Chapter II

Disinformation and Cyberterrorism in Light of the Standards of the Council of Europe

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ & MONIKA NOWIKOWSKA

Abstract We live in an age where the internet is the main source of information. We can find reliable facts there, but it is also easy to come across misrepresentations, half-truths or news stories that are only intended to sow panic. This is how disinformation works. In the age of the internet, manipulating information has become a powerful tool. Disinformation in the new media is entirely intentional and deliberate. It involves the transmission of false or manipulated information that causes the recipient to be misled. Disinformation creates an image of the world that is inconsistent with reality. It leads to erroneous decisions and actions and creates a false view of a particular piece of information. Disinformation can influence election results, shape public behaviour and affect the mood of a country. Disinformation on the internet has become one of the biggest threats to the digital space. Today, it is not limited to individual states, but affects institutions at the international level.

Also linked to technological advances and the development of the global internet is the phenomenon of cyber-terrorism. Cyber-terrorism is a combination of classic terrorist activities and the use of the latest ICT devices. States are becoming increasingly aware of the threats emanating from the network and are taking up the fight against them in order to protect the most important elements of critical infrastructure that guarantee the smooth functioning of a country. States need to be ready at both a legal and practical level for the occurrence of a cyber-terrorist attack in order to be able to effectively repel and defend themselves. This article

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, Kozminski University, College of Law, ul. Jagiellonska 57/59, 03-301 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com, ORCID: 0000-0003-0188-5704. Monika Nowikowska, Ph.D., Assistant Professor, War Studies University in Warsaw, Faculty of Law and Administration, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

https://doi.org/10.4335/2024.2.2 ISBN 978-961-7124-25-5 (PDF)
Available online at http://www.lex-localis.press.

examines the issue of Disinformation and Cyberterrorism in Light of the Standards of the Council of Europe.

Keywords: • cyberterroris • cecurity threats • human rights • journalist • disinformation

1 Introductory remarks

Disinformation constitutes a serious security threat for contemporary democratic societies – states, international organisations, and individuals. It should be stressed that this phenomenon is becoming one of the most significant and complex challenges of the 21st century. As an element of measures related to threats, disinformation is a phenomenon that resembles terrorist actions. As regards the notion of terrorism, despite comprehensive studies of the subject, no widely acceptable definition has been developed since 1937 when the League of Nations prepared the first draft Convention on the Prevention and Punishment of Terrorism. This results from the fact that there are fundamental differences in opinions, attitudes, and interests, arising from historical, cultural, and religious conditions. The situation is similar to the definition of disinformation. Currently, in the context of the rapidly developing new threats to security and public order, characteristic of the convergence era, activities based on information technology are becoming fundamental. This refers to the preparation and implementation of individual undertakings as well as to organising and financing decentralised networked structures. The shift of the paradigm, as part of which the traditional forms of actions, including acts of terrorism, are disappearing, gives rise to the fact that the sphere of new threats is being identified, including interrelations between terrorism and digital media, or digital services in general, considered to be the key accelerator of changes to the global information system, which in turn constitutes the foundation on which contemporary societies are shaped. It is currently possible to speak about the emergence of a clear cultural pattern which brings together the spheres of telecommunications, information technology and media, and forms an intricate system, a peculiar multi-communication environment spanning multiple levels, distribution platforms and types, including printed media, linear and non-linear audio-visual services and their Internet forms, so-called digital media (Chałubińska-Jentkiewicz, 2023a: 228).

Speaking of disinformation as an act of terrorism in the theatre of contemporary times, or referring to digital media as the oxygen thanks to which it can assume completely new forms, has become the canon of defining mutual relationships between them. However, research into this sphere has not revealed any such straightforward links. Scholars do not offer clarity as to a comprehensive theory indicating major trends in respect of the relationships between disinformation as an act of cyberterrorism and digital media (Nacos, 2009: 4–5). On the one hand, terrorists use the existing social communication media as an effective distribution platform, create them, or are active users of new communication and information services, particularly social media. On the other hand, digital media constitute an intriguing area of wholly new threats, from the perspective of the mission undertaken by the media, the nature of marketing activities and the commercial approach. Terrorists strive to attract global public attention to the objectives and causes for which they organise and conduct their operations. Carrying out attacks, often targeting unspecified, anonymous and numerous victims, is aimed at evoking fear, and the widespread dissemination of information about such attacks may favour its intensification, at times compelling public authorities to make decisions that the terrorists expect. It is similar with disinformation. The regular use of digital media for disinformation purposes, as in the case of terrorism, might also result in their legitimisation, according to the agenda setting concept. As Ch. de Franco aptly notes, “the narratives produced by the media, especially those constructed around one or more images, do create a reality effect which impacts not only the public at large but also policymakers. Those narratives constitute a mediated reality which interferes with the policymaking process because they affect the mental image of a given issue through which policymakers interact and based on which they take decisions” (Franco, 2012:47).

Digital media, which are currently functioning in an environment characterised by unprecedented competitiveness, where information flow, in addition to its cultural dimension, is becoming an important economic sector, are searching for pieces of news that are highly attractive to the audience. It seems that the pressure for fast and topical messages favours their tabloidisation, and dramatic and bloody images are somewhat consistent with the expected pattern, so one can speak about their overrepresentation in social communication media. Disinformation may be built around such stories.

2 Cyberterrorism

It should be stressed that a lot of online information might affect the types of targets and weapons selected by terrorists and their operational methods. Cyberterrorism consists of using information technologies, i.e., computers, software, telecommunications devices, and the Internet, to reach the goals that a given group has set. As B. Hołyst aptly noted, “just like multiple corporations use the Internet for making their activities more effective and flexible, terrorists leverage the power of technology (IT) to develop new operational doctrines and organisational forms” (Hołyst, 2011:63). The emergence of terrorist groups linked in a network constitutes a part of a concept called netwar. Cyberterrorism involves the disruption or destruction of opponents’ information systems and the seizure of their strategic data. Terrorist organisations using the web are characterised by informal communication depending on their needs and cross-border reach, i.e., moving beyond state borders, dispersion and mutual trust, with no hierarchical bureaucratic structure (Chałubińska-Jentkiewicz, Nowikowska, 2020: 305).

While cyberterrorism is defined as a phenomenon characterised by a high degree of abstraction, the progressing development of information technologies allows the statement that the risk of a terrorist cyberattack is increasing. The actuality of the deployment of such cyberattacks stems from the fact that terrorists use the Internet to plan and conduct physical attacks, to spread ideologies, to manipulate public opinion and the media, to recruit and train new terrorists, to acquire and build up funds, to obtain information on potential targets, to control the operations being conducted, or to gain access to confidential information constituting a secret of various types (Smarzewski 2017: 66).

