European Research Studies Journal
Volume XXVIII, Issue 2, 2025

pp. 824-852

Information Management in Times of Extraordinary Threats

Submitted 23/04/25, 1st revision 10/05/25, 2nd revision 19/05/25, accepted 30/06/25

Magdalena Majchrzak[1], Monika Mocianko-Pawlak[2], Krzysztof Gorazdowski[3]

Abstract:

Purpose: *The aim of the article is a multi-level analysis of information management in the face of extraordinary terrorist threats.*
Design/methodology/approach: *The aim of the research was achieved by applying the methodology of theoretical and empirical research on the phenomenon of disinformation in Poland. Due to the variety of disruptions in the infosphere and the adopted framework for analyzing the phenomenon, theoretical research covered both management issues, applicable legal regulations, and issues related to security and social order. However, empirical research included groups of internally coherent entities whose functioning and development are based on professional knowledge (police officers) and heterogeneous groups (students).*
Findings: *The research conducted proved that information management requires a specialized and organized information system. Information management can provide numerous benefits as long as the information is accurate, complete and up-to-date. Failure to meet these assumptions may lead to disinformation. Disinformation processes intensify especially in times of extraordinary threats, including those of a terrorist nature, and this has economic, political, social and health consequences. In order to effectively counteract disinformation, it is necessary to introduce systemic solutions.*
Practical implications: *The research results may be an indication for central and local authorities, non-governmental organizations, educational institutions and other entities responsible for building civil society. One of the foundations of developed civil societies is the ability to communicate and trust. Due to the strong and long-term impact of disinformation, these values disappear. Disinformation is often a way of managing information in autocratic (despotic) systems. Therefore, it seems that education in the area of critical thinking skills and verification of received information is necessary to ensure communities based on democratic principles.*
Originality/Value: *In considerations on information management in times of extraordinary threats, an innovative combination of aspects from the field of management and quality sciences, legal and social aspects was used. It is unheard of in Polish and foreign literature devoted to extraordinary terrorist threats. This approach to the problem allows for a broad analysis of the phenomenon, while filling the information gap in this area.*

[1]*Prof., The College of Economics and Social Sciences, Warsaw University of Technology, Warsaw, Poland, magdalena.majchrzak@pw.edu.pl;*
[2]*PhD., Komenda Wojewódzka Policji w Szczecinie, Szczecin, Poland, mtpawlak@o2.pl;*
[3]*PhD., The Jacob of Paradies University, Gorzów Wielkopolski, Poland, kgorazdowski@ajp.edu.pl;*

Keywords: *Information management, disinformation, terrorism, crisis management, criminal liability, social threats.*

JEL codes: *H12, O32, D80, K14.*

Paper type: *Research article.*

Acknowledgments: *We appreciate the effort of the reviewers and business entities' employees, experts who agreed to participate in the study.*

1. Introduction

The beginning of the 21st century was marked by an increase in terrorist threats, which was influenced by the events of September 11, 2001 and numerous subsequent acts of terrorism. At the same time, there is a dynamic development of new technologies, which, when properly used, provide powerful support for humanity, while at the disposal of terrorists they become a powerful weapon.

Changes in the methods of information flow and the lack of systemic control over their content and form have resulted in an increase in the intensity of the phenomenon of disinformation, which is actively used in terrorist activities. In this context, cooperation with the media in the crisis response system becomes increasingly important.

In the face of terrorist threats, legislation that is compatible with the existing operating conditions and awareness of the social consequences caused by disinformation become particularly important. The above premises led to considerations aimed at a multi-level analysis of information management in the face of extraordinary terrorist threats (Velinov *et al.,* 2023; Grima *et al.,* 2023).

The innovative combination of aspects from the field of management and quality sciences, legal and social aspects is unprecedented in Polish and foreign literature on terrorist threats. This approach to the problem allows for a broad analysis of the phenomenon, while filling the information gap in this area.

2. Literature Review

2.1 Information Management in Times of Extraordinary Threats

The information society of the third decade of the 21st century is a reflection of the ongoing social and economic changes. Information has become the most important resource (Drucker, 2000), and its creation, collection and transmission are becoming

particularly important. Valuable and obtained at the right time, it increases the confidence in making the right decisions.

The essence of information was first approached by Claude E. Shannon, who put it in the context of communication theory and mathematics. Information, according to him, was a measure of the reduction of uncertainty in the system after obtaining the news. C. E. Shannon introduced the concept of entropy as a measure of the average amount of information associated with a certain data source. This was a measure of uncertainty or randomness in the set of possible messages.

He also pointed out that the amount of information provided by a message depends on its probability. Less frequent messages carry more information. If the message is certain (probability equal to 1), the amount of information is zero because it does not reduce any uncertainty. Shannon further defined the basic unit of information-bit. According to him, this was the amount of information needed to distinguish between two equally likely events.

Although Schannon's theory does not directly define information, it allows for accurate measurement of the amount of information in messages, which is crucial in many areas of the economy (Shannon, 1948). Börje Langefors (Langefors, 1973) created an information theory that was competitive to C.E. Shannon. In the infological model, he emphasizes that the concepts of "information" and "data" are not the same. Data becomes information only when it is processed and interpreted by the recipient. The main aspects of information systems are included in the TELOS model by B. Langefors, which includes:

- T (Technical): Technical aspects, i.e. hardware and software.
- E (Economic): Economic aspects, i.e. costs and benefits associated with the system.
- L (Legal): Legal aspects, i.e. regulations and legal standards.
- O (Organizational): Organizational aspects, i.e. the organization's structure and procedures.
- S (Societal): Social aspects, i.e. the impact of the system on society.

These aspects are important in understanding information. Data in itself has no information value until it is interpreted in the appropriate context.

In addition to the above-mentioned theories, both in Polish and foreign literature on the subject, there are many definitions of information. Information can be viewed as a representation of the past, present and future. It is associated with identification processes and is considered a measure of complexity and diversity as well as a causative and controlling factor (Oleński, 2000).

Therefore, information describes reality and facilitates effective action. Information is also a specific presentation of events, states of affairs, objects, etc., from the

perspective of the past, present or future. Its structure consists of four elements, namely: content, carrier, symbol by which the information is recorded, and the method of its transfer (Czekaj (red.), 2012). According to Bogdan Stefanowicz:

1) information is an intangible concept and its disclosure requires data;
2) from an infological perspective, it can be treated as a relationship;
3) it exists independently of subjective reception, so it is objective;
4) has different meanings for different recipients;
5) is a reflection of a certain feature of the object or a fragmentary description of it;
6) is a model of a specific section of reality;
7) shows the feature of synergy;
8) is combined by recipients with other information known to them;
9) although it is not energy, it is subject to quantitative measurement;
10) shows diversity resulting from the different objects under consideration, the variety of sources, and the interpretative subjectivity of recipients;
11) is subject to duplication and transfer in time and space, as well as processing, it is not destroyed, but only distorted and deformed;
12) it is an inexhaustible resource, which results from the possibility of duplicating it, an infinite number of objects and their infinite complexity;
13) obtaining, storing, transmitting and sharing information requires certain costs;
14) the distribution of information in the environment is uneven, which causes its asymmetry, i.e., unequal availability for different recipients due to the sources and costs of obtaining it, preferences in determining facts and other factors (Stefanowicz, 2010).

Information comes from data that has been processed so that it becomes useful in making management decisions (Martin, and Powell, 1992). It is also presented in this context by Adam Stabryła. Its purpose is to provide users with information about specific needs. Information management includes identification, diagnostic and decision-making functions as well as specific functions such as: planning information needs and resources, IT supervision, controlling information technology processes, coordinating the work of task teams (Stabryła (red.), 2018).

