Legal aspects of information operations in Poland

Правові аспекти інформаційних операцій у Польщі

Krzysztof Chochowski * [1] [A]

***Corresponding author**: [1] PhD student, e-mail: krzysztof.chochowski@onet.pl, ORCID: 0000-0003-3198-9619

[A] Prof. Stanisław Tarnowski State Vocational University in Tarnobrzeg, Poland

Кшиштоф Чоховскі * [1] [A]

***Corresponding author**: [1] PhD student, e-mail: krzysztof.chochowski@onet.pl, ORCID: 0000-0003-3198-9619

[A] Prof. Stanisław Tarnowski State Vocational University in Tarnobrzeg, Poland

Received: February 1, 2022 | Revised: February 20, 2022 | Accepted: February 28, 2022

DOI: 10.33445/sds.2021.12.1.1

Purpose: The purpose of this article is to outline the essence of information operations, their relation to the hybrid warfare and most of all indicate the legal aspects of information operations in Poland.

Design/Method/Approach: This article presents considerations about legal aspects of information operations in Poland.

Findings: The dynamic development of information systems and accompanying technologies, apart from undoubted positives, generates new threats. With their help, it is possible to create a false image of reality, leading to a morale collapse of the subject against whom information operations are directed.

Practical implications (if applicable): In the reality of a democratic state ruled by law, all actions, including those that are a manifestation of information warfare, must be taken only on the basis of the law and within its limits. In the case of Poland, there is no one universal legal regulation that would deal with this issue in a comprehensive manner. Existing standards are scattered across various laws and only indirectly deal with information operations. This is major neglect on the part of the decision-making elites of the Polish state. The events that have taken place over the past few months on the Polish-Belarusian border have highlighted the normative deficits in this regard.

Originality/Value: Information was, is and will be one of the most important resources of any organization, including the state. It is not a surprise that, on the one hand, it is systemically protected, and on the other hand, it is sometimes the target of various types of attacks. Nowadays, thanks to the ubiquitous ICT technologies and global communication, it is possible – with the help of information – to influence not only the individual but also entire social groups, and finally the society of a given country. These organized actions take the form of information operations as part of information warfare in the noosphere. Moreover, they can be considered a permanent element of hybrid wars.

Research limitations/Future research: It is the need for urgent action by the parliament in order to pass a law dedicated to the possibility of undertaking information warfare by designated entities and services, with particular emphasis on secret forces. In this way, Poland's resilience to threats resulting from the concept of hybrid war will be increased.

Paper type: Theoretical.

Key words: information operations, security, law, Enlargement, hybrid war.

Мета роботи: Метою статті є окреслення сутності інформаційних операцій, їх відношення до гібридної війни, а насамперед – правові аспекти інформаційних операцій у Польщі.

Дизайн/Метод/Підхід дослідження: У статті представлені міркування про правові аспекти інформаційних операцій у Польщі.

Результати дослідження: Динамічний розвиток інформаційних систем та супутніх технологій, окрім безсумнівних позитивів, породжує нові загрози. З їх допомогою можна створити хибний образ дійсності, що призведе до морального краху суб'єкта, проти якого спрямовані інформаційні операції.

Практична цінність дослідження: У реальності правової демократичної держави всі дії, у тому числі й такі, що є проявом інформаційної війни, мають здійснюватися лише на основі закону та в його межах. У випадку з Польщею не існує єдиного універсального правового регулювання, яке б регулювало це питання комплексно. Існуючі стандарти розпорошені по різних законах і лише опосередковано стосуються інформаційних операцій, це нехтування з боку еліти польської держави, яка приймає рішення. Події, що відбулися протягом кількох останніх місяців на польсько-білоруському кордоні, підкреслили нормативний дефіцит у цьому плані.

Оригінальність/Цінність дослідження: Інформація була, є і буде одним із найважливіших ресурсів будь-якої організації, в тому числі й держави. Не дивно, що, з одного боку, він системно захищений, а з іншого, іноді стає об'єктом різного роду атак. Нині, завдяки повсюдним IT-технологіям та глобальній комунікації, можна – за допомогою інформації – впливати не лише на окрему людину, а й на цілі соціальні групи, зрештою, на суспільство певної країни. Ці організовані дії мають форму інформаційних операцій у рамках інформаційної війни в ноосфері. Більше того, їх можна вважати постійним елементом гібридних воєн.

Обмеження дослідження/Майбутні дослідження: Це необхідність термінових дій парламенту для ухвалення закону, присвяченого можливості ведення інформаційної війни визначеними установами та службами, з особливим акцентом на секретні сили. Таким чином підвищиться стійкість Польщі до загроз, які випливають із концепції гібридної війни.