From the perspective of cyberterrorism, new communication methods reduce transmission time, which allows online participants-terrorists to communicate despite being dispersed, as well as to reduce communication costs and to extend the scope and comprehensiveness of information. In addition to network forms of terrorist organisations, IT also contributes to improving the collection and analysis of materials as part of terrorist intelligence activities, consisting of the search for attack targets via the Internet. The above conditions facilitate the deployment of various types of offensive informational operations, such as propaganda campaigns (recruitment of members, acquisition of funds, and public outreach) – attacks against virtual targets (electronic attacks, computer system choking, sending of unsolicited e-mail at a mass scale, web bugs) – used for physical damage.

3 The Council of Europe’s standards on combating disinformation

Since the beginning of its existence, the Council of Europe has taken up the topic of terrorism on multiple occasions, generally placing the issue in the sphere of cooperation within the justice system in criminal matters. It should be stressed that the perspective was unchanged, determined by human rights and the need to protect them. This meant balancing initiatives taken to maintain fundamental rights and freedoms as the key values defining the shape of its axiological system. The Council of Europe adopted two conventions: the Convention on the Prevention of Terrorism of 16 May 2005 (OJ EU L 159/3) and the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism done in Warsaw on 16 May 2005 (Journal of Polish Law 2008, No. 165, item 1028). Article 1(1) of the Convention on the Prevention of Terrorism includes a definition of a terrorist offence, which means any of the offences within the scope of, and as defined in, one of the treaties listed in the Appendix to the Convention. Under the Convention, the Parties are obliged to establish public provocation to commit a terrorist offence, recruitment and training for terrorism as criminal offences (Articles 5–7). Taking the above solutions into account, a general definition of an act of terrorism can be adopted, according to which it is any offence committed by individuals or groups resorting to violence or threatening to use violence against a country, its institutions, its population in general or specific individuals which, being motivated by separatist aspirations, extremist ideological conceptions, fanaticism or irrational and subjective factors, is intended to create a climate of terror among official authorities, specific individuals or groups in society, or the general public. Therefore, it spans across the multitude of contemporary forms of the phenomenon being discussed, from organised, international group “undertakings” to single acts committed on the territory of a given state by individuals, motivated by irrational or subjective factors, as stated above (Chałubińska-Jentkiewicz, 2023a: 230).

It is worth noting here that disinformation activities constitute a vital part of terrorism and cyberterrorism. From the perspective of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), referring to the freedom of expression, the Council of Europe defined the scope of such relationship in its Declaration of 2 March 2005 on freedom of expression and information in the media, in the context of the fight against terrorism. The authors stressed the negative impact of the phenomenon of terrorism on human rights and referred to the need to achieve unity between the Member States of the Council of Europe to unequivocally condemn all acts of terrorism as criminal and unjustifiable, threatening and destabilising social life, wherever and by whoever committed. In this context, governments face a challenge to balance the need to uphold the freedom of expression, as the foundation of democratic and pluralistic societies, and the assurance of security (Chałubińka-Jentkiewicz, Nowikowska 2022: 20). It was asserted that the free and unhindered dissemination of information and ideas is one of the most effective means of promoting understanding and tolerance, which can help prevent or combat terrorism. This also applies to the phenomenon of disinformation. As per Article 10(1) of the ECHR, everyone has the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom of expression exercised by the media, including digital media, is not absolute and unlimited, as it carries responsibility and the resulting obligations. It should be stressed that the freedom of expression may be subject to restrictions which, however, do not go beyond the boundaries set by the provisions of Paragraph 2 of the Article being discussed, construed in line with the case law of the European Court of Human Rights, unifying its interpretation.

From the perspective of disinformation related to the phenomenon of cyberterrorism, it is possible to speak about restricting the freedom of speech based on such criteria as public safety and, given the increasing threat of cybercrime, preventing the disclosure of information protected by law (Chałubińska-Jentkiewicz, Nowikowska 2022: 115). Measures derogating from the obligations under the ECHR may be taken in times of war or other public emergencies threatening the nation’s life. However, they should not be contradictory to other obligations under international law (Article 15(1)). The states have been obliged to make every effort to refrain from adopting measures threatening the freedom of the media, constituting one of the pillars of democratic societies, particularly exploited by disinformation actors. Therefore, every instance of restricting the freedom of expression must be subject to formalities prescribed by law and necessary in a democratic society (Chałubińska-Jentkiewicz, 2023a: 230).

As already mentioned, disinformation relies on digital democracy. It should be noted that, in the context of limiting the freedom of expression, the Committee of Ministers called on public authorities in Member States not to introduce any new restrictions unless they are strictly necessary and proportionate in a democratic society and subject to examining carefully whether existing laws or other measures (hard or soft) are not already sufficient, and to refrain from adopting measures equating media reporting on the phenomena of terrorism with support for terrorism. Moreover, as regards the issues being discussed, Member States were obliged to ensure access by journalists to information regularly updated, in particular by appointing spokespersons and organising press conferences, with due respect for human dignity and subject to the right to respect for private life. Journalists should also have access to, follow, and report on judicial proceedings and the judgements referring to persons who are the subject of anti-terrorist judicial proceedings, with due respect for the presumption of innocence (Article 6(2) of the ECHR). It was stressed that any potential restrictions meeting the aforementioned requirements may be based on the criterion of the so-called good of the justice system, in special circumstances and to the extent strictly necessary in the opinion of the court, where publicity would prejudice the interests of justice (Nowikowska 2023: 113). The press may be excluded from all or part of a trial, for example, in the interests of national security (Article 6(1)). It is also vital to respect media independence and the right not to disclose sources of information and also to refrain from any pressure on the media, etc.

Firm suggestions are also addressed to the media, particularly to journalists, whilst they are made from the perspective of their responsibility for the contents being disseminated. This means that they should not support terrorist organisations or the operations they conduct by, for instance, offering a platform to terrorists to present their objectives and ideas, giving them disproportionate attention, adding to the feeling of fear in society, or even unintentionally serving as a vehicle for violence through the expression of racist or xenophobic feelings or hatred. However, this should not be coupled with self-censorship, as the effect of this would be to deprive the public of necessary and desired information, including expert opinions and results of consultations. In addition, the media should not disseminate information in situations when such actions would jeopardise the safety of persons and the due conduct of anti-terrorist operations or judicial investigations of terrorism. Finally, the media should not abstain from respect for the right to dignity and private life, particularly concerning the victims of terrorist attacks and their families (Article 8 of the ECHR). They should also adhere to the rule of the presumption of innocence regarding potential perpetrators, taking into account the distinction between suspected or convicted terrorists.