The role of information management is therefore to acquire, store and deliver the right information to the right people at the right time (Krztoń, 2017). Information management exhibits the features identified by M. Świgoń:

- concerns explicit knowledge contained in books, magazines, patents, databases and others,
- the key factors are: speed, responsibility, cost, storage, search and manipulation of data and information,
- focuses on managing structured and formalized information that is easy to identify, organize and distribute,
- information is managed for use by individuals or institutions (Świgoń, 2012).

Information management is an extensive process that involves collecting, storing, sharing, protecting, analyzing and using information in a way that supports the goals and activities of an organization or entity.

Table 1. *Elements of information management*

Elements of information management	**Interpretation**
Information collection	The process of identifying information sources and collecting data. It may include internal data (e.g. financial reports, employee databases) and external data (e.g. market reports, information from customers).
Information storage	It concerns the management of the place where information is stored. This may be both physical storage of documents and digital storage of data on servers, in the cloud or on data carriers.
Sharing information	Enabling access to information to appropriate people in the organization, while ensuring an appropriate level of security and access control. It is important that information is available in an understandable and useful form.
Information protection	Ensuring that information is protected against unauthorized access, loss or damage. This includes both technical aspects (e.g. security of IT systems) and organizational aspects (e.g. information security policies).
Analyzing information	The use of analytical tools and statistical methods to process collected data, which allows drawing conclusions and supporting decision-making processes.
Use of information	Practical application of collected and processed information to achieve the organization's strategic goals, make operational decisions and optimize business processes.

Source: *Own study based on: R. Borowiecki, J. Czekaj (ed.) 2012, p. 29; M. Pańkowska 2001, p. 16.*

The efficiency of the information management process depends not only on fulfilling the basic functions described in table 1. Information management requires a specialized and organized information system, which includes, among others:

- continuous updating and compilation of information helping the company to quickly respond to the changing reality inside and outside the organization,
- providing useful information to recipients in a form suitable for immediate use,
- taking into account technological progress, e.g. the possibility of computerization of methods of collecting, processing, storing and flow of information,
- providing options for tracking the course of processes taking place in subsequent areas of activity, thanks to the speed and frequency of data circulation, effective use of information is guaranteed, data should be up-to-date, complete and segregated, these features help their proper diffusion,
- securing information (Czekaj (ed.), 2012).

Information management can bring numerous benefits provided that the information itself meets certain conditions, namely it is accurate (reflects reality), complete (provides the recipient with all available facts) and current (available in time for action). Failure to meet these assumptions may lead to disinformation understood as misleading. It may take the form of: misinformation, disinformation and malinformation.

Misinformation refers to the transmission of false information unintentionally (Pennycook, Mcphetres, Zhang, Lu, and Rand, 2020). Disinformation means information that was intended to be deliberately misleading (French and Monahan, 2020). Malinformation, in turn, means the reconfiguration of real information (Brennen, Simon, Howard, Kleis, and Nielsen, 2020). Malinformation differs from disinformation and misinformation in that it is based on real facts, which are, however, presented in such a way as to mislead and harm the reputation of a person, organization or group.

The effects of social disinformation (in any form) may include:

- undermining trust in institutions (government, media, experts, scientists),
- social polarization (division of society, intensification of social tensions),
- impact on public health (false medical advice, lack of trust in vaccinations),
- disruption of democratic processes (manipulation of election results, weakening public debate),
- economic consequences (decrease in consumer confidence, disruption of financial markets),
- psychological effects (stress and uncertainty, sense of threat),
- weakening of international relations (international conflicts, breaking of cooperation).

Disinformation processes intensify especially in times of extraordinary threats, including terrorist ones. Society and services function in a different way than the standard one. The role of the media is then enormous, as they can often have a positive impact on calming social moods and, as a result, also on the effectiveness of anti-terrorist services and state structures. Journalism and the media, by acquiring and transforming news and data, give them certain features that have the value of specific knowledge (Borowiecki and Kwieciński (ed.) 2003).

Therefore, false or incorrectly provided information, which, among others: thanks to the Internet and social media, they spread very quickly and may contribute to the infopandemic effect (Sztuba, Mirek-Rogowska, Rączy, 2021).

One solution may be sustainable information management interpreted as a series of integrated processes and practices that ensure effective, responsible and sustainable management of data and information.

The key elements of sustainable information management are:

1. Identification and classification of information, including:
- information audit. Conducting a detailed audit to identify all the data and information the organization has.
- data classification. Defining data categories (e.g., public, internal, confidential) for better management and protection.

2. Data management, including:
- data collection. Collecting data in a legal and ethical manner, taking into account the principle of data minimization, i.e., collecting only the information that is necessary.
- data storage. Ensuring safe and effective data storage, including retention and archiving policies.

3. Data processing and analysis including:
- process automation. The use of modern technologies to automate data processing processes, which increases efficiency and reduces costs.
- data analysis. Using analytical tools to process data and generate valuable conclusions that support decision-making.

4. Data protection and information security, including:
- data protection measures. Implementation of advanced technologies and procedures to protect data against unauthorized access, loss or damage.
- risk management. Identification of potential threats and implementation of risk management strategies.

5. Compliance with regulations and standards, i.e.:
- legal regulations. Compliance with local and international data protection and privacy regulations (e.g. GDPR in the EU, HIPAA in the US).
- norms and standards. Implementing international standards such as ISO/IEC 27001 to ensure a high level of information management.

6. Transparency and ethics:
- transparency. Informing interested parties about the methods and purposes of collecting and processing data.
- code of ethics. Develop and adhere to a code of ethics for information management that addresses privacy, responsibility and integrity.

7. Education and awareness, including:
- training. Regular training for employees on best practices in information management, data protection and information security.
- information campaigns. Conducting educational campaigns among stakeholders to increase awareness of sustainable information management.

8. Monitoring and continuous improvement:
- monitoring. Regular monitoring and audits of information management systems to assess their effectiveness and compliance with regulations.
- continuous improvement. Making improvements based on monitoring and audit results to adapt processes to changing requirements and technologies.

9. Stakeholder engagement:
- cooperation. Engaging all key stakeholders, including employees, customers, business partners and local communities, in the information management process.
- feedback. Regularly collecting feedback from stakeholders in order to adapt the information management strategy to their needs and expectations.

Sustainable information management is an approach that involves the effective and responsible management of data and information in a way that supports the long-term goals of the organization, society and the environment.

The aim of this approach is not only to optimize processes related to information processing, but also to ensure that information is managed in an ethical, transparent and consistent manner with the principles of sustainable development.

2.2 Criminal Liability for Propagating Disinformation in the Media

Information is one of the most powerful weapons on the modern battlefield, not only in times of war, but also in times of peace. Modern conflicts take the form of the so-called "hybrid war", i.e., activities combining elements of military and non-military activities, an important element of which is disinformation and propaganda, which constitutes a serious challenge to the contemporary security of states, including the security of the Republic of Poland (Kacała, 2015).

Disinformation in Poland, with particular emphasis on fake news, constitutes a significant challenge in terms of legal regulations. The legislator is expected to take appropriate actions that would reduce the prevalence and threats associated with this phenomenon.

Disinformation affects many aspects of social life, therefore creating the need to develop appropriate legal frameworks and regulations, both at the national level and internal regulations, e.g., those governing the most popular social networking sites. In the legal context, it is possible to identify several key aspects related to disinformation and fake news in Poland.

Disinformation often violates the personal rights of individuals, such as good name, privacy or human dignity. Polish law contains regulations regarding media activities, including the principles of reliable journalism. An important value is providing information truthfully and respecting the principles of journalistic ethics.

Violation of these rules may lead to legal liability under criminal or civil law. There are provisions in Polish law that allow for claims for the protection of personal rights in the event of publication of false information that may damage reputation or violate privacy.

In some cases, disinformation may constitute a crime, such as fraud or defamation. Polish criminal law provides for the application of sanctions against persons responsible for disseminating false information in order to obtain material benefits or cause damage to others (Article 286, Article 212 § 1 of the Criminal Code) or in the form of offenses, e.g. misleading an authority or institution (Article 65 of the Criminal Code), causing a false alarm (Article 66 of the Petty Offence Code).

