

[5] Gabriel Weimann, 'Gabriel Weimann Cyberterrorism How Real Is the Threat?' (20041) <https://www.usip.org/sites/default/files/sr119.pdf> accessed 8 November 2023.

		result in violence against persons or property, or at least cause enough harm to generate fear; may cause damage to materials or victims; an offence of a terrorist nature.
Method	How	An assault on electronic communication networks; damage or disrupts vital computer systems; damage or destroy computer systems; to shut down critical national infrastructures; destruction and/or disruption of services; militant operations in cyberspace; terrorist attack.
Platform	Where	Electronic communication networks; cyberspace; computer systems; cyber tools; computers and telecommunications; computers; networks and the information stored; cyber-infrastructure, particularly control systems.

From the analysis of the different definitions, we can conclude that cyberterrorism is *a cyber-attack that creates damage, disruption, or destruction of information and operation technology that produces fear or even causes damage or victims to influence states or organizations to perform political, social, or religious changes*.

3. EU Legislation to Counter Cyberterrorism

States and international organizations are increasingly realising that combating cyberterrorism requires international cooperation. International organizations such as the European Union, NATO, and OSCE have taken significant legislative and policy actions to address cybersecurity. In order to create international standards that will aid in the prevention of cyberterrorism, states, international organizations, and the private sector have all actively collaborated. Standards for encryption and standards for financial transactions have been the two primary areas of attention (Gable, 2021, p. 94).

The frequency and sophistication of cyberattacks and cybercrime are rising throughout Europe. With an estimated 41 billion devices globally expected to be connected to the Internet by 2025, this trend will continue (Cybersecurity: how the EU tackles cyber threats, 2023).

A new EU cybersecurity strategy was presented in December 2020 by the European Commission and the European External Action Service (EEAS). By implementing this strategy, Europe will be more resilient to cyberattacks and be able to fully utilize digital tools and services that are dependable and trustworthy for businesses and citizens alike. Concrete recommendations for the use of investment, policy, and regulatory tools are included in the new strategy. The Council adopted cybersecurity strategy conclusions on March 22, 2021, emphasizing the need for

cybersecurity in the construction of a resilient, environmentally conscious, and technologically advanced Europe (Cybersecurity: how the EU tackles cyber threats, 2023).

3.1. The Cybersecurity Act

The Cybersecurity Act creates a framework for cybersecurity certification for goods and services and fortifies the European Union Agency for Cybersecurity (ENISA). The EU's cybersecurity agency, ENISA, is now more powerful. The agency is given a permanent mandate, additional resources, and new tasks by the EU Cybersecurity Act. By laying the technological foundation for particular certification schemes, ENISA will play a crucial role in establishing and managing the European cybersecurity certification framework. Through a special website, it will be in charge of educating the public about the certification programs and the certificates that have been issued. "*ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises*" (The EU Cybersecurity Act, 2023).

3.2. The EU Agency for Cybersecurity

With a broader mandate and a permanent position, the new EU agency for cybersecurity expands upon the framework of its predecessor, the European Union Agency for Network and Information Security. Additionally, it has kept the same acronym (ENISA). In response to cyberattacks, it assists EU institutions, member states, and other relevant parties (Cybersecurity: how the EU tackles cyber threats, 2023).

Within Europol, a dedicated European cybercrime center has been established to assist member states in their efforts to disrupt criminal networks and conduct online investigations.

3.3. European Police Organization (Europol)

Member states are conducting a security initiative called the European Multidisciplinary Platform against Criminal Threats (EMPACT) to identify, prioritize, and address threats posed by international organized crime. One of its top priorities is to defend against cyberattacks.

The European Commission put forth new legislation in May 2022 to address the issue **of online child sexual abuse and exploitation**. The Council is currently debating the new regulations. As a workaround for articles 5(1) and 6(1) of the ePrivacy directive, the EU has established temporary regulations. A provisional

agreement was reached in May 2021 by the representatives of the European Parliament and the Council regarding temporary measures that permit providers of web-based email and messaging services, as well as other electronic communications services, to keep track of, remove, and report instances of child sexual abuse online until more permanent legislation is settled.

3.4. Encryption

In order to ensure that robust encryption technology is used going forward and that law enforcement and the judiciary have the same authority to operate as they do in the offline world, the EU is working to establish an active dialogue with the technology industry. A resolution on encryption was adopted by the Council in December 2020, emphasizing the necessity of both security via encryption and security despite encryption (Cybersecurity: how the EU tackles cyber threats, 2023).

4. Conclusion

Since the development of WMDs, cyberterrorism may be the biggest threat to both national and international security. The effects of a cyberterrorist attack will be greater as states and their economies become more intertwined, largely because of the Internet and the international financial system of global trade. Similar to this, cyberterrorists' attacks are likely to get more effective as they gain experience undermining national governments and taking down vital infrastructure (Gable, 2021, p. 118).

The Internet creates a huge development potential in all areas of social life, its applications being practically unfailing. The current technology, however, opens new horizons for the commission of crimes. Ease of use, low cost, speed, and anonymity make the Internet an environment conducive and accessible to crimes. Due to the global feature of the network and its huge complexity, the perpetrator's "hidden" possibilities are practically unlimited, thus encouraging the commission of crimes.