It should also be asserted that the media should bear in mind the positive role they can play in preventing hate speech, promoting mutual understanding, and creating an atmosphere of tolerance. Press representatives are also encouraged to hold training courses on the broadly understood theme of terrorism, from its historical, cultural, religious and geopolitical aspects to practical issues related to improving their safety, and to invite journalists to follow these courses. Following the above recommendations, the media should adopt self-regulatory measures or adapt the existing alternatives to laws to effectively respond to the ethical issues raised by media reporting on terrorism.

The Committee of Ministers of the Council of Europe monitors the implementation of the above recommendations and suggestions by the governments of Member States, in particular in the legal field, considering the issues from the perspective of standards related to fighting terrorism and their effect on the freedom of expression in the media. The assumptions put forward in the Declaration are confirmed in Recommendation 1706 (2005) Media and Terrorism. The Parliamentary Assembly of the Council of Europe, referring to previous documents concerning the fight against terrorism in the context of human rights, including the freedom of speech, stressed the significance of the rights of democratic societies to be informed about matters of public concern. This also includes such acts as threats and terrorist attacks or the response by the state and international organisations to these threats and acts. At the same time, the Parliamentary Assembly indicated that terrorist acts were intended to create terror, fear or chaos among the public. The effect of such acts depends largely on how they are reported in the media. Messages that are disseminated at a global level and repeated multiple times are dramatised and sensationalist. They often result in distorting and exaggerating the real issues out of proportion. The public and the media must be aware that perpetrators intentionally utilise such acts to have the strongest possible impact.

However, the above considerations do not change the fact that, subject to the right to privacy, it is essential to inform the public about terrorist acts. In specified cases, properly disseminated information might contribute to forming adequate political responses. The Assembly also recommended that Member States take account of this recommendation in their national work and hold a debate on this issue in their respective national parliaments, inform the public and the media regularly about government strategies and actions, and inform, upon their request, media about the specific situation to avoid journalists investigating terrorism being unnecessarily exposed to dangers. It is also important to cooperate with law enforcement authorities to prevent the dissemination of illegal messages and images by terrorists on the Internet. Member States should place special emphasis on abstaining from prohibiting or even restricting unduly the dissemination of information and opinions in the media, as well as on the reaction by state authorities to terrorist acts and threats under the pretext of fighting terrorism. Of course, the recommendations refer to information about terrorist activities, but they also include a significant context related to disinformation.

The media are encouraged to develop, through their professional organisations, a code of conduct for journalists, photographers, and other professionals dealing with the subject-matter to keep the public informed about terrorism issues, in line with the highest professional standards. This is a crucial matter. It also includes the need to organise training courses for media professionals to increase their awareness of the sensitive nature of media reports on the issues in question. In particular, emphasis was placed on the cooperation between individual media entities and their professional organisations to avoid a race for sensationalist news and shocking images which violate the privacy and human dignity of victims or increase the negative effect of such acts on the public, which is what terrorists expect. It is also important to avoid aggravating fear and the societal tensions underlying terrorism, and to refrain from disseminating any hate speech by offering terrorists a platform for presenting their news, views, and opinions. As already mentioned, the Council of Europe also issued Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, adopted on 26 September 2007. It is generally based on the principle of freedom of expression, treated as the basis for the functioning of contemporary democratic societies and the personal development of every human being. The protection covers not only desirable and non-offensive information and ideas but also messages that are shocking and not widely acceptable (Nowikowska, 2020: 54). This stems from such values as pluralism and tolerance, which are essential to the Council of Europe. In particular, the protection should include broadly understood freedom of speech in matters of public concern, artistic expression or commercial communication. Therefore, Member States that impose restrictions must substantiate a strong societal need, making such interference indispensable, legitimised based on publicly available domestic laws, and falling within European standards. The restrictions must be proportional to their objectives, and it should be noted that stricter limitations, for example in relation to penal sanctions, will require stronger justification. At the same time, the Council of Europe's standards do not authorise absolute and unlimited access to classified government information. The above approach should be applied in times of crisis, where authorities are especially tempted to impose restrictions on society. The Council of Europe condemns all violent acts, including the killings of media professionals, while stressing the need for dialogue between governments, media professionals and civil society to guarantee freedom of expression. Journalists play a crucial role in times of crisis by providing accurate, timely and comprehensive information. They also have the capacity to foster a culture of tolerance and understanding between different social groups. According to the provisions of Section I, state authorities are free to adopt their definition of crisis, whilst the Council of Europe has provided a relevant framework, giving examples of such situations in the form of a non-exhaustive list. Terrorist attacks are one of them. The term *times of crisis* is not associated with an officially and legally introduced state of war or other emergencies but it generally refers to the factual circumstances. Similarly, a comprehensive definition of "media professionals" is proposed to ensure the widest possible protection to all persons working in the information flow sector. In Section II, an obligation was placed on Member States to ensure, to the fullest extent, national and foreign media professionals' safety, provided that measures taken to this end must not be used by Member States as a pretext to unnecessarily limit the rights of media professionals, such as their freedom of movement and access to information or areas affected by the crisis. Restrictions may be applied only when absolutely necessary. Authorities should also provide regular information to all media professionals covering the events equally through various channels, e.g., press conferences. If possible, they should set up information centres. The above postulates result from the threats that journalists encounter while on a mission to inform the public about crises (Chałubińska-Jentkiewicz, 2023a: 236–237).