In terms of regulations regarding social media, the Polish legislator has introduced provisions regarding the activities of those who operate them. online platforms that oblige these entities to effectively combat disinformation. The introduction of such regulations is an attempt to limit the spread of fake news in the online environment. As part of the fight against disinformation, it is also important to shape legal awareness in society. Legal education can help citizens recognize fake news and understand its legal implications.

A special type of threat caused by the deliberate and conscious dissemination of false information is facilitating or even enabling a terrorist attack by effectively diverting attention from the actual source of danger or causing a lower level of sense of security among citizens of the attacked state in order to reduce trust in its legal authorities. and causing civil disobedience or panic.

In the Act of June 6, 1997, the Criminal Code, disinformation in the context of threats to state security, including those of a terrorist nature, was penalized in Art. 130 § 9 and in Art. 132 of the Criminal Code. The legal definition of a terrorist offense is contained in Art. 115 § 20 of the Criminal Code, which states directly that it is a prohibited act punishable by imprisonment of at least 5 years, committed or the threat of its commission, undertaken in order to:

1) seriously intimidating many people,
2) forcing a public authority of the Republic of Poland or another state or a body of an international organization to take or refrain from taking specific actions,
3) causing serious disturbances in the political system or economy of the Republic of Poland, another country or an international organization.

A special provision sanctioning disinformation in the context of terrorist threats is Art. 130 § 9 of the Criminal Code penalizing behaviour consisting in taking part in the activities of a foreign intelligence service or acting on its behalf, conducting disinformation, consisting in disseminating false or misleading information aimed at causing serious disruptions in the system or economy of the Republic of Poland (RP), an allied state or an international organization of which the Republic of Poland

is a member, or persuading a public authority of the Republic of Poland, an allied state or an international organization of which the Republic of Poland is a member, to take or omission of certain activities.

This provision entered into force on September 23, 2023 under the Act of August 17, 2023 amending the act -The Criminal Code and certain other acts (Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz. U. 2023 poz. 1834)). From the parliamentary justification for the bill of the cited Act of April 17, 2023 (Parliament Paper No. 3232), we can conclude that the change in legal regulation was necessary to adapt the features of the crime of espionage to the constantly changing geopolitical situation, technological progress, as well as constant modifications to the methods of operation of potential perpetrators. prohibited acts described in Art. 130 of the Criminal Code (Uzasadnienie do Poselskiego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, druk no. 3232 z 17 kwietnia 2023 r.).

It is worth adding that in Polish criminal law the behavior of taking part in foreign intelligence was already known as one of the forms of espionage under the Criminal Code of 1932. (Article 7) and the Criminal Code of the Polish People's Republic of 1969 (Articles 122, 124-125, 128-129) (Taras, 1970). Of course, these regulations had a political tinge and their discussion is not useful for the considerations, because their adoption had no value of legislating in the system of a democratic state, especially the indicated provisions of the Criminal Code of 1969.

Before assessing the legal regulations in force in Poland in the context of penalizing the dissemination of false information as a crime, the concept of disinformation should be defined. This concept is relatively new, it is believed to have originated in Russia in 1923, although intuitive methods and techniques of disinformation were used much earlier.

The theory of disinformation was thoroughly described by Vladimir Volkoff. The above researcher elevates disinformation to the rank of a doctrine, while calling misleading only a technique (Volkoff, 1991). The term disinformation itself was used in a publication in the London monthly*„The Whitehall Gazette& St James`s Review"* w 1926 (Brzeski, 2014).

Examples of disinformation operations (conducted, among others, by the Eastern Bloc) were described, for example, by Anatoly Golitsyn and Ion Mihai Pacepa, who defined disinformation (by which he meant the strategic disinformation of the USSR, mainly since 1958) as systematic efforts aimed at spreading false information and falsifying or blocking information regarding the actual situation and policy of the communist world.

As a consequence, disinformation practices were intended to confuse, mislead and bias the non-communist world, to undermine its policy and to induce the Western

adversary to unknowingly contribute to the achievement of communism's goals (Golicyn, 2007).

In Polish literature, the concept of disinformation appeared for the first time in 1929 in the Instruction of the Second Department of the Main Staff of the Polish Army, defining it as providing the enemy's intelligence with messages concealing one's own intentions and forcing him to treat the information provided by his own intelligence as true, or forcing the intelligence alien to analyze inspired messages for a longer period of time (Wachowicz, 2019).

The essence of disinformation is the provision of false information for a specific purpose, which is the basis for such action, and therefore, in the legal and forensic aspect, it is necessary to look at the purposes for which it is used. As M. Konieczny points out, the purpose of disinformation is the broadly understood benefit of the entity that uses it. The benefit is the effect of disinformation, which consists in providing the disinformed person with some apparent knowledge that does not refer to facts or distorts reality, while making the recipient believe in its authenticity and credibility.

The perpetrator undertakes such an action in order to achieve a previously established goal, which is what determines the direction of disinformation, e.g. persuading the person to whom the information is provided to take certain actions (Konieczny, 2021). Disinformation is characterized by systematic actions, professional preparation and organization, and consistent use of mass media.

In fact, it is the implementation of a consistent program whose goal is to replace views identified in the consciousness and even subconsciousness of the mass recipient with falsified content. The recipients of disinformation consisting in replacing unfavorable views from the disinformer's point of view with desirable and previously prepared views are entire populations, not individual people (Kacała, 2015).

Disinformation messages may take various forms: textual or audiovisual, they may be disseminated consciously or unconsciously, but they will always have a negative impact on the recipients by influencing the change of judgments, opinions, decisions or strengthening a specific worldview. Trolls, bots, but also opinion leaders, politicians and journalists supporting a specific political trend may take part in their dissemination. The purpose of disinformation campaigns may be, among others: polarization of society by imposing narratives that arouse a sense of threat and fear, reinforcing anti-scientific theses or antagonizing specific people or groups, such as aggressive messages against Ukrainian refugees, media photographs of immigrants of a specific skin color, arousing fear of radiation, religious or other threats (Kodeks Dobrych Praktyk w zakresie dezinformacji, https://www.nask.pl/pl/aktualnosci/4992,Powstal-Kodeks-Dobrych-Praktyk-w-zakresie-dezinformacji.html?search=16089815518).

According to the already mentioned V. Volkoff, the following tools can be distinguished, aiming to achieve the same goal as disinformation, although different from it, namely:

- deception – (subversive actions), i.e., constant threats to distract the enemy and attack in a more vulnerable place;
- intoxication – (misleading), e.g., the action of the Persians who, by retreating, effectively misled the Trojans into believing that the artificial horse was a gift to be taken to the city;
- open propaganda - (white propaganda), i.e., open action aimed at reducing the enemy's morale and strengthening the fighting spirit of supporters, which may also convince people who have not yet been decisive in the conflict to participate in the fight;
- secret propaganda – (black propaganda) hidden, covert activities that take the form of real information, usually the source of the information is hidden and therefore it is not known whether the information comes from an enemy, an ally or third parties.
- influence – a more subtle method than secret propaganda, which involves an agent influencing the course of events in such a way that they harm the enemy state; the agent is an agitator with the general goal of destabilizing society (Volkoff, 1991).