Тип статті: Теоретична.

Ключові слова: інформаційні операції, безпека, право, розширення, гібридна війна.

1. Introduction

Modern societies are based on information, so information is treated as one of their most valuable resources. It is not an exaggeration to say, that information can create reality and influence states, nations and individuals. Of course, everyone instinctively assume that information presented to them is true, but it is not always the case. Today distorted or false information can be a weapon as harmful as tank, rocket or a jet fighter. Modern conflicts more and more often take place in info-sphere as a competition for our hearts and minds, thus they do not take physical form. Because of

that, we can witness dynamic development of methods and means of information warfare used in information operations. In turn these operations are integral part of hybrid wars.

The purpose of this article is to outline the essence of information operations, their relation to hybrid wars and most of all, indicate legal aspects of information operations in Poland. Furthermore, I will try to determine if legal instruments available in Poland are sufficient and adequate to threats present in modern reality.

2. Results

I. The concept and essence of information operations

Information operations are complicated and complex projects aimed to impose your perception of reality on the other side of conflict. Their purpose is moral disintegration of a society, in particular their elite and decision makers, and convincing other subjects of international law of the rightness of your actions. Of course, they also include the means of protection of your own information, info-sphere and information related infrastructure. Information operations can be offensive or defensive, but they always aim to gain information advantage over the enemy (Operational Law Handbook, s. 412).

According to NATO Doctrine JP 3-13 information operation is a set of activates that aim to influence information and information systems of your adversary, while at the same time defend your own information and information systems. Information operations are used in every phase of military operations including physical conflict, and on every level of military operations. Information operations are integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (Joint Doctrine for Information Operations).

Information operations include activities such as confusing adversaries, PSYOPS (psychological operations), electronic warfare and physical destruction of information infrastructure (Olechowski, M.).

Information operations are defined in a draft of RP information security doctrine from 25 July 2015. According to it, information operations are actions taken to influence information and/or information systems in order to shape and take over decision making processes of adversaries (automated or involving the human factor) while defending your own decision-making processes. From a military perspective information operation are actions taken to influence morale, cognition and military capabilities of adversaries, potential adversaries or other sides of a conflict that support the objectives of the current mission. Information operations include offensive and defensive actions. Offensive actions include psychological operations, confusing actions, destruction, electronic warfare, information attacks and activities that involve social communications. Defensive actions include Information security, protection, anti-propaganda, counter-espionage, electronic warfare, special information actions (Draft Information Security). As can be seen, the definition of information operations is basically the same as the definition of these operations from the NATO doctrine JP 13-3. Which, due to Poland's membership in the North Atlantic Alliance, is fully understandable.

The goal of information operations, as R. Szpyra emphasizes, is to gain an advantage in command (Szpyra, R.). A similar view is presented by A. Lelonek, who claims that the main objective of such operations is to influence the processes based on communication and information transfer, regardless of whether they are automated or involving a human factor. The scope of information operations includes, among others: intelligence, support for communication systems, information systems and coordination on various levels of activity, resulting from a coherent action strategy. To

be successful, information operations must be integrated with air, land, sea, space and special operations, and be consistent with national and military objectives (Lelonek A.).

Information operations, as emphasized by Z. Modrzejewski, must be based on effective reconnaissance and intelligence support. Good, reliable, accurate and timely information is a factor that can give an advantage over your adversary (Modrzejewski, Z., 2013, s. 138, 139). This advantage should be understood as the ability to gather, store, process and distribute information, maintain its uninterrupted flow and make full use of it, while having the ability to prevent the adversary from carrying out similar information actions (Aleksandrowicz, T. R., 2016, s. 107). Information advantage over your adversary is a factor that determines the success of the information operation (Sienkiewicz, P., 2004, s. 376). The conflicting parties gain the information advantage by selecting adequate tools, depending on the type of activities and the conditions (Kaźmierczak, D., 2017, s. 113).

Modern information techniques allow, as stated by M. Wrzosek, manipulation of image and sound, and thus make it possible to publish untrue, processed, and manipulated information in order to achieve a specific goal of information warfare. The information broadcasters can intentionally present material that comes from a different place, other time and present a situation in a different light. Due to limitations in the method of information transmsion, the average recipient is not able to recognize the manipulation (Wrzosek, M., 2018, s. 173).

The author develops the above thesis by adding that "The main level of the confrontation is "invisible war" carried out in the sphere of propaganda, disinformation and counteracting information. In this context, information operations target the system, not individuals, and are therefore sometimes invisible to the public. Meanwhile, by using the methods of direct influence (eg mass media, social networks), the opinions of specific social groups are formed" Wrzosek, M., 2018, s. 308).