Military and civilian agencies in charge of managing crises are also expected to take practical steps to promote the understanding of crises, including the ones related to terrorism or cyberterrorism, in cooperation with media professionals dealing with these issues. Employers should strive for the best conceivable protection of their media staff on dangerous missions, including by providing safety equipment, comprehensive counselling (from legal to psychological), and life and health insurance. Furthermore, journalism schools and professional media associations are encouraged to provide specialised safety training for media professionals. Another significant requirement is that member states should protect the right of journalists not to disclose their sources of information, especially information referring to the identity of informants, as the foundation of personal safety and the control function that media professionals play (Nowikowska, 2023:106). Moreover, they should not misuse in libel and defamation legislation against media professionals, and thus limit their freedom of expression. Times of crisis do not entitle states to restrict the freedom of expression of the media beyond the limitations allowed by Article 10(2) of the ECHR, especially in matters of key importance to the public. When imposing potential restrictions in the event of, e.g., incitement to violence or public disorder, such terms should be adequately and clearly defined. It is also necessary to consider that the media might contribute to resolving crises as, for instance, public service media might be a vital factor for social integration between various groups. In times of crisis, Member States' maintenance of a favourable environment for freedom of expression and independent media, in line with the standards set by the Council of Europe, should also include the possibility of criminal or administrative liability for those public officials who try to manipulate public opinion by exploiting its special vulnerability. This might take place in specific matters concerning the examination of whether certain information or documents should be revealed to journalists, and the final decisions in this respect (Chałubińska, 2023a:238).

In times of crisis, such as terrorist attacks, the process is, to a large extent, affected by the inclination to disclose partial, manipulated, or even false data. In the discussed situations, the media also have a special responsibility as they are expected to adhere to the highest professional standards, including ethical ones. In such circumstances, the regular provision of factual, accurate, timely and comprehensive information to the public can play a major part in awareness-raising and calming down public sentiments. In transmitting such information, as regards its content, form and context, the media should be attentive to the rights of other people, their distinct sensitivities, and their possible feelings of uncertainty and fear.

Digital media are developing separate guidelines, partly in fear of the regulatory measures that public authorities might but, generally speaking, they are not convinced about such solutions, as they require the widest possible extent of freedom and operational flexibility. In this respect, cooperation is needed between self-regulatory bodies at the national, regional and European levels, coupled with support from state authorities and other stakeholders engaged in these issues.

It should be added that the amendment to the Audiovisual Media Services Directive introduced significant modifications in this sphere. As part of implementing its provisions in the Polish legal system, obligations concerning digital content for video-sharing platforms were introduced (bearing in mind that, according to the definition of such platform, it also includes a place where users share other content, not just video files). Furthermore, the Digital Services Act (the DSA) refers to all online platforms and other online service providers operating in the EU, including marketplaces, e.g., Amazon, social media and search engines. The obligations laid down in the said Regulation depend on the size of a given enterprise – the larger the entity, the more extensive the list of obligations. The categories of very large online platforms (VLOPs) and very large online search engines (VLOSEs) include companies which have the average monthly number of active recipients of the service in the Union equal to or higher than 45 million. Major American platforms (i.e., Google, YouTube, Amazon, Apple, Meta) fall within these categories. Enterprises defined as VLOP and VLOSE will have to continuously analyse and mitigate so-called systemic risks, such as the dissemination of illegal or harmful content (e.g., disinformation) or manipulation of users' behaviour. VLOPs will also be obliged to provide (national and Union-level) supervisory authorities and researchers with access to the data and algorithms that would allow a detailed assessment. The DSA also provided a crisis response mechanism. As part of the mechanism, if an event posing a threat to public safety or health occurs (such as the Russian invasion of Ukraine or the COVID-19 pandemic), the European Commission may oblige VLOPs to adopt specific measures, for instance, to remove for three months selected contents that spread harmful disinformation or accounts of users who incite dangerous behaviours. Comprehensive and constructive dialogue between government authorities, the media and other domestic entities interested in combating disinformation and the establishment of a platform for debates favour the assurance of freedom of expression in times of crisis. It should be added that Directive 2018/1810 does not provide grounds for sanctioning user activities beyond the right to restrict access to contents that violate the provisions of the Directive. The only sanctions imposed on users include blocking such content and limiting the possibility of publishing new content. In addition, users may be subject to liability on general terms if the contents they publish infringe the provisions of other legal acts (for example, if they contain child pornography or incite terrorism) (Chałubińska-Jentkiewicz, 2023a: 239).

Cooperation at an international level, particularly with the Council of Europe and other organisations, facilitating information exchange and monitoring possible violations effectively, is also desirable. Non-governmental organisations have the potential to contribute to the safeguarding of freedom of expression and information by monitoring infringement of the freedom of speech in various ways, such as maintaining helplines for consultation, reporting harassment of journalists and other alleged violations targeting the media and their mission. Such entities should also cooperate in offering comprehensive support and training to media professionals. The addressees of the guidelines should include Member States, media organisations, and other interested civil society entities.

Nonetheless, unlike other spheres of communication operations where responsibility is distributed in similar proportions, in the case of disinformation strictly related to the category of security, the burden of implementing the Council of Europe's standards should be essentially imposed on domestic public authorities. As for normative standards referring to human rights, states were left with substantial flexibility in assuring public safety and order, consisting of the possibility to introduce restrictions on the freedom of expression under the ECHR, particularly taking into account the public safety criterion. Although they are obliged to refrain from introducing new restrictions other than the ones that are strictly necessary and proportional in a democratic society, and only where existing legal instruments and other alternative measures are insufficient, and although the criteria for the establishment of restrictions on freedom of expression are listed on a *numerus clausus* basis in Article (2) of the ECHR, such criteria are defined in detail at a national level. It should also be noted that the temptation to put in place restrictions towards cross-border activities and media operating at a global scale intensifies in the circumstances of a crisis, where terrorist acts become more severe and violent. What is more, such restrictions are more willingly tolerated or even approved by the public in such circumstances.

In general, the Council of Europe's standards concerning the protection of the freedom of expression do not require any changes. However, their implementation at the Member State level might give rise to certain doubts. Regarding restrictions, public authorities may adopt extremely diverse approaches, ranging from a *laissez-faire* policy to censorship. Self-regulation or co-regulation is a potential third option. Moreover, the objectives of governments and the media are not always convergent. While the mass media usually strive for complete independence, effectiveness, also in commercial terms, and safety of its operations, governments expect that they should support the objectives, strategies and, at times, even specific operations conducted as part of counteracting the practices discussed in this paper. They also expect that the perpetrators of terrorist acts are presented as criminals whose conduct cannot be justified in any way.