It is worth looking at this list from the point of view of the achievements of the jurisprudence of common courts. In the judgment of the District Court in Warsaw of March 20, 2017, i.e., passed before the amendment of the Criminal Code of 2023, in point 4 of the operative part we find an example of the description of a prohibited act, which could currently meet the criteria of Art. 130 § 9 of the Criminal Code, namely: (...) participated in military intelligence activities (...) directed against the Republic of Poland by holding operational meetings with designated officers (...) and, after prior intelligence training, undertook carrying out the tasks assigned to him by the officers (...) consisting of: (...) propaganda activities involving the publication in the media of articles consistent with the official policy of the Federation (...) and depreciating the activities of the Polish side in the field of energy (...), including:

- identified the mass media in Poland - journalists and experts from the energy industry and prepared a study containing their characteristics in terms of their susceptibility to Russian influence and the possibility of using them in an information campaign regarding energy based on Russian assumptions, and then took actions to promote the Russian point vision in the energy sector by offering payment for such publications;
- inspired the writing of the pro-Russian and anti-Polish article "(...)" and its publication in influential industry media (Wyrok Sądu Okręgowego w Warszawie XII Wydział Karny, sygn. akt XII K 91/16

https://orzeczenia.warszawa.so.gov.pl/details/$N/154505000003606_XII_K_000091_2016_Uz_2017-05-23_001).

In view of the provisions of Article 130 § 9 of the Criminal Code, which defines a qualified form of the crime of espionage (constituting a crime punishable by imprisonment from 8 to 30 years), it should be noted that the type of participation in the activities of a foreign intelligence service is not the same as activity on behalf of a foreign intelligence service. Taking part in the activities of a foreign intelligence service means consciously participating in the activities undertaken by a foreign intelligence service, as well as belonging to its organizational structures, e.g. as an informant, a person recruiting or collecting information.

At the same time, participation in the activities of foreign intelligence does not require formal accession to it, because an important element defining this participation is the actual bond between foreign intelligence, which is usually personified by an officer, a leading agent, who is an officer of the intelligence services, and the perpetrator.

In the justification of the judgment issued in case no. No. XII K 91/16, it was indicated that "the lack of a requirement to formally confirm membership in a foreign intelligence service, resulting from the interpretation of the statutory definition of 'participation in the activities of a foreign intelligence service', is obvious, taking into account the specific nature of the activities of a foreign intelligence service, which involves taking non-transparent activities, especially towards authorities and citizens of the foreign country in which it conducts intelligence activities. In the case in question, pursuant to the Crimnal Code of 1997, the Court of Appeal in Warsaw issued the most severe sentence for espionage (reference number XII 91/16), sentencing the accused to 7 years' imprisonment.

In order to attribute the features of this act to the perpetrator, it is necessary to conduct disinformation, consisting in disseminating false or misleading information in order to cause serious disruptions in the political system or economy of the Republic of Poland or to induce a public authority of the Republic of Poland, an allied country or an international organization of which the Republic of Poland is a member. , to take or refrain from taking certain actions. The condition for attributing the commission of an act under Art. 130 § 9 of the Criminal Code is the perpetrator's act of willful misconduct with direct intent.

The letter of May 16, 2023 containing comments of the Helsinki Foundation for Human Rights and the Panoptykon Foundation on the draft act amending the Act - Criminal Code and certain other acts indicates difficulties that may arise on the part of law enforcement authorities related to the binding demonstration that the disinformation was intended to cause serious disruptions in the political system or economy of the Republic of Poland or another state or international organization (Kładoczny, 2013).

This remark is particularly important in the context of using disinformation in the information fight against an enemy state or organization, or even in the context of terrorist threats - conducting deterrent activities using false information. In particular, the features of this act would include the activities of double agents, which can hardly be considered the legislator's intention.

Disinformation in warfare most often aims to gain an advantage over enemy troops. „War is based on deception*"* (Tzu, 2003), therefore, in this type of activities, intelligence disinformation is a necessary element, because thanks to false information you can influence the development of an unfavorable enemy strategy and thus increase your own chances of victory. It is worth remembering that the crime of disinformation is inextricably linked to the concept of "espionage" (Iwiński, Rosenau).

The legislator in Art. 130 § 6 of the Criminal Code, as if in response to the above comments and requests of representatives of the secret services, introduced a new type of espionage, not yet penalized in Poland, regarding the control of the activities of foreign intelligence services on the territory of the Republic of Poland, not directed against the Republic of Poland.

This provision constitutes a specific counter-type exempting from criminal liability persons participating in foreign intelligence activities not directed against the Republic of Poland, if they obtain consent to such activities from the competent authority. These issues are regulated in the Act on Internal Security Agency and Intelligence Agency and the Act on Military Counterintelligence Service and Military Intelligence Service (Hoc, 2023).

During the amendment of criminal law, doubts also arose regarding the impact of criminalization of disinformation on the functioning of freedom of speech and the question of whether disinformation should not refer only to the territory of Poland and be prosecuted only in this territory.

There are also practical problems, such as with the current wording of Art. 130 § 9 of the Criminal Code, law enforcement authorities are to demonstrate that the disinformation was intended to cause serious disruptions in the political system or economy of the Republic of Poland or another state or international organization (Hoc, 2023).

However, it seems that from the point of view of the purpose of spreading disinformation and fake news in contemporary conflicts, including those included in the catalog of tools used by terrorists, which also include disruption of democratic processes, polarization of society, undermining its position in the international arena, including building reluctance, opposition or lack of trust among citizens towards the ruling group, such regulation is necessary.

Of course, a discussion on changing criminal law is still needed, but it must be accompanied by serious arguments resulting from doctrine and practice, and it cannot only be utilitarian considerations of the secret services (Hoc, 2021).

P. Burczaniuk (2024) points out that the amendment to the provisions of the Criminal Code, including, among others, the use of new concepts in the definition of prohibited acts, including: such as disinformation, which have not yet appeared in the legal system, including many ambiguous concepts and susceptible to different interpretations, will have to be verified in terms of their effectiveness in the course of applying the law, in particular in the context of possible decriminalization of a specific spectrum of behaviors recognized by the services as hybrid threats conducted by foreign special services (Burczaniuk, 2024).

This is especially true since disinformation activities have been undertaken particularly frequently in recent years, e.g. by the Russian Federation. An example is the Russian Troll Factory (Internet Studies Agency) created by Yevgeny Prigozhin (https://www.wprost.pl/swiat/11095837/to-jewgienij-prgozyn-stworzyl-rosyjska-fabryke-trolli-ingerowala-w-wybory-w-usa.html).

Another provision regulating the issues of disinformation is Art. 132 of the Criminal Code. According to it, the perpetrator who, while providing intelligence services to the Republic of Poland, misleads the Polish state authority by providing counterfeit or forged documents or other items or by concealing true or providing false information of significant importance for the Republic of Poland is subject to criminal liability.

Only those who, using the tool of disinformation, inflict it against the Republic of Poland will be subject to punishment, hence this provision penalizes behavior consisting in acting as part of intelligence disinformation. The legislator left a certain possibility of broader criminalization of behavior by using specific methods of committing a prohibited act, i.e. hiding true or providing false news that is important for the Republic of Poland, which theoretically allows for the prosecution of disinformation also transmitted in the media.

On this basis, it can be assumed that providing information that harms the state through the media, especially false information, is penalized. The crime of disinformation is of an individual nature, which means that the perpetrator of this crime can only be a person who acts as part of intelligence services of his own free will. The provision in question is related to covert intelligence activities and potential disinformers are again used as the so-called "double spies", hence the case law in this area is quite poor, as it does not reach wider public knowledge (Iwiński, Rosenau).

An unresolved issue is the possibility of bringing criminally liable people who spread disinformation in a conscious manner, although not meeting the criteria of a

crime under Art. 130 § 9 or art. 132 of the Criminal Code, or other provisions, such as, for example, Art. 212 § 1 of the Criminal Code, art. 286 of the Criminal Code, or Art. 65 or art. 66 of the Petty Offence Code, when the purpose of their actions is solely to achieve a particular, often party (politicians) or economic (politically engaged journalists) interest, most often associated with gaining or maintaining power or profit.

Unfortunately, despite the horrendous social costs described later in this study and the often thoughtless endangering of the country's internal security and weakening its effectiveness in counteracting hybrid and terrorist threats, the dissemination of false information - under the banner of freedom of speech or the right to criticize - is allowed and, in principle, unpunished .