Based on the above theses, it can be concluded that information operations are an important component of information warfare, or more broadly, information war. The latter, in turn, should be seen as an element of the so-called hybrid war.

II. Information warfare and hybrid war

Information warfare, contrary to some opinions voiced in media, is not a new concept A. Żebrowski aptly points out that "The history of information warfare is as long as the human history. However, it was not documented. Furthermore – it has never even been called information warfare. However, this does not mean that the functions of obtaining information, information disruption and information defence associated with it today appeared only at the end of the 20th century. They have always existed. (...) In the initial period, the information warfare took place only in the personal information space, where the basic source of information was other man, as well as the phenomena occurring in his immediate and further surroundings. At that time, only direct observation and participation in the conversations, or written communications gave access to knowledge about the opponent and enabled decisions and actions to be taken. The ongoing civilization changes, accompanied by the intensive development of science and technology, mean that the information warfare also takes place in the technical information space" (Żebrowski, A., 2017, s. 91). Therefore, the information warfare has not only a personal but also a technical dimension, which, due to technological progress, is becoming more and more important. The special agencies of a state play a significant role in these struggles, which in the domestic realty is related to the activities of both civil and military intelligence and counterintelligence (Wiszniewski, L. 2020, s. 66). The special agencies are actually predestined to lead and direct the information warfare.

Referring to the issue of information warfare (information war) as one of the basic elements of hybrid war, it is best to define what information warfare is and then relate that definition to the issue of hybrid war. The concept of information warfare can be defined as a complex of actions that

include supportive actions, counteraction and information defence, carried out according with one concept and plan, in order to fight and maintain control over the enemy in the field of information during the preparation for military operations and conducting combat operations (J. L., 1999, s. 80). Information warfare is defined somewhat differently by P. Sienkiewicz, who recognizes that "Information warfare (infowar) is all offensive and defensive activities necessary to gain an information advantage over the opponent and to achieve the intended military (political) goals. The essence of the fight understood in this way is:

1) Destruction (or degradation of value) of the opponent's information resources and information systems.

2) Ensuring the security of your own information resources and the information systems" (Sienkiewicz, P., 2004, s. 375).

NATO standards define information warfare as information operations carried out during a crisis or conflict in order to achieve or promote specific goals in relation to a specific opponent or opponents. This warfare may include actions to deny access, use or destroy the enemy's information and information systems, and to protect one's own information resources and systems, including information systems. Information warfare is any attack against the information system, regardless of means (Grimes, D. I., Rawcliffe, J., Smith, J., 2006). On the other hand, in Russia, as J.L. notes, "Russian specialists perceive information warfare as a complex of undertakings – including support, counteraction and information defence – carried out according to a uniform concept and plan in order to fight and maintain control over the enemy in the field of information while preparing a military operation and conducting combat operations" (J. L., 1999, s. 80). Regardless of whether we consider the issue of information warfare in the context of the NATO or the Russian doctrine, its aim is always to gain an information advantage over the enemy. This issue is presented in a similar way by M. Wrzosek, who claims that "Information warfare becomes the main area of conflict, because "gaining" an advantage (dominating) in the area of information is the basic necessity for effective and precise activities" (Wrzosek, M., 2018, s. 188).

Information warfare is all offensive and defensive activities necessary to obtain an information advantage over the enemy and to achieve the intended military (political) goals. In this fight, diplomacy, propaganda, psychological campaigns, influencing political and cultural processes, disinformation, media manipulation, infiltration of computer networks are used as tools (Aleksandrowicz, T. R., 2014, s. 30-32; Olechowski, M., 2018). Information warfare, as pointed out by D. Kaźmierczak, may be: an autonomous phenomenon, a component supporting military operations, the main component supported by military operations. He then states that the elements of information warfare are: physical destruction, security operations, psychological operations, sabotage, electronic warfare (Kaźmierczak, D., 2017, s. 112).

The doctrine indicates that information warfare is not the exclusive domain of the armed forces, it is also conducted by non-military entities, both in times of peace and in times of crisis (Żebrowski, A., 2017, s. 95). Therefore, it should be noted that both state and non-state entities have a rich set of tools at their disposal to be used in information warfare. These are, for example: financing scholarship programs, grants, research programs for students, scientists, experts, journalists or artists and using their emotional or personal attachment to a given environment, structure or simply friends in the country and abroad related to the donor; supporting student, expert and industry exchanges or taking patronage over similar events; selecting and assisting in the career of promising or not very promising journalists, politicians or experts, and through them influencing the information space, public opinion and decision-making process in a given country in the future; corruption of politicians, officials, military structures, journalists, employees of the financial sector, experts, social activists, activists or people of culture and science, both in the form of direct financial gratification and indirect (assistance in a career, offering positions in controlled private sector companies or international structures); establishing, taking over or destroying