The media are, on the one hand, seen as the pillar of rights and freedoms, including freedom of speech, and as a factor facilitating the spread of disinformation, on the other hand. This gives rise to the yet unsolved dilemma of whether, when, and to what extent public authorities may introduce restrictions on access to information. The states may refer to issues related to the criteria for restrictions in a more precise way, also at the interpretation level, using the case law of the European Court of Human Rights, which is obvious. Guidelines should be developed in close cooperation with the media. Concerning self-regulatory measures being applied by the media in the sphere of disinformation, if they prove to be ineffective, the concept of co-regulation should be considered in the scope in question (preferably in the initial approach formula). Summing up, it can be stated that refraining from censorship is a crucial principle resulting from the Council of Europe's standards. In the context of disinformation, this measure should not be excluded, for example, if a given (online) medium is directly controlled by hostile foreign services or if illegal content needs to be removed or blocked. Features of terrorist activities may be noted in disinformation campaigns, which brings the phenomenon closer to cyberterrorism acts, i.e., acts of aggression in cyberspace. Cyberterrorism is a multidimensional phenomenon covering financial resources, state-of-the-art technologies, and broadly understood logistics. The power of cyberterrorism, as a certain branch of terrorism, stems from the fact that one person having specialist knowledge and equipped with basic computer devices can paralyse air traffic, affect the transmission of electricity or cause a failure of banking systems, robbing ordinary citizens, institutions or even state enterprises of their funds, as well as influence human behaviour, stance, and emotions. The combat against cyberterrorism is very problematic and laborious due to the vastness of cyberspace and the challenges related to locating perpetrators. A large proportion of such offenders are still unattainable to law enforcement authorities. One of the ways to fight cyberterrorism is to cut off funds by eliminating financing sources. Other methods consist of developing a stable strategy model that would mark out shared activities in combating cyberterrorists and establishing international organisations to combat or mitigate cyberterrorism and to eliminate disruptions in state critical infrastructure. It is worth noting that, according to D.E. Denning, cyberattacks motivated by political objectives may be a manifestation of cyberterrorism. It is important to assert, however, that a situation must occur where not only the legal and economic order is disrupted, which gives rise to considerable loss whose dimensions are becoming purely material and physical, affecting people (Denning, 2002: 79). As can be noticed, to a large extent, terrorists increasingly often use non-conventional weapons and less complex modes of their operations. Disinformation measures may be characterised by the properties of cyberterrorism. Attracting attention is the basis for existence in digital media. This, in turn, is necessary for the so-called agenda setting to work. It is a concept according to which information in the media is treated as significant by the audience. Disinformation evokes and acts on fear to reach political transformations. Undoubtedly, we are dealing here with a form of psychological warfare. Vivid examples of how the atmosphere of fear can be built effectively across society include the disinformation activities related to COVID-19 and 5G. The theory concerning the origin of the coronavirus was the greatest fake news of all time. According to the thesis, it was a biological weapon created to destroy a competitive economy. Another fake news that added to the atmosphere of fear was the link between COVID-19 and 5G. Fake information was published on social media saying that the emitted electromagnetic radiation would accelerate the spread of the virus. The effects of this absurd theory were real, as mobile network towers were burnt in numerous cities across Europe.

The objective of disinformation actors using the media was to disseminate their convictions, ideologies, and motives. The Internet allows them to achieve the objective to a greater extent than the traditional media. Terrorists are becoming the authors of their image and are not dependent on journalists assuming their role. This allows them to demonstrate their operations not as barbaric acts but as an uneven battle between an oppressed group of partisans and world powers. Numerous videos posted on such websites as YouTube may serve as an example. It is not the intention of disinformation actors to be seen positively. What they mostly want is to present their ideologies and demands. It can be described as propaganda through action. A part of their message is lost in information noise and is misrepresented or forgotten by recipients. All that is remembered is the slogan, for example, fighting against Ukrainian fascists.

Current or potential members or enthusiasts of a given theory belong to a significant target group that various actors try to reach through the media. Enthusiasts are a vital element which every organisation needs, as they are the ones who support disinformation activities. Such assistance may be effective as they are not directly related to the informational message. Thus, they are not responsible for its content. A clear example of how the atmosphere of support for a given theory can be built effectively was disinformation related to the anti-vaccine movement. In the analysis by the Academic Centre for Cybersecurity Policy (*Analysis Concerning the Impact of the Social Phenomenon of Anti-Waxxers on the Security of the Polish State,* performed by Inserq sp. z o.o. for the Academic Centre for Cybersecurity Policy, dated 12 December 2021), to fulfil research objectives, two types of objects were used: a Twitter account and threads. Each of the objects offers different analysis possibilities. The study included the identification of specific Twitter accounts which had a specified influence on Polish information space and generated the greatest quantities of digital content, and specific information about COVID-19 and vaccines that was further shared on Twitter. In early 2020, i.e., at the beginning of the pandemic, when the SARS-CoV-2 virus started spreading across Europe, it was noted that the main axis of public interest included the informational content produced by major opinion-forming media in Poland, e.g., Fakty TVN, Polsat News, TVP Info, as well as media centres related to medicine, for example, the Ministry of Health, MedOnet and other outlets. According to the collected data, in the initial phase of the pandemic in Poland and Europe, there were no groups strictly and explicitly negating the existence of the SARS-CoV-2 virus and the COVID-19 disease. Instead, the dominating place was taken by the emotions of fear, the demonstration of a strong will to obtain the greatest possible number of pieces of information on the threat, mockery of the circumstances and the fear, and opinions that the virus is far away (in the Far East), so there is no need to discuss it. Accounts that negated the existence of the virus in general, its mortality rates and the devastated health of infected patients began appearing in the media space around March and April 2020, and the highest surge of such accounts, including the most popular ones followed by tens of thousands of users, was recorded around mid-2020. Moving from negating the existence of the virus to negating the existence, necessity and effectiveness of using vaccines against SARS-CoV-2 was a natural continuation of the trend (Chałubińska-Jentkiewicz, 2023a: 245–246).

4 The phenomenon of acceptance and justification of disinformation

As regards terrorism, an interview with a terrorist, conducted by media representatives, can be seen as a kind of legitimising such acts. For instance, the TVN24 channel decided to take such a step in interviewing Ali Ağca. Another dangerous trend that can be observed in the media is attempting to understand terrorists' motives, resulting in the unintentional justification of their conduct. Experts, often invited to television studios, try to refer to cultural, social, economic, or psychological considerations. Undoubtedly, the most important factor for media operations in the free digital single market are numbers of viewers, listeners or readers who decide to use a given communication medium. The proceeds to the budget of a given media institution (mostly from advertisers) depend on them. Therefore, potential recipients must be provided with a product that is "attractive" enough for them.