3. Materials and Methods

Disinformation, as a disruption of the information flow process, is important for the effectiveness and efficiency of management. At the same time, considered as a legal fact, it determines the need to analyze applicable legal provisions in order to assess the effectiveness of the adopted regulations as the state's response to the disruptions to the established order determined by them.

However, from the point of view of security and social cohesion, the phenomenon of disinformation triggers the need to define the sources of society's susceptibility to this type of negative impact and the social consequences it causes.

Since this article is of an interdisciplinary nature, the adopted methodological assumptions, which are applied in such sciences as management sciences, legal sciences and social sciences (sociology and security sciences), are also complex.

Verification of the research hypothesis and implementation of the assumed research goal will take place through:

1. Theoretical identification of variables determining the effectiveness of disinformation in disorganizing information flow models adopted in management.
2. Review of scientific literature in the field of management sciences, law sciences and in the field of sociology and security, describing the phenomenon of disinformation and presentation of the authors' position.
3. Critical analysis of legal literature, including the jurisprudence and interpretation in force in Poland, and identification of revealed gaps in the law.
4. Empirical research method, i.e. cross-sectional and casual observation, including participant observation.
5. Qualitative analysis of social phenomena defined as the effects of

dissemination of disinformation, and as a result, inductive reasoning, determination of proposed solutions aimed at minimizing the effectiveness of disinformation both in the context of management, implementation of legal functions, as well as security and social order.

The research objectives will be achieved by using the following methods and techniques:

a. logical methods used: deduction and induction, in order to verify the correctness and coherence of all components of scientific and research work, and then check the hypothesis;
b. a critical approach to the issues presented by current science, in particular through a critical analysis of the literature on the subject and false information published on the Internet along with comments;
c. participant observation of social groups and their reactions to false information, including readiness to verify information;
d. conducting casual interviews with representatives of the observed social groups and in-depth interviews with experts.

The choice of research methods and techniques results from the interdisciplinarity of the undertaken research activities, on the one hand, and, on the other hand, it is a consequence of the multi-aspect approach to the undertaken issues (J. Sztumski, Introduction to methods and techniques of social research, Śląsk Sp. z o. o., Katowice 1999, W.W. Skarbek, Selected issues in the methodology of social sciences, Naukowe Wydawnictwo Piotrkowskie, Piotrków Trybunalski 2013).

Participant observation was carried out in a professional group (policemen) and in groups of security and criminology students (University of Szczecin, Academy of Applied Sciences TWP in Szczecin). The in-depth interview technique was carried out with security experts from Szczecin universities and the West Pomeranian Police.

Susceptibility to disinformation is an individual feature, depending on the level of knowledge in a given field and the level of development of critical thinking skills, therefore, taking into account the diversity of representatives of both selected groups, participant observation of reactions to false information allows drawing conclusions regarding the negative social consequences of the phenomenon of disinformation.

Detailed interviews with experts allow for verification of the correctness of observations, assessment of the context and understanding of social reality, and formulation of recommendations, including defining threats to the social order and methods of counteracting these threats. The sample was selected using the expert method, based on the knowledge and experience of specialists in the field

of the phenomenon under study.

Free interviews with experts were conducted in the second and third quarter of 2024 based on the results of participant observation. Free interviews with experts complemented the observations conducted in groups of students and police officers.

In the area of analysis of the applicable legal order, a detailed, critical analysis was carried out not only on the legal provisions in force in Poland, with a focus on the provisions of the Act of June 6, 1997, Penal Code (consolidated text: Journal of Laws of 2024, item 17), but also case law in the context of criminal liability for propagating disinformation in the media.

The justification of the judgment of the District Court in Warsaw, 12th Criminal Division of March 20, 2017, issued in case no. file XII K 91/16 and the judgment of the Court of Appeal in Warsaw of November 2017, issued in case no. act II AKa 269/17 with a commentary by Stanisław Hoc.

The practical dimension of the application of law combined with the analysis of changes introduced by the legislator in the legal system allow the formulation of conclusions including the diagnosis of legal loopholes (extra legem, intra legem, contra legem) in the law in force in Poland, as well as the desired directions of amendment.

All the empirical research conducted complements and verifies the conclusions from theoretical research on the subject literature.

Since all social science disciplines are interdisciplinary in nature, the added value of this article, in the methodological context, is the use of the potential and achievements of such social sciences as: management sciences, law, sociology and security sciences.

While emphasizing the interdependence of the above-mentioned sciences in the study of the phenomenon of disinformation, it is impossible not to emphasize that broadening the spectrum of research conducted increases the complementarity of this study in the context of the analysis and conclusions regarding its understanding, determinants and social consequences. Disinformation, thanks to an interdisciplinary approach, can also be analyzed in the spectrum of related human social problems.

4. Discussion

The beginning of the 21st century is not only a rapid development of new technologies, in particular ICT, but also a new era in the context of the development of methods and techniques used by terrorists. The year 2001 defines the entry into a

higher level of terrorist threats. The attack on the World Trade Center in New York carried out by Al-Qaeda on September 11, 2001 made everyone aware that the threats in question are global and virtually every person, anywhere in the world, can potentially experience the effects of a terrorist attack.

Already during the 3rd Public Media Conference "Media towards terrorism" organized by the supervisory boards of Telewizja Polska S.A. and Polskie Radio S.A. on September 10-11, 2002, i.e. on the first anniversary of the attack in the USA, the Chairman of the National Broadcasting Council, Juliusz Braun, emphasized that in the global information society, the rank and significance of an event is determined not so much by the event itself, but by its reflection and multiplication in the media (Sprawozdanie Krajowej Rady Radiofonii i Telewizji z rocznego okresu działalności, Warszawa 2003, https://orka.sejm.gov.pl/druki4ka.nsf/($vAllByUnid)/06C8FB6E717C586CC1256CFE00324BF0/$file/1476.pdf).

The observed changes in the tactics of attackers and terrorist organizations clearly indicate the deliberate use of the media and the developing Internet as a tool to intensify fear, spread panic and influence social mood. Particular activity in this respect is observed primarily in the area of disinformation activities focused on shaping radicalized social attitudes, polarization and reducing social cohesion.

Natalia Hatalska (2022) points out that in a polarized society, disinformation spreads more widely, faster and more intensively, because warring groups do not maintain contact with each other, but only perpetuate negative, often false information about themselves. Polarization of society facilitates destabilization, because as it increases, trust decreases on every level: interpersonal, in all legal authorities, in institutions and administrative bodies, including the loss of trust in the democratic system (Hatalska, 2022). Polarization promotes aggression in all its forms, significantly hinders social communication, which in turn leads to antagonism and anomie. Such social phenomena not only facilitate terrorist activities, but are now their goal and effect.

The consequence of exploiting fears, intensified in a society suffering from anomie, is an increase in mobilization focused on ensuring security. Such activity intensifies due to the strengthening of the sense of the omnipresence of dangers in the form of unpredictable events and behavior of people perceived as enemies that must be fought (Kozlova, 2013).

Referring to the definition of Albert Pawłowski, who postulated that "terrorism should be understood exclusively as the use of violence by individuals or groups of people in order to influence both the government and public opinion, as well as groups of people and individual" (Karolczak, 1995) and defined seven rules accompanying this phenomenon, including the following: "a violent act here - apart from a few and specific cases - has a spectacular character, because publicity

(mainly through the press, radio or television, but not only) constitutes both a 'broadcast' , as well as an "amplifier" of the power and range of influence of terrorists" (Kaczmarek, 2001), it is noticeable that the popularization of information about the attack was and still is of great importance for achieving the attacker's goal. It is worth emphasizing that A. Pawłowski's publication dates back to 1980, i.e. before the spread of the Internet.