analytical centres, think-tanks and similar research and development initiatives that could pose a threat to a given narrative in domestic or foreign policy; establishing, taking over or destroying organizations, movements and social initiatives, political parties or organizations of an economic nature (e.g. cooperatives) at the local, regional and national level; disseminating false or manipulated information in whole or in part, aimed at influencing emotions, social moods, patriotic feelings, issues that are painful from the historical or political point of view, through own and friendly mass media; releasing false or manipulated information through official and unofficial, public and covert channels; disseminating secret information to the media, which would not be obtained in any legal way, and the publication of which may have an impact on the public mood or public opinion; acquiring, using and disclosing agents of foreign services or the so-called "Agents of influence" who were recruited using the above-mentioned methods, and whose deployment at various levels of state administration, in the media or private companies, especially in the financial sector, in the enemy country is most often much more effective, cheaper and safer than large-scale political media campaigns (Lelonek A.).

Today the information warfare is more and more important. It has, as correctly stated by M. Wrzosek, an impact on the processes shaping both international security and security of individual countries and citizens. In this context, however, it should be clear that non-state entities are most significant participants in the information warfare, whose activities often violate the security of the international community, e.g. terrorism, organized crime, industrial concerns. In addition, it covers a wide spectrum of impact on the internal and external environment of virtually all countries, as well as non-state entities. Thus, information warfare is present in human life, social groups, nations, states, international organizations and other non-state entities (e.g. criminal organizations, terrorist organizations, companies offering military services) (Wrzosek, M., 2018, s. 151, 152).

Gaining an information advantage appears to be a necessary condition for information security, a process and condition for the freedom of access, collection, processing and flow of high-quality information (achieved through substantive selection) is ensured, combined with rational, legal and customary separation of categories of informations to be protected or rationing of information, due to the safety of entities they concern (Felhler, W., 2016).

Information warfare is unanimously considered to be one of the manifestations of the so-called hybrid war. Concept of hybrid war appeared in literature for the first time in 2002 in the work of WJ Nemeth titled Future war and Chechnya: A case for hybrid warfare (Nemeth, W. J., 2002), although it should be noted that in the work of Sun Tzu Art of War one can find substitutes of what nowadays it is called a hybrid war. He stated that "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill". Here the essence of information warfare as a component of hybrid war is fully revealed.

The etymological origin of the terms, "hybridity" comes from the Latin word hybrid. An individual that is a result of cross-breed between two genetically different individuals belonging to different species, varieties or races. Hybridity is a property resulting from the mixing of features, elements belonging to different, often structurally different and genetically distant, opposing objects, organisms or states. Hybridization means the merging of essentially different features around one, separate being, while maintaining specific species properties that determine the "superiority" of a new, hybrid organism in terms of, for example, resistance to disease, endurance or greater adaptability.

Work on the development of the concept of hybrid war and was undertaken simultaneously within NATO and the Russian Federation. The works of F.G. Hoffman (Hoffman, F. G., 2007) and W. Gierasimow (Gerasimov, V., 2013) were fundamental for that concept. Also, in Poland, the issue of hybrid war was raised by representatives of the doctrine (Antczak – Barzan, A., 2016, s. 259-282; Skoneczny, Ł., 2015, s. 39 – 50; Lewandowska, A., 2016, s. 187-199; Piotrowski, M. A., 2015, s. 7-38).

Hybridization in relation to armed conflicts is the coexistence of elements of "old" and "new" wars, classic armed conflicts and "postmodern" wars, clashes of national armies and asymmetric conflicts, super-military technologies and primitive weapons, struggles for territories and resources, and disputes over identity and values, confrontation of parochialism and cosmopolitanism.

Therefore, we can justify the statement of K. Surdyk that "The most important principle of the hybrid war strategy is to ensure the maximum concentration of resources in sensitive places in order to effectively destabilize the political and military leadership of the enemy state, its economic and social structures, and the cultural sphere, and then dismantle the state as a sovereign entity of international law and hand them over to external control" (Surdyk, K., 2018). For this purpose, many different instruments are used, but as emphasized by E. Sadowska, information is an excellent weapon in waging a hybrid war (Sadowska, E., 2017). Due to information warfare, it is possible to achieve the goals of hybrid war, and therefore it should be considered one of its important determinants. Therefore, it is necessary to win the information fight or, more broadly, a hybrid war, not only to disintegrate the enemy's information and information systems, but also to ensure the information security of one's own resources.