Media theory authors indicated properties that a given event should have to become a valuable media product for the audience. These include 1) timeliness – an event should be "fresh", preferably published nearly real-time; 2) intensity – the spectacular and intense nature of the event has a positive impact on its media value; 3) unambiguity – an event should be easy to assess by most recipients; 4) importance – an event should be important in the sense of its impact on society; 5) conformity – understood as meeting the audience's predictions and expectations, which may be based on stereotypes; 6) surprise – the extraordinary nature of a given event; 7) continuity – an event should last for an extended time; 8) references to prominent individuals or major international relations actors – events that affect the most important entities are interesting; 9) complementarity – the possibility to link a given event with specific individuals or past events; 10) negativism – negative events are more spectacular than the positive ones (Chałubińska-Jentkiewicz, 2023a: 246–247).

Given the above list of characteristics of newsworthy events that are attractive to the audience, it can be concluded that disinformation messages meet most of the criteria. The media are not only used by disinformation actors but also leverage the newsworthiness of disinformation-related events for their own purposes. For instance, false information was disseminated in the media concerning a deadly game called the Blue Whale Challenge. The game was allegedly to cause the death of over 130 teenagers. According to the thesis, teenagers aged between 14 and 17 were to complete challenges assigned by their mentor. The objective was to strive for their death. The matter gained publicity when *The Sun*, a British tabloid, wrote about it. The information was further copied by several Polish websites, after which facts were mixed with fiction and passed on by nearly all mainstream media. "Hyperbolisation" is one of the characteristics of the Internet. And this property was used in the Blue Whale story. So far, no reliable sources or tangible evidence have been identified to prove that such danger occurred.

"For commercial media, breaking news, often the most tragic, is – horribile dictu – a blessing. This is their logic, and ethics will not be able to do much about it (...)". Therefore, the media are showing blood, sensationalism, and human drama. A colourful tabloid and a reputable opinion-forming newspaper will approach such events differently (but none would disregard it). Various ways of approaching a given theme are called formatting.

The following piece of news presented in various formats may serve as an example:

1. Informational format (agency-style): "Four people were killed and 33 were injured after a bomb exploded in a café in Paris on Thursday morning".
2. Sensationalist format (in a reputable newspaper): "A bomb thrown by a terrorist in a busy Paris café lethally wounded four people and left 33 others covered in blood".
3. A story format (a piece of news in a tabloid newspaper, illustrated with a huge photograph showing scattered remains): "A newlywed couple on their honeymoon died on Thursday when a bomb destroyed a café in Paris. The young wife and husband, who had got married a day before, were among the four killed and 33 injured in a bomb explosion".
4. Educational format (a commentary in a serious newspaper): "The bomb attack in a Paris café on Thursday seems to herald a new wave of violence inflicted by Islamic fundamentalists outraged by French foreign policy in the Middle East".

Media experts have noted that, currently, we are dealing with a shift towards reporting on events in the tabloid story format. This is because the mass audience expects reader-friendly information which is spectacular at the same time. The process has also spread across the informational activities of online users. The development of digital democracy has contributed to changes in the media market in the economic and organisational context, and in the information sphere, taking into account the quality and significance of information itself. We are dealing with media power, which can be defined in several ways. N. Couldry and J. Curran define it as a label for the net result of organising a society's resources so that the media sector has significant independent bargaining power over and against other key sectors (big business, political elites, cultural elites, and so on) (Couldry, Curran, 2003:39). The power defines most relationships that are formed around the media and are practised at multiple levels, individual and collective players, organisations, institutions and networks of connections. Since power is practised at various levels of media activities, relationships of power are multidimensional and complex, especially in light of the emergence of new forms of media practice, such as networked journalism. Networks are defined as "complex structures of communication constructed around a set of goals that simultaneously ensure unity of purpose and execution flexibility by their adaptability to the operating environment. They are programmed and self-configurable at the same time. Their goals and operating procedures are programmed in social and organisational networks, by social actors. Their structure evolves according to the capacity of the network to self-configure in an endless search for more efficient networking arrangements. This definition by Castells suggests that networks are ever changing and evolving towards a higher degree of efficiency, which in turn means a higher degree of power" (Bebawi, Bossio 2014: 125). In the 19th century, groups opposing state authorities created their own means of communication, aware of the role the media plays. An anarchist newspaper, The Truth, published in the USA, may serve as a good example. Its slogan said: "The Truth costs 2 cents, and dynamite is 40 cents a pound. Buy them: read the paper, use the dynamite". Vladimir Lenin also spoke about the establishment of media independent of state authorities. Revolutionary press, both legal and illegal, was needed to "agitate, propagate, and organise". Also, Carlos Marighella argued that, despite reports of the activities of revolutionaries/guerrillas/terrorists in official media, they should establish their means of communication (Chałubińska-Jentkiewicz, 2023a: 249).

5 Concluding remarks

The Internet has become a medium of fundamental importance. Thanks to the Internet and advanced technologies, the arsenal of terrorist communication methods has been extended by multimedia materials, audio and video recordings, blogs, and other websites, utilising numerous interactive tools, such as fora, discussion lists, chats or messaging apps. Furthermore, the properties of websites are favourable to the activities of groupings opposing state authorities. Internet advantages that terrorist organisations may benefit from include a) easy access, b) limited state control, c) the possibility to reach a wide audience, d) anonymous activities, e) the speed of information transfer, f) low cost, g) media convergence (multimedia), and h) the possibility to influence traditional media that often use the Internet to search for information. Relying on these properties of the Internet, terrorist groups use the web to conduct propaganda and publicity operations of the group, gain supporters, communicate within their internal structures, recruit and mobilise terrorists, or acquire funds.

Based on the above deliberations, a conclusion can be drawn that online operations create possibilities to reach a wider public than traditional media. Moreover, the Internet has become a medium resembling a worldwide press agency. Information posted online by terrorists are likely to be used by traditional media and websites. Videos of hostage executions by terrorists or terrorist group leaders' appeals may serve as an example here. Such types of news are published on websites related to terrorists and then spread across the Internet, reaching television, radio and press.