The assumptions for the National Anti-Terrorism Program for 2015-2019, developed at the Ministry of Interior in 2014, indicate that terrorism is an international threat, one of the main threats to global, regional and individual state security. The authors of the above Program they noted that, and I quote: "the variability of the methods used by terrorists means that we must have appropriate instruments to properly recognize and assess threats and effectively counteract possible incidents.

In the event of a terrorist attack, we must be prepared to take immediate and adequate measures to respond and eliminate its effects. Achieving these goals requires close and comprehensive cooperation not only of all services, local bodies and institutions, the mass media, the private sector, non-governmental organizations and the entire society" (Uchwała Nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019" (Dz. Urz. 1218M.P. z 2014 r. poz. 1218)).

Terrorists, like every human being, use the achievements of science and new technologies, acquire new skills in order to carry out an attack in an unexpected, brutal way and often with live broadcast via traditional and social media. As Krzysztof Karolczak points out, I quote: "Over two thousand years of recorded history, terrorists' methods of operation have changed with technological progress, but it was rather the addition of new tools to existing, proven ones" (Karolczak, 2022).

A globalized world characterized by sources of uncertainty and threats in the political and existential dimension, devoid of physical values that cannot be seen with the eye, including: such as migration and terrorism, as well as the collapse of hierarchical models of knowledge transfer, result in a trust deficit and are a source of the so-called post-truth era. The previously dominant culture of knowledge has been replaced by a culture of threats, based on a network of collective strategies used to first create and then maintain a state of tension and fear.

Theoretically, social media make it possible to publicize the opinions of people who did not have their own representation in traditional media, but at the same time their expectations, expressed dissatisfaction or frustration are used to take political control over them (Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich, Think Tank Parlament Europejski, source: https://www.euro-parl.europa.eu/thinktank/pl/document/IPOL_STU(2019)608864).

The social environment shaped in such conditions is extremely susceptible to manipulation and disinformation, especially by professionals, who often include members of terrorist organizations.

Grzegorz Bator and Monika Knapik point out the possibility that currently up to 90% of terrorist activities on the Internet take place via social media, and a significant part of terrorist activities in cyberspace consists in disseminating propaganda, thus enabling the recruitment or radicalization of people who may become terrorists or conduct activities intelligence activities involving the identification of people and places that may be the target of a planned attack (Bator, Knapik 2020).

When diagnosing the social conditions that enable the unrestrained development and dissemination of disinformation, attention should be paid to the fact that it is widely used not only by terrorists, but also by legally functioning power elites. Rafał Brzeski sees the reasons for the effectiveness of this state of affairs in a kind of ignorance by choice, the model of which he built on four elements:

1. citizens received imperfect information - information that was incomplete or devoid of situational context,
2. citizens are aware that they have imperfect information - the information obtained is clearly distorted or questionable, the source of the information has not been indicated or is questionable,
3. high costs of information verification - this element also includes the cost of obtaining additional information as well as the analysis and evaluation of additional information,
4. the expected benefits will be lower than the costs incurred to verify the information - citizens are aware that the cost of confirming the information received will be higher than the profit from undertaking verification activities (Iwiński, Rosenau).

Based on the assumptions of the above model, societies in which public opinion is formed on the basis of information, not facts - the threat of disinformation is growing, and undesirable actions from the point of view of security and resilience in crisis situations are becoming more important.

Additionally, modern society, known as the information society, operates in an environment overstimulated with information, which causes the phenomenon of information noise. Such conditions also significantly facilitate the use of disinformation, which uncontrollably penetrates public awareness and favors the internalization of values and norms desirable from the point of view of terrorist organizations.

In the conditions described, mass media become an easy-to-use and very effective tool for conducting, among others: psychological warfare by transmitting false or

contradictory information in order to create a sense of fear among recipients, including: by publishing drastic photos, videos and statements. It is worth emphasizing, however, that this tool is used by both sides of the fight against terrorism (Kołodziej, 2019).

At this point, it should be noted that the widespread ignorance and lack of willingness to verify the information received also produces an effect similar to a self-fulfilling prophecy. This phenomenon was first formally defined by Robert Merton in 1948 as an inaccurate definition of a situation causing new behaviors that turn initially false predictions into social reality (Trusz, 2018).

Thus, seemingly irrelevant information, but relating to socially important issues, such as migration, showing an individually specific case of violating the law by a migrant, unverified, devoid of context and repeatedly repeated with pejorative connotations in relation to nationality, race or religion, will result - in a relatively short time - in the development of negative attitudes towards every person who has the characteristics in question.

If the described mechanism includes false information and critical thinking is still disabled in society, the gate leading to the field of information warfare will remain wide open for terrorists.

Moreover, it is thanks to the media that terrorists' goals, including, above all, causing terror, e.g. by broadcasting the decapitation of a kidnapped tourist or journalist in the media, multiply the power of their impact on societies, which modern terrorism takes into account when selecting the methods and means of attack used.

How easy it is to distort the perception of reality using a false narrative is shown by the example of Orson Welles's radio broadcast from 1938, entitled "The War of the Worlds", about the Martian invasion of Earth. The radio show started at 8 p.m., but then most of the audience was listening to the competing NBC radio station, which broadcast a popular sketch until 8:12 p.m. When the audience switched to O. Welles' radio play, it had already lasted several minutes, and the listeners received information, among others: about a meteorite hitting the earth and Martians landing.

Many recipients considered this story to be true information, which caused panic among the inhabitants of New Jersey - the city where the broadcast took place. Regardless of the actual scale of the above-mentioned panic. the radio play confirmed that the right narrative can significantly distort reality and make people believe in fiction (Kołodziej, 2019).

As soon as such an opportunity arose, terrorist organizations began to use technological means as propaganda outlets. The public network, including the environment of social media and discussion forums, provides them with unlimited access to recipients, among whom they find new supporters, funders and even

recruits. A platform that is also a place for them to inspire people under the influence of fundamentalist ideology and encourage them to commit suicide attacks, as exemplified by detailed instructions on how to prepare a bomb or plan and carry out an attack placed on the Internet (Kołodziej, 2019).

A separate, but no less important issue is the increased curiosity about news, addiction to media adrenaline and indifference to suffering, habituation to cruelty and brutalization of media content. That is why the media and journalists are responsible for filtering published content. In a situation of tension and high level of emotions, responsible media must play a soothing role instead of heating up the message, even at the cost of losing some of the viewership profits. Such an approach that implements the assumptions of the common good in the long run, reinforced with appropriate educational messages, is likely to bring long-term benefits in the form of trust and the opinion of a reliable sender.

Nowadays, information is the most valuable commodity, and the 21st century is called the information era, hence the global society is preceded by the adjective information. Information is therefore treated as a strategic resource - it has its own value, its acquisition and use entails certain costs, and its lack is tantamount to lack of effectiveness in action (Liedel, Piasecka, and Aleksandrowicz, 2013), which is particularly important in the context of terrorist threats.

From a social point of view, the condition for the functioning of a lively and rational debate is the implementation of the following, equivalent freedoms: freedom of the media, freedom of expression and freedom of obtaining information. Although the current media environment provides citizens with opportunities to express their views on any issue, the pluralism in worldviews is overwhelming. In the thicket of information, searching for and gaining access to reliable information is significantly difficult, if not impossible, for the average person.

The previous filtering function of the media system allowed for selection by professional editors and control by political elites. These control tools, often criticized for limiting freedom of speech and expression, also supported the maintenance of the stability of democratic systems (Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich, Think Tank Parlament Europejski, source:
https://www.euro¬parl.europa.eu/thinktank/pl/document/IPOL_STU(2019)608864).