Information security is one of the most important aspects of public security. It is the state's responsibility to ensure it, although private institutions may be used for this purpose. However, the state is always, the entity that is originally entitled to a monopoly on the use of legal coercion. It may, even if it entrusts a private entity with some public task in the discussed sphere, withdraw its decision in the field of public security, including information security. This means that the currently fashionable process of privatization of public tasks is – in the context of ensuring the said security – completely reversible, if the state deems it justified. The essence of the existence of public administration is service for the common good (Chochowska, A., 2019).

III. Legal bases of information operations in Poland

There is still an issue of legal basis for information operations in Poland to be clarified as part of this article. It seems that there are large deficits in this matter, and the existing legal instruments do not meet the requirements of modern times. The special forces of a given country are naturally predestined to conduct information warfare. It is no different in the case of Poland, where the Internal Security Agency and the Foreign Intelligence Agency play a leading role, as well as military special forces in the form of the Military Counter-intelligence Service and the Military Intelligence Service. The usefulness of the last of the Polish secret services, namely the CBA in the field of information operations being a manifestation of information warfare and hybrid war, is very limited due to the purpose of its operation.

During the analysis of Polish legislation in the context of information operations, it must be noted that there is no uniform normative act that comprehensively regulates this issue. The existing law that regulates information operations is scattered between a number of different laws and only indirectly relate to the issue at hand. We are talking here, for example, about the Act of 5 August 2010 on the protection of classified information, which in art. 1 clause 1 defines classified information as information the unauthorized disclosure of which would cause or could cause damage to the Republic of Poland or would be unfavourable from the point of view of its interests; the Act of 5 July 2018 on the National Cybersecurity System, which main drawback in the context of information warfare is that it only covers the cyber-sphere, and not the entire information sphere; the Act of June 10, 2016 on anti-terrorist activities, which under Art. 60 sec. 1 imposes on recipients of pre-paid services the obligation to register them, significantly eliminating their anonymity, and thus often also impunity; as well as service pragmatists for Polish secret forces, i.e. the Act of May 24, 2002 on the Internal Security Agency and the Foreign Intelligence Agency and the Act of June 9, 2006 on the Military Counter-intelligence Service and the Military Intelligence Service.

Both intelligence and counter-intelligence agencies in Poland can conduct information operations, and it does not matter whether they are civil or military. Of course, these actions are often negatively perceived by the ruling elites in democratic countries as actions unworthy and contrary to ethics, nevertheless, from the perspective of the state's interests, in some situations they are even necessary.

When analysing the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, it should be stated that the tasks of the Internal Security Agency, pursuant to Art. 5 sec. 1 and 3 are: to identify, prevent and combat threats to the internal security of the state and its constitutional order, in particular the sovereignty and international position, independence and inviolability of its territory, as well as the defence of the state, as well as obtaining, analysing, processing and providing competent authorities with information that may be of significant importance for the protection of the internal security of the state and its constitutional order (Chochowski, K., 2021). As can be seen, this quite generally outlines the scope of tasks assigned to the Internal Security Agency and includes the possibilities of undertaking and implementing information operations, although no provisions of the act expressis verbis indicate this.

However, in relation to the second of the agencies indicated in the referred to act, the Foreign Intelligence Agency, its tasks are described in Art. 6 sec. 1, and include: obtaining, analysing, processing and forwarding to the competent authorities information that may be of significant importance for the security and international position of the Republic of Poland as well as its economic and defence potential; identifying and counteracting to the external threats to security, defence, independence and inviolability of the territory of the Republic of Poland; protection of foreign representative offices of the Republic of Poland and their employees against the actions of foreign secret services and other actions that may be detrimental to the interests of the Republic of Poland; ensuring cryptographic protection of communication with Polish diplomatic and consular posts and courier services; recognizing international terrorism, extremism and international organized crime groups; identification of international trade in weapons, ammunition and explosives, narcotic drugs and psychotropic substances as well as goods, technologies and services of strategic importance to the state's security, as well as recognition of international trade in weapons of mass destruction and threats related to the proliferation of these weapons and their means of delivery; identifying and analysing threats in the areas of international tensions, conflicts and crises affecting the security of the state, and taking actions to eliminate these threats; identifying, counteracting and preventing terrorist events directed against citizens or property of the Republic of Poland outside the state, excluding events of a terrorist nature directed against the personnel or property of the Polish Armed Forces; conducting electronic espionage; undertaking other activities specified in separate acts and international agreements.

The implementation of the above tasks by the Foreign Intelligence Agency may take place through information operations or, more broadly, information warfare. However, also in this case, Polish legislation does not contain provisions that would directly regulate the issue in question, leaving this special service a large scope of freedom in the taken actions.