To discover such facts, a high degree of specialized personnel and the use of sophisticated technologies are necessary, which must, however, keep pace with the means and methods used by criminals. Moreover, although access to the network is global, the investigation of crimes committed in this way - which can be cross-border in nature - runs into national barriers, the lack or insufficiency of international regulations as it is incriminated in the matter, and even the lack of specific incrimination in national legislation, lagging far behind this development.

So, although the diversity of acts committed through the Internet is huge, they are incriminated in the common legislation, which does not cover all the situations

specific to this means of committing. For example, electronic harassment can become very dangerous due to the possibility that the perpetrator has to preserve his anonymity and especially carry out acts of harassment, bullying, being put in a very advantageous position, which encourages him to continue - the inability to locate and the lack of direct physical contact with the victim are likely to remove certain psychological barriers or inhibitions of the perpetrator and, at the same time, amplify the victim's fear. In certain forms of execution, the acts of electronic harassment can be included in crimes such as threats, sexual harassment, or blackmail, etc.

Cybercrime is criminal activity directed at or using a computer, computer network, or networked device. Most cybercrimes are committed by cybercriminals or hackers who are after a quick and undeserved gain. However, there are also cases where cybercrime aims at damaging computers or networks for reasons other than profit, such as political or personal reasons. Cybercrime can be committed by both individuals and organizations. Some cybercriminals are organized, use advanced techniques, and are highly technically skilled.

International law is the most practical means of deterring cyberterrorism due to the inherent realities of cyberspace. Likely, the most practical means of prosecution and, consequently, deterrence is the universal jurisdiction. The threat of cyberterrorism can be significantly decreased with a multilayered strategy of deterrence and mitigation. It's only a matter of time until cyber terrorists unleash a cyber apocalypse, unless and until states are willing to exercise universal jurisdiction over cyberterrorist acts as part of that layered approach (Gable, 2021, p. 118).

5. References

Argomaniz J, 'European Union Responses to Terrorist Use of the Internet' (2014) 50 http://dx.doi.org/10.1177/0010836714545690 250 <https://journals.sagepub.com/doi/abs/10.1177/0010836714545690> accessed 5 November 2023

Brickey J, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace' (2012) 5 Combating Terrorism Center at West Point <https://ctc.westpoint.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace/> accessed 6 November 2023

Bucaj E, 'The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law' (2017) 13 Acta Universitatis Danubius. Juridica 141

'Cyber Security Strategy of Romania' (2013) <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania/@@download_version/1b41c7f470b14b52be67866e84007f87/file_en> accessed 7 November 2023

'Cyberspace Protection Policy of the Republic of Poland' (2013) <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf> accessed 7 November 2023

'Cyber-Terrorism' (*Vocabulary.com*) <https://www.vocabulary.com/dictionary/cyber-terrorism> accessed 5 November 2023

'Cyberterrorism' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/cyberterrorism> accessed 5 November 2023

'Cyberterrorism' — — (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/cyberterrorism> accessed 5 November 2023

'Dale L. Watson Assistant Director, Counterterrorism/Counterintelligence Division Bureau of Investigation Before the Senate Select Committee on Intelligence' (6 February 2002) <https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-the-united-states> accessed 5 November 2023

Foggetti N, 'Cyber-Terrorism and the Right to Privacy in The Third Pillar Perspective' (2009) 3 Masaryk University Journal of Law and Technology 365

'Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace' (2013) <https://www.osce.org/files/f/documents/4/b/103500.pdf> accessed 7 November 2023

McLean I and McMillan A, 'The Concise Oxford Dictionary of Politics' [2009] The Concise Oxford Dictionary of Politics

'National Strategic Framework for Cyberspace Security' (2013) <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> accessed 7 November 2023

Saulawa MA and Marshal JB, 'Cyberterrorism: A Comparative Legal Perspective' (2015) 33 Journal of Law, Policy and Globalization <https://heinonline.org/HOL/Page?handle=hein.journals/jawpglob33&id=1&div=&collection=> accessed 5 November 2023

Tehrani PM, Abdul Manap N and Taji H, 'Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime' (2013) 29 Computer Law & Security Review 207

'Terrorist Threats to the United States - Statement of Dr. Denning' (23 May 2000) <https://irp.fas.org/congress/2000_hr/00-05-23denning.htm> accessed 6 November 2023

'US Army Training and Doctrine Command' (2005) <https://web.archive.org/web/20121009012948/http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA439217> accessed 7 November 2023

Walker C, 'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' (2005) 110 Penn State Law Review

<https://heinonline.org/HOL/Page?handle=hein.journals/dlr110&id=635&div=&collection=> accessed 5 November 2023

Weimann G, 'Gabriel Weimann Cyberterrorism How Real Is the Threat?' (20041) <https://www.usip.org/sites/default/files/sr119.pdf> accessed 8 November 2023

White KC, 'Cyber-Terrorism: Modem Mayhen' (1998) <https://apps.dtic.mil/sti/pdfs/ADA345705.pdf> accessed 5 November 2023

Cybersecurity: how the EU tackles cyber threats. (2023, 11 02). European Council: https://www.consilium.europa.eu/en/policies/cybersecurity/#:~:text=The%20EU%20invests%20much%20effort,measures%20against%20cyberattacks%2C%20and%20sanctions.

Gable, K. A. (2021). Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal. *43 Vanderbilt Law Review 57*, 88-118. https://scholarship.law.vanderbilt.edu/vjtl/vol43/iss1/2

The EU Cybersecurity Act. (2023, 11 10). European Commission: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act