The excess of information, with the simultaneous lack of systemic filtration, makes it necessary for the recipient to develop some kind of information filter that will allow him to focus on the information that he considers important and that does not cause him a feeling of cognitive dissonance, i.e. is not inconsistent with his beliefs, values, views. This state of affairs, as T. Aleksandrowicz points out, means that, and I quote: “in the modern infosphere, effective information attacks can be carried out in a quite simple way, aimed at persuading specific social groups to behave as

expected by the attacker, e.g. to vote for a specific candidate in elections or protest against government policy" (Aleksandrowicz in: Boćkowski, Dąbrowska-Prokopowska, Goryń, and Goryń, 2022).

It should also be remembered that the loss of trust is a damage that will be very difficult for the compromised entity to make up for, and this state of affairs is desirable from the point of view of terrorists who are directly interested in undermining trust in the legal authorities or elites, which at the same time brings disastrous social consequences when counteracting and combating the consequences of terrorist attacks.

Social systems are not isolated systems, and the sources of threats may be located outside the system as well as inside (e.g., deviant behavior, anomie in Durkheim's sense). An internal threat will also be a situation when the institutions established to regulate processes themselves become a source of dysfunction.

Regardless of the sources and nature of threats, in a crisis situation, which includes, among others: terrorist attack, an adequate and proportionate system response to the threat is expected. In the event of an accidental disruption of the normal functioning of the local system, no long-term negative effects are expected in the system, which can be controlled with a small amount of effort and resources.

Of course, only if the information about such an event is factual, reliable and objective. If not, we may be dealing with panic caused by disinformation - which in the case of terrorist threats is a success for the perpetrators. According to Jan Poleszczuk, I quote:

Panic may be a direct experience resulting from observing the behavior of others (imitation), but its source may also be communication processes, i.e. disinformation and conspiracy theories. Panic is characterized by strong (escalatory) mobilization dynamics of the system and is an example of spontaneous correlated action - it arises quickly (arouses strong fear reactions), but also disappears quickly.

From the perspective of the institutions controlling and monitoring the system, panic causes surprise mainly due to the difficulty of quickly mobilizing resources, the inefficiency of standard decision-making procedures, the difficulty of verifying the reliability of information and the credibility of social (including political) communication.

Panic may turn into a "crisis" when it takes the form of a cascade and goes beyond the local horizon (spatial or sectoral). (…) A crisis is an example of a "domino effect" when a disruption in part of the system may spread to the entire system (Poleszczuk in: Boćkowski, Dąbrowska-Prokopowska, Goryń and Goryń, 2022).

If the social system is in a state of relative balance, then minor disturbances

(deviations and panic) do not produce significant destabilizing effects. In the case of crises, the greatest importance will be the strength of the system in terms of resistance to the cascading threat process that it is able to withstand.

The highest level of threat to the functioning of the system is posed by disasters and cataclysms. As Jan Poleszczuk emphasizes, every social system is fragile and may fall apart irreversibly when the limits of flexibility are exceeded.

The scale of systemic threats - from disruption to destruction - is not a simple continuum: deviation-panic-crisis-disaster-disaster, but a complex construct describing various aspects of the processes to which the system is exposed: from individual deviations from the norm, through correlated behavior, to triggering cascades of an unpredictable and irreversible nature at the macrosystemic level (Poleszczuk in: Boćkowski, Dąbrowska-Prokopowska, Goryń, and Goryń, 2022).

In a situation of uncertainty and fear, organizational chaos and disinformation, concepts and theories are born that keep our consciousness in a state of relative balance, thanks to which we internalize the belief that the decisions we make are appropriate and correct.

Being overstimulated with fear causes distrust and the imagination of a certain collusion in the event of an encounter with the unknown (Konopka in: Boćkowski, Dąbrowska-Prokopowska, Goryń, and Goryń, 2022).

If the source of such a situation are the actions of terrorists, then all anti-terrorist activities (including anti-terrorist prevention) will be doomed to failure. When little information is subject to substantive verification, government and security authorities must be aware that the described disinformation chaos can only be interrupted by education, especially in the area of critical thinking skills.

The ability to think critically is a driving force for change leading to building climate-conscious communities as a competence that allows one to become familiar with a specific problem, analyze it and take action to solve it in a rational, objective and conscious way (Krytyczne myślenie,
https://globalna.ceo.org.pl/tematy/klimat/krytyczne-myslenie/).

Social media can play an important and positive role in crisis management, e.g. in the case of warnings about a terrorist attack, acting as an additional communication channel, e.g., in connection with the possibility of transferring the crisis to virtual space; as a result of the fact that the source of the crisis may be, for example, ineffective communication with users or the fact that in social media there are actions of people directed against the social system, but only if such communication is properly prepared and planned (Chodyński, 2017).

As B. Hoffman points out, "terrorism is supposed to create power where it does not

exist or consolidate power where it is weak. By using the notoriety gained through violence, terrorists seek to gain influence and power that they do not have to effect political change at the local or international level" (Zwolan, 2015).

That is why now, in the face of terrorist threats, disinformation - as a phenomenon that determines the weakening of social structures, escalating antagonisms and strengthening the level of fear and anxiety in society while undermining trust in authorities and public institutions - has a strong negative impact on communities and cannot be illusions that this is a random phenomenon.

5. Conclusion

The multi-level research conducted in the field of information management in the face of extraordinary terrorist threats allowed for the fulfillment of the assumed research goal and the formulation of several recommendations and conclusions:

- Information management requires a specialized and organized information system;
- Information management can bring numerous benefits provided that the information meets certain conditions, namely that it is accurate, complete and up-to-date. Failure to meet these assumptions may lead to disinformation understood as misleading;
- Social disinformation has economic, political, social and health consequences;
- Disinformation processes intensify especially in times of extraordinary threats, including terrorist ones. Sustainable information management can counteract them;
- Sustainable information management involves the effective and responsible management of data and information in a way that supports the long-term goals of the organization, society and the environment;
- The aim of sustainable information management is to optimize processes related to information processing and to ensure that information is managed in an ethical, transparent and consistent manner with the principles of sustainable development;
- In order to effectively counteract disinformation, it is necessary to introduce systemic solutions, in particular by creating authority-based media. The media will verify the information provided on many levels, so that the recipients receive facts, not half-truths or fake news;
- Criminal liability should be extended to all persons who intentionally and consciously disseminate false information - regardless of the purpose for which they do it. The solutions present in the Polish legal system seem to be insufficient - taking into account the scale and type of threats;
- One of the foundations of developed civil societies is the ability to communicate and trust - due to the strong and long-term impact of disinformation, this foundation is crumbling. Disinformation is often a way of managing information in autocratic (despotic) systems. Therefore, it seems that education in the area of

critical thinking skills and verification of received information is necessary to ensure communities based on democratic principles.

References:

Bator, G., Knapik, M. 2020. Rola mediów społecznościowych jako instrumentu terroryzmu: analiza zamachu Brentona Tarranta. Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate, 10(1).

Boćkowski, D., Dąbrowska-Prokopowska, E., Goryń, P., Goryń, K. (red.) 2022. Dezinformacja – Inspiracja – Społeczeństwo. Social CyberSecurity, Białystok.

Boćkowski, D., Goryń, P., Goryń, K. (ed.) 2020. Bezpieczeństwo i jego percepcja w dyskursie społecznym i militarnym. Białystok.

Borowiecki, R., Czekaj, J. (ed.) 2012. Zarządzanie informacją i komunikacją w organizacjach gospodarczych i instytucjach sektora publicznego. Toruń.

Borowiecki, R., Kwieciński, M. (ed.) 2003. Informacja w zarządzaniu przedsiębiorstwem. Kraków.

Brennen, J.S., Simon, F., Howard, P.N., Kleis Nielsen, R. 2020. Types, Sources, and Claims of Covid-19 Misinformation. https://reutersinstitute.politics.ox.ac.uk/types-sources--and-claims-covid-19-misinformation.

Burczaniuk, P. 2024. Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku. Przegląd Bezpieczeństwa Wewnętrznego nr 30.