The Act of June 9, 2006 on the Military Counter-intelligence Service and the Military Intelligence Service defines the legal status of military special forces in Poland, also indicating their tasks. Regarding the MCS, its basic tasks were defined by the legislator in Art. 5 sec. 1 and 2, and they include: recognition, prevention and detection of crimes referred to in art. 5 sec. 1 point 1 of the act; cooperation with the Military Police and other agencies authorized to prosecute the crimes listed in art. 5 sec. 1 point 1 of the act; identification, prevention and detection of terrorist events and crimes affecting the security of the defence potential of the state, the Polish Armed Forces and organizational units of the Ministry of National Defence; implementing, within its jurisdiction, the tasks specified in the provisions of the Act of 5 August 2010 on the protection of classified information (Journal of Laws of 2016, items 1167 and 1948 and of 2017, item 935); obtaining,

collecting, analysing, processing and transferring to the competent authorities information that may be of importance for the state's defence, security or combat capability of the Polish Armed Forces or other organizational units of the Ministry of National Defence, within the scope specified in art. 5 sec. 1 point 1 of the Act, and taking actions to eliminate the identified threats; conducting radio-electronic counter-intelligence and undertakings in the field of cryptographic protection and cryptanalysis; participating in planning and carrying out control over the implementation of international agreements on disarmament; protection of the security of military units, other organizational units of the Ministry of National Defence and soldiers performing official tasks outside the state; protection of the safety of scientific research and development works commissioned by the Armed Forces of the Republic of Poland and other organizational units of the Ministry of National Defence as well as the production and trade in goods, technologies and services for military purposes ordered by the Armed Forces of the Republic of Poland and other organizational units of the Ministry of National Defence, to the extent specified in art. 5 sec. 1 point 1 of the act; taking actions provided for by the MCS, in other acts, as well as international agreements by which the Republic of Poland is bound (Chochowski, K., 2019, s. 231-240).

The catalogue of the MCS tasks was extended pursuant to the provision of Art. 5 sec. 1-point 2a of the Act, adding to them the identification, prevention and detection of terrorist events and crimes affecting the security of the defence potential of the state, the Polish Armed Forces and organizational units of the Ministry of National Defence. Noticing the problem of terrorist activity as well as the possibility of hostile actions by other countries in a legally undefined state, no longer peace but not yet war, is a specific response of the legislator to the changing nature of threats. This problem is particularly visible in the context of the so-called hybrid war, and its importance is proved, for example, by Russia's activity towards Ukraine, the aim of which was the annexation of Crimea. An essential change of the discussed legal regulation is also the introduction of Art. 29a, on the basis of which, the Head of the Military Counter-intelligence Service can allow to use devices that prevent telecommunications. This blockade is applied in a specific area for the time necessary to perform activities of MCS, taking into account the need to minimize the effects of the inability to use telecommunications services. The Head of the SKW shall immediately inform the President of the Office of Electronic Communications about the use of devices that prevent telecommunications. Thus, we see a specific response to the progressive development of ICT, social media and the possibility of using them in anti-state activities (Chochowski, K., 2021, s. 171, 172).

In turn, in relation to the Military Intelligence Service, the catalogue of tasks of this service is indicated in Art. 6 sec. 1 of the Act, according to which the tasks of the CSG include: obtaining, collecting, analysing, processing and transferring to the competent authorities information that may be of significant importance to the security of the defence potential of the Republic of Poland, the security and combat capability of the Polish Armed Forces, the conditions for the implementation of tasks abroad by the Polish Armed Forces; identifying and counteracting to the external military threats to the defence of the Republic of Poland, threats imposed by international terrorism; identification of international trade in weapons, ammunition and explosives as well as goods, technologies and services of strategic importance for state's security, as well as identification of international trade in weapons of mass destruction and threats related to the proliferation of these weapons and their means of delivery; identifying, counteracting and preventing terrorist events directed against the personnel and property of the Polish Armed Forces abroad and combating the effects of such events; identifying and analysing threats in the areas of international tensions, conflicts and crises, affecting the state's defence and the combat capability of the Polish Armed Forces, as well as taking actions to eliminate these threats; conducting electronic intelligence for the Polish Armed Forces and undertakings in the field of cryptanalysis and cryptography; cooperation in organizing Polish military representations abroad; participating in planning and carrying out control over the implementation of international agreements on disarmament;

undertaking other activities provided for by the CSG in separate acts, as well as international agreements by which the Republic of Poland is bound. In addition, the tasks of the CSG include identifying, counteracting and preventing terrorist events directed against the personnel and property of the Polish Armed Forces outside the state and combating the effects of such events, as stated in Art. 6 sec. 1-point 3a (Chochowski, K., 2021, s. 178, 179).