Secondly, it can be stated that disinformation has become a form of entertainment whose advantage over other forms consists in its sensationalist nature. Disinformation actors provide attractive topics to the media which use the opportunity meticulously to generate profit. Reports on activities in Ukraine can be cited as examples of how appropriately selected tactics for presenting acts of terrorists or military operations can affect the market position of a given medium. Hybrid operations are a constant part of Russian strategies towards other countries. Russia relies on various narratives for its propaganda, operations of influence and psychological operations, although they may be grouped by their mutual features (Nowikowska, 2022: 164–165). The attempts to prove the alleged hatred in the mutual relationships between Poles and Ukrainians was a fairly popular trend in disinformation activities. An example of this is a false piece of information that appeared in the Ukrainian and Russian-speaking media sphere in September 2019. It was about an alleged murder of a Ukrainian soldier committed by a Polish soldier. The murderer was to be a Polish instructor from the Joint Multinational Training Group Ukraine, and the offence was said to have been committed in Javoriv near Lviv. The place was not randomly selected. The training ground was crucial not only for security building in this part of Europe but also for Polish and Ukrainian relations in the military sphere. At the time, it was a ground intended for the operations of Joint Multinational Training Group Ukraine, established by Poland, the USA, Canada, Denmark and Lithuania, to support the Ukrainian army to allow them to reach NATO compliance standards (Gliwa, 2022). It is worth noting that, by analysing Polish information space, we can clearly see that military operations were conducted concurrently with activities in the information sphere. Disinformation following the Russian invasion and the refugee crisis that it triggered had two directions. One of them was intended for the Polish information space (addressed to the Polish society), and the other one, referring to Poland, was destined for the global market. Given the second path, we can speak about the attempt to discredit, in the eyes of the international public, the work of Polish soldiers, border guards, and individuals selflessly helping the Ukrainians fleeing war.

Thirdly, online activities seem the best way to gain supporters and potential recruits. Any person keen on the ideology and operational methods of terrorists will search for the information they are interested in on the Internet. Being aware of the fact, terrorists publish a lot of material glorifying their attitudes. Thus, many young and frustrated people might get fascinated by radical views and, in extreme situations, even become new attackers. Information terrorism is a phenomenon which is developing and spreading actively, posing a threat to the entire global community.

Notwithstanding their motives, terrorists' overall objective is to attract the attention of public opinion and to intimidate a large number of people. The media plays a key role in terrorist organisations. Terrorists' strategy assumes, *inter alia*, making as many people worldwide as possible aware of such brutal incidents. Terrorists have effectively used the mechanisms of media influence on the audience for a long time. That is why they plan their attacks in a way that allows them to attract media attention and to place information on a given event on top of the daily information agenda. Information weapons include information resources which are strategically designed or built to conduct information warfare, to cause damage, confusion or inconvenience, or to carry out any other malicious activities. Information terrorism is characterised not only by cyberspace but also by manipulating and falsifying information, and, in some cases, also by creating false facts, as a result of which disinformation occurs to intimidate and evoke paranoid thoughts among the targeted population (Chałubińska-Jentkiewicz, 2023a: 254).

The characteristics of information terrorism include:

- organised violence, a specific type of psychological terror;
- dissemination via the media;
- psychological impact on a wide population;
- attention;
- intimidation and deprivation of the population;
- the surprise effect;
- public and ostentatious nature of operations (Chałubińska-Jentkiewicz, 2023a: 254–255).

Information terrorism may be additionally divided into: a) information and psychological terrorism, or media terrorism (controlling the media to spread disinformation, demonstrating the power of terrorist organisations to destabilise societies), and b) information and technological terrorism or cyberterrorism (damage to a specified part or the whole of the opponent's information environment).

Social media generally serve two basic functions to terrorists: the information and propaganda function and the tactical and operational function. According to a report prepared by experts from the United Nations Office on Drugs and Crime (UNODC), it is possible to list several key areas of Internet use by terrorist organisations: 1. spreading online propaganda, including the recruitment of new members and incitement to terrorist attacks, 2. financing, 3. training, 4. planning terrorist attacks, including the preparation and use of encrypted communications and use of open source intelligence; 5. executing attacks, 6. cyberterrorism. Considering the meaning of the notion of cyberterrorism, it should be stressed that legal commentators have aptly noted that cyberterrorism is something more than just a prefix added to standard terrorist activity (Smarzewski, 2013: 184). According to the definition by K. Liedel, cyberterrorism is a politically inspired attack or a threat of attack against computer information networks or systems, aimed to destroy infrastructure, intimidate governments and individual citizens or impose far-reaching political and social objectives upon them (Liedel, 2006: 36). D. Jagiełło uses a different definition of cyberterrorism, stating that it includes politically or militarily inspired attacks or a threat of attack against information and communication (ICT) systems and networks or collecting data to paralyse or severely damage state critical infrastructure, intimidate or impose far-reaching political and military actions on governments or communities, as well as the intentional use of ICT networks and the Internet by terrorist organisations, national liberation movements and insurgent movements to paralyse national critical infrastructure or to intimidate or impose specified conduct on governments or the population (Jagiełło, 2013: 12). A different approach was suggested by J.A. Lewis who states that cyberterrorism is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation) or to coerce or intimidate a government or civilian population (Lewis, cited in Siegel, Worrall

2014: 638). In this sense, common features of disinformation and cyberterrorism can be observed (Siegel 2012: 385).

Finally, it should be stressed that the World Wide Web, one of the benefits of the digital era, has become a weapon of those trying to combat harmful phenomena and disinformation. The combat against disinformation in cyberspace may become one of the most significant challenges contemporary legislators will need to face. It is worth stressing here that counteracting disinformation should not consist of mass control and censorship of the Internet because the only winners, in this case, would be the enemies of one of the most important individual liberties, i.e., freedom of expression. The procedure for removing and blocking content might become one of the most significant solutions concerning disinformation. According to the currently applicable provisions of the Radio and Television Broadcasting Act, if user-published contents violate the applicable legal regulations, which includes disinformation, hate speech, contents containing aggression, or rules (which users are obliged to comply with under the Act on the Provision of Service by Electronic Means), the platform provider will be authorised to demand that such user remove the said infringements. If the contents are not returned to a legitimate state (through flagging or removal, depending on the type of violation), the platform provider will have the right to block access to such contents to other users. The contents will not be removed from a platform, and only the users who have published the contents will have access to them. After the contents are blocked, they will not be available to the general audience of the contents presented on the platform. Besides, in the event of further infringements by a given user, the platform provider can temporarily block the relevant account (to temporarily block the publication of new content). In the most serious situations, where the user concerned publishes contents that incite terrorism or include child pornography, the platform provider will be able to permanently prohibit such publications, for instance, by liquidating the account. Technology development is a challenge for future legislators and regulators. The responsibility for digital content is becoming the domain of intermediaries.