Brzeski, R. 2014. Wojna informacyjna – wojna nowej generacji. Komorów.

Chodyński, A. 2017. Zarządzanie mediami a bezpieczeństwo. Bezpieczeństwo. Teoria i Praktyka 2017, nr 4. http://hdl.handle.net/11315/18786

Czekaj, J. (ed.). 2012. Podstawy zarządzania informacją. Wydawnictwo Uniwersytetu Ekonomicznego. Kraków.

Dezinformacja i propaganda – wpływ na funkcjonowanie państwa prawa w UE i jej państwach członkowskich, Think Tank Parlament Europejski, źródło: https://www.europarl.europa.eu/thinktank/pl/document/IPOL_STU(2019)608864.

Drucker, P.F. 2000. Zarządzanie w XXI wieku. Warszawa.

French, M., Monahan, T. 2020. Dis-Ease Surveillance: How Might Surveillance Studies Address Covid-19? Surveillance & Society, No. 18(1). https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13985/9169.

Golicyn, A. 2007. Nowe kłamstwa w miejsce starych. Biblioteka Służby Kontrwywiadu Wojskowego. Warszawa.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Hatalska, N 2022. Spolaryzowane społeczeństwo łatwiej destabilizować. FORSAL.PL: 07 marca 2022, https://im¬pact.forsal.pl/8373933.Spolaryzowane-spoleczenstwo-latwiej-destabilizowac.html.

Hoc, S. 2021. Glosa do wyroku Sądu Apelacyjnego w Warszawie z 24.11.2017 r., II AKa 269/17. Prawo W Działaniu. Sprawy Karne Tom 45. Instytut Wymiaru Sprawiedliwości. Warszawa.

Hoc, S. 2023. Szpiegostwo w znowelizowanym Kodeksie karnym. Nowa Kodyfikacja Prawa Karnego Tom LXVII. Wrocław.

Iwiński, M., Rosenau, D. 2020. Odpowiedzialność karna za dezinformację jako forma działań wywiadowczych. https://kpsw.edu.pl/pobierz/wydawnictwo/Miscellanea/T_VIII_Z1/Maciej%20Iwi%C5%84ski,%20Dominik%20Rosenau.pdf.

Kacała, T. 2015. Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa. Przegląd Prawa Konstytucyjnego, no. 2.

Kaczmarek, J. 2001. Terroryzm i konflikty zbrojne a fundamentalizm islamski. Atla2. Wrocław.

Karolczak, K. 1995. Encyklopedia terroryzmu. Oficyna Wydawnicza SPAR. Warszawa.

Karolczak, K. 2022. Terroryzm XXI wieku – wybrane aspekty. Terroryzm – studia, analizy, prewencja, no. 1(1).

Kładoczny, P. 2013. Pismo z dnia 16 maja 2023 r. https://panoptykon.org/sites/default/files/druk_sejmowy_nr_3232_uwagi_hfpc_i_fundacji_panoptykon.pdf.

Kołodziej, A. 2019. Fake news jako broń przeciw terroryzmowi. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5c5a5669-275a-4719-9fc4-baf33f0214b0.

Konieczny, M. 2021. Wokół pojęcia dezinformacji w aspekcie prawno-kryminalistycznym. De Securitate et Defensione. O Bezpieczeństwie i Obronności, no 2(7). Siedlce.

Kozlova, O. 2013. Anomia jako choroba społeczna. Miscellanea Anthropologica et Sociologica 14/2.

Krytyczn e myślenie. https://globalna.ceo.org.pl/tematy/klimat/krytyczne-myslenie/.

Krztoń, W. 2017. Zarządzanie informacją w procesach decyzyjnych organizacji. Modern Management Review. MMR, vol. XXII, 24 (3).

Langefors, B. 1973. Theoretical analysis of information system. 4th ed. Studentliteratur, Lund, Sweden, Surbach Publishers inc., Philadelphia, PA.

Liedel, K., Piasecka, P., Aleksandrowicz, T.R. 2013. Analiza informacji. Teoria i praktyka. Warszawa.

Martin, C., Powell, P. 1992. Information systems. A management perspective. McGraw_Hill, London.

Oleński, J. 2000. Standardy informacyjne w gospodarce. Warszawa.

Pańkowska, M. 2001. Zarządzanie zasobami informatycznymi. Warszawa.

Pennycook, G., Mcphetres, J., Zhang Y., Lu, J.G., Rand, D.G. 2020. Fighting Covid-19 Misinformation On Social Media: Experimental Evidence For A Scalable Accuracy-Nudge Intervention. Psychological Science, 31(7), 770-780. doi 10.1177/0956797620939054.

Powstał Kodeks Dobrych Praktyk w zakresie dezinformacji, https://www.nask.pl/pl/aktualnosci/4992,Powstal-Kodeks-Dobrych-Praktyk-w-zakresie-dezinformacji.html?search=16089815518.

Shannon, C.E. 1948. A mathematical theory of communication. Bell System Technical Journal, vol. 27, no. 4.

Sprawozdanie Krajowej Rady Radiofonii i Telewizji z rocznego okresu działalności, Warszawa. 2003. https://orka.sejm.gov.pl/druki4ka.nsf/($vAllByUnid)/06C8FB6E717C586CC1256CFE00324BF0/$file/1476.pdf.

Stabryła, A. (ed.). 2018. Podstawy organizacji i zarządzania. Podejścia i koncepcje badawcze. Wydawnictwo Uniwersytetu Ekonomicznego. Kraków.

Stefanowicz, B. 2010. Informacja. Warszawa.

Sztuba, D., Mirek-Rogowska, A., Rączy, K. 2021. Zarządzanie informacją w mediach cyfrowych w dobie COVID-19-pomiędzy możliwym a niemożliwym-próba konstruktywnej analizy. Kultura-Media-Teologia, no 48.

Świgoń, M. 2012. Zarządzanie wiedzą i informacją. Podstawy teoretyczne. Badania w wymiarze indywidualnym. Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Olsztyn.

Taras, T. 1970. Przestępstwo szpiegostwa w świetle nowego Kodeksu karnego z 1969 r. Palestra 14/3(147).

Trusz, S. 2018. Mechanizm samospełniającego się proroctwa jako czynnik efektywności pracy ludzkiej, Ruch Pedagogiczny no 3. Wyższa Szkoła Pedagogiczna ZNP. Warszawa.

Tzu, S. 2003. Sztuka wojenna. Wydawnictwo vis-a-vis Etiuda. Kraków.

Uchwała Nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019" (Dz. Urz. 1218M.P. z 2014 r. poz. 1218).

Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. z 2023 r. poz. 2119).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2024 r. poz. 17).

Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2023 r. poz. 1834).

Uzasadnienie do Poselskiego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, druk nr 3232 z 17 kwietnia 2023 r., https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/%24File/3232.pdf.

Wachowicz, M.J. 2019. Ujęcie teoretyczne pojęcia dezinformacji, Wiedza Obronna no 1-2. Towarzystwo Wiedzy Obronnej, Warszawa. https://www.wprost.pl/swiat/11095837/to-jewgienij-prgozyn-stworzyl-rosyjska-fabryke-trolli-ingerowala-w-wybory-w-usa.html.

Wyrok Sądu Apelacyjnego w Warszawie z listopada 2017, sygn. akt II AKa 269/17.

Wyrok Sądu Okręgowego w Warszawie XII Wydział Karny z dnia 20.03.2017 r. sygn. akt XII K 91/16, https://orzeczenia.warszawa.so.gov.pl/details/$N/154505000003606_XII_K_000091_2016_Uz_2017-05-23_001.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 147-158). Emerald Publishing Limited.

Volkoff, V. 1991. Dezinformacja – oręż wojny, Wydawnictwo Delikon. Warszawa.

Zwolan, M. 2015. Współczesny terroryzm międzynarodowy – metody i sposoby zwalczania. Facta Simonidis, no 1(8).