Summarizing the considerations on the legal basis of information operations in Poland, some gaps and shortcomings can be noticed. The existing legal regulations do not seem to notice this issue, which is so important from the perspective of information warfare and hybrid warfare. Indirectly, these operations are legitimized by the provisions contained in the official pragmatics of Polish secret forces, as well as the Act of August 5, 2010 on the protection of classified information, or the Act of July 5, 2018 on the national cybersecurity system. However, there is no universal, comprehensive normative act sanctioning these operations. Thus, there is an urgent need to undertake legislative work in this area, as evidenced by the action conducted by A. Lukashenka, who, by using foreigners, aims to destabilize the internal situation in Poland, leading against it, inter alia, information fight.

3. Conclusions

Information was, is and will be one of the most important resources of any organization, including the state. It is not a surprise that, on the one hand, it is systemically protected, and on the other hand, it is sometimes the target of various types of attacks. Nowadays, thanks to the ubiquitous ICT technologies and global communication, it is possible – with the help of information – to influence not only the individual but also entire social groups, and finally the society of a given country. These organized actions take the form of information operations as part of information warfare in the noosphere. Moreover, they can be considered a permanent element of hybrid wars.

The dynamic development of information systems and accompanying technologies, apart from undoubted positives, generates new threats. With their help, it is possible to create a false image of reality, leading to a morale collapse of the subject against whom information operations are directed. This in turn requires an appropriate response on the part of the state, as an organization which bears the burden of responsibility for the security of entities under its authority. In the reality of a democratic state ruled by law, all actions, including those that are a manifestation of information warfare, must be taken only on the basis of the law and within its limits (Piasecki, B., 2021; Minkina, M., Gałek, B., 2015; Słoń, M., Wójcik, S., 2020; Budzisz, M., 2021).

In the case of Poland, there is no one universal legal regulation that would deal with this issue in a comprehensive manner. Existing standards are scattered across various laws and only indirectly deal with information operations. This is a major neglect on the part of the decision-making elites of the Polish state. The events that have taken place over the past few months on the Polish-Belarusian border have highlighted the normative deficits in this regard. Hence the need for urgent action by the parliament in order to pass a law dedicated to the possibility of undertaking information warfare by designated entities and services, with particular emphasis on secret forces. In this way, Poland's resilience to threats resulting from the concept of hybrid war will be increased.

4. Funding

This study received no specific financial support.

5. Competing interests

The authors declare that they have no competing interests.

References

Aleksandrowicz, T. R., Liedel, K. *Społeczeństwo informacyjne-sieć-cyberprzestrzeń. Nowe zagrożenia,* [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* [Information society – network – cyberspace. New threats, [in:] Network-centric security. War, peace and terrorism in the age of information], pod red. K. Liedel, P. Piasecka, T. Aleksandrowicz, Warszawa 2014, s. 30-32. (in Polish)

Aleksandrowicz, T. R. *Podstawy walki informacyjnej* [Basics of information warfare], Warszawa 2016, s. 107. (in Polish).

Antczak – Barzan, A., Śliwa, Z., Zaniewski, R. *Wojna XXI wieku. Początki wojny "trzeciej fali"* [The war of the twenty-first century. The Beginnings of the "Third Wave" War], Warszawa 2016. (in Polish).

Budzisz M., *Wszystko jest wojną* [Everything is war], Warszawa 2021. (in Polish).

Chochowska A., Public administration as the service for the common good, *Zeszyty Naukowe Uniwerystetu Rzeszowskiego. Seria Prawnicza. Prawo,* №27, (2019).

Chochowski K., *Rola i zadania polskich służb specjalnych w zapewnieniu bezpieczeństwa jednostki,* [w:] *Jednostka – Społeczeństwo – Państwo. Księga Pamiątkowa ku czci Profesora Jerzego Rebety* [The role and tasks of Polish secret services in ensuring the security of an individual, [in:] Unit – Society – State. Memorial Book in honor of Professor Jerzy Rebeta], pod red. A. Poraza, W. Gizicki, Lublin 2019. (in Polish)

Chochowski, K. *Służby specjalne w Polsce* [Secret services in Poland], Sofia, 2021. (in Polish).

Felhler W., *O pojęciu bezpieczeństwa informacyjnego,* [w:] *Bezpieczeństwo informacyjne w XXI w.* [On the concept of information security, [in:] Information security in the 21st century], Siedlce, 2016.

Gerasimov, V. *Tsennost' nauki v predvidenii* [The value of science in foresight], *Military Industrial Courier*, 2013. (in Russian)

Grimes D. I., Rawcliffe J., Smith J., Operational Law Handbook, Charlottesville, Virginia 2006.