The most recent law governing this sphere is Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ EU L. 277/1 of 27.10.2022). The DSA retains the responsibility rules applicable to service providers and intermediaries specified in Directive 2000/31/EC on Electronic Commerce, considered the foundation of the digital economy. In the DSA, the term “illegal content” was not defined in detail. As per Article 3(h) of the DSA, “illegal content” means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which complies with Union law, irrespective of the precise subject matter or nature of that law. This means that the identification of illegal content will be determined by the system of values in place in a given Member State (Chałubińska-Jentkiewicz, 2023b: 193). According to the intentions of EU legislators, the DSA will guarantee clear criteria for removing online content, and ensure an effective complaint and redress mechanism in the event of blocking user content and its publication. New obligations arising from the DSA, for instance, those imposed on the providers of online platforms, include the assurance of transparent recommender systems and online advertising, the need to ensure the traceability of business users, the provision of services taking into account the fundamental rights, including the freedom of expression, taking care of appropriate measures to protect against misuse (mechanisms for users to signal such contents, and in the event of platforms mechanisms for cooperation with "trusted flaggers", or the establishments of points of contact aimed to ensure direct communication with Member States' authorities, the Commission, the European Board for Digital Services, and recipients of the services. The objective of the regulation is to protect citizens' rights and prevent disinformation.

New technologies are making us all smarter. Should we be concerned about the linking of existing values and the ever-present domination of technology? In the literature on the subject, it is indicated that, by 2045, humans will have multiplied their intelligence by a billion by connecting their cerebral cortex wirelessly with a new synthetic cortex in the cloud. Questions related to the security of such development and exploitation of this sphere remain unanswered. They are mainly related to transforming citizens into e-citizens, the divergent interests of market and political stakeholders, and the political arena. The most critical issue to resolve is who decides what is wrong and right, i.e., what is legal and why (Kerikma, Rull 2016: 13–14).

Perhaps mediation will become a vital part of combating disinformation, like the procedure for removing and blocking content in media laws. R. Hill identifies several elements of effective negotiations, such as approaches facilitating the achievement of a common position. He describes it as the power-negotiating tactic. The five pillars of the tactic have been described below:

1. "Don't react: go to the balcony". The author warns against excessively emotional reactions that might lead to confrontation. Sometimes, it is better not to react by expressing rigid and extreme positions but to step back and let things cool down before negotiations are resumed.
2. "Don't argue: step to their side". The author suggests not to argue but "turn" to the opposing side. Confronting what seems to be an unreasonable demand from one of the parties, one should not react by restating an extreme position. Instead, we should acknowledge the points both parties agree on and restate calmly our requirements. It is important to overcome suspicion and mistrust.
3. "Don't reject: reframe". In confronting an unacceptable request, it is better not to reject it immediately but to ask why the other party is making it and find ways to restate the problem so both parties can benefit from continuing their negotiations.
4. "Don't push: build them a golden bridge". While approaching understanding in a delicate matter, it is better not to push approval too intensely. Instead, we should find ways to evoke a sense that a shared position has been worked out.

5. “Don’t escalate: use power to educate”. If there is a threat of rejecting a compromise proposal, which could end negotiations, it is better not to escalate the problem through pressure. A more effective solution is to calmly indicate the consequences of the lack of consent and inform the other party about the advantages of the compromise and the problems that might arise if it is not reached (Hill, 2014: 148–150).

References:

Bebawi, S. & Bossio, D. (2014) *Social Media and the Politics of Reportage The ‘Arab Spring’* (New York: Palgrave Macmillan).

Chałubińska-Jentkiewicz, K. (2023a) *Prawne granice dezinformacji w środkach społecznego przekazu. Między wolnością a bezpieczeństwem* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K. (2023b) *Cyberodpowiedzialność. Wstęp do prawa cyberbezpieczeństwa* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Bezpieczeństwo, tożsamość, prywatność – Aspekty prawne* (Warszawa: C.H. Beck).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2022) *Prawo mediów* (Warszawa: C.H. Beck).

Couldry, N. & Curran, J. (2003) *Contesting media power: alternative media in a networked world* (London: Rowman & Littlefield Publishers).

Denning, D. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warszawa: WNT).

Franco, Ch. (2012) *Media Power and the Transformation of War* (London: Palgrave Macmillan).

Gliwa, S. (2022) Polak winny morderstwa ukraińskiego żołnierza? To fake news, *CyberDefence24.pl*, available at: https://cyberdefence24.pl/fake-news/polak-winny-morderstwa-ukrainskiego-zolnierza-to-fake-news (March 20, 2022).

Hill, R. (2014) *The New International Telecommunication Regulations and the Internet* (Heidelberg: Springer-Verlag GmbH Berlin).

Hołyst, B. (2011) *Terroryzm* (Warszawa: LexisNexis).

Jagiełło, D. (2013) Cyberterroryzm, *Edukacja Prawnicza*, (5), pp. 10-14.

Kerikma, T. & Rull, A. (2016) *The Future of Law and eTechnologies* (Switzerland: Springer International Publishing).

Liedel, K. (2006) *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego* (Toruń: Wydawnictwo Adam Marszałek).

Nacos, B.L. (2009) Revisiting the Contagion Hypothesis: Terrorism, News Coverage and Copycat Attacks, *Perspectives on Terrorism*, 3(3), pp. 3-13.

Nowikowska, M. (2023) Tajemnica dziennikarska o dobro procesu karnego, *Palestra*, 5, pp. 101-115.

Nowikowska, M. (2020) *Granice dozwolonej krytyki prasowej działalności osób pełniących funkcje publiczne* (Warszawa: C.H. Beck).

Nowikowska, M. (2022) SYOPS as an element of information warfare, In: Chałubińska-Jentkiewicz, K. & Evsyukowa, O. (eds.) *Information disinformation cybersecurity* (Toruń: Wydawnictwo Adam Marszałek), pp. 163-170.

Siegel, L.J. (2012) *Criminology* (Belmont: Cengage Learning).

Siegel, L.J. & Worrall, J.L. (2014) *Introduction to Criminal Justice* (Belmont: Cengage Learning).

Smarzewski, M. (2013) Bezpieczeństwo państwa jako przedmiot ochrony niektórych przestępstw popełnianych za pośrednictwem sieci teleinformatycznej, In: Dziemianko, Z. & Kijas, A. (eds.)

Bezpieczeństwo współczesnego świata. Edukacja i komunikowanie (Poznań: Wydawnictwo Wyższej Szkoły Handlu i Usług), pp. 173-192.

Smarzewski, M. (2017) Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym, *Ius Novum*, (1), pp. 64-74.