Hoffman, F. G. Conflict in the 21st century: Rise of the Hybrid Wars, Arlington, 2007.

Joint Doctrine for Information Operations. JP 3-13 Joint Doctrine for Information Operations (c4i.org). Retrieved from : https://www.c4i.org/jp3_13.pdf., date of access09.12.2021.

Kaźmierczak, D. (2017). *Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje* [Information warfare in contemporary conflicts and its social consequences], *Studia de Securitate et Educatione Civili*, № 7. (in Polish)

L. J. (1999). *Rosyjska koncepcja walki informacyjnej* [The Russian concept of information warfare], *Wojskowy Przegląd Zagraniczny*, № 1. 1999.

Lelonek A. *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie* [Information warfare, information and psychological operations: concepts, methods and applications], 05PL_Lelonek.pdf (capd.pl) data dostępu 09.12.2021.

Operational_Law_Handbook (Microsoft Word – OpLaw HB 06 Master.doc (ndu.edu)), s. 412, Retrieved from : https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1F2_Operational_Law_Handbook.pdf., date of access 09.12.2021.

Minkina, M., Gałek, B. *Kłamstwo i podstęp we współczesnym świecie* [A lie and a trick in the modern world], Warszawa 2015. (in Polish).

Modrzejewski, Z. (2016). *Rozpoznawcze wsparcie operacji informacyjnych* [Reconnaissance support for information operations], *Zeszyty Naukowe AON*, 2013, № 1, (90). (in Polish).

Nemeth, W. J. Future war and Chechnya: A case for hybrid warfare, Monterey 2002.

Olechowski M., *"Wojna psychologiczna" – próba zdefiniowana pojęcia* ["Psychological war" – an attempt to define the concept], *Wiedza obronna,* 2018, № 1-2. (in Polish).

Piasecki, B. *Kontrwywiad. Atak i obrona* [Counterespionage. Attack and defense], Łomianki 2021. (in Polish).

Piotrowski, M. A. (2015). *Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych, Sprawy międzynarodowe*, № 2. (in Polish).

Draft Information Security Doctrine of the Republic of Poland.pdf (bbn.gov.pl) p. 4, Retrieved from : chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.bbn.gov.pl%2Fftp%2Fdok%2F01%2FProjekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf&clen=335274&chunk=true. Access date 09.12.2021.

Sadowska, E. (2017). *Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie* [Asymmetric threats – definition, social awareness and role in the modern world]*, Rocznik Bezpieczeństwa Międzynarodowego*, №2, 2017, s. 21. (in Polish).

Sienkiewicz P., *Wizje i modele wojny informacyjnej,* [w:] *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* [Visions and models of information warfare, [in:] Information society. Vision or reality?], *Tom 1,* pod red. L.H. Haber, Kraków 2004. (in Polish).

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia,* "Przegląd Bezpieczeństwa Publicznego" [Hybrid War – Challenge of the Future? Selected issues, "Review of Public Safety"], *Wydanie specjalne*, 2015. (in Polish).

Słoń M., Wójcik S., *Tajemnice wywiadu wewnętrznego* [Secrets of internal intelligence]*,* Warszawa 2020. (in Polish).

Surdyk K., *Rola służb wywiadowczych w wojnie hybrydowej,* "ANTE PORTAS Studia nad Bezpieczeństwem Konflikty asymetryczne i wojny hybrydowe w XXI wieku" [The role of intelligence services in hybrid warfare, "ANTE PORTAS Security Studies Asymmetric Conflicts and Hybrid Wars in the 21st Century"], № 2 (11), 2018.

Szpyra, R. *Militarne operacje informacyjne* [Military information operations]*,* Warszawa 2003. (in Polish).

Wiszniewski, L. (2020). *Rola i znaczenie analizy informacji wywiadowczej w zapewnieniu bezpieczeństwa państwa* [The role and importance of intelligence analysis in ensuring state security]*, Przegląd Bezpieczeństwa Wewnętrznego*, № 22 (12).

Wrzosek, M. *Wojny przyszłości. Doktryna, technika, operacje militarne* [The wars of the future. Doctrine, technology, military operations]*,* Warszawa 2018, s. 173. (in Polish).

Żebrowski A., *Determinanty walki informacyjnej,* [w:] *Walka informacyjna: uwarunkowania, incydenty, wyzwania* [Determinants of information warfare, [in:] Information warfare: conditions, incidents, challenges]*,* pod red. H. Batorowskiej, Kraków 2017. (in Polish).

The Act of August 5, 2010 on the protection of classified information.