Piotr Milik*

Lawfare – Hostile Actions Against the Legal System of the State Through Activities in Cyberspace

Abstract

The article analyses important and current issues concerning the use of modern information technologies in hostile actions against the state in the international environment. First, the concept of lawfare was defined as a method of conducting information warfare. Then, the focus was on the potential manifestations of lawfare in cyberspace, indicating possible gaps in the state's information security system and sensitive areas susceptible to methods of hostile shaping of the state's legal system.

Key words: lawfare, social engineering, information warfare, cyberspace

* Assoc. Prof. Piotr Milik, PhD, War Studies University in Warsaw, e-mail: p.milik@pracownik.akladem ia.mil.pl, ORCID: 0000-0002-1204-4882.

Lawfare as a method of conducting information warfare

Lawfare can be defined as one of the covert social engineering methods aimed at fulfilling the objective of shaping an opponent's legal order (system) in a hostile way. Thus, lawfare is becoming one of the methods for conducting information warfare in contemporary hybrid (asymmetrical) conflicts.

The term „lawfare" is a combination of words based on „warfare", which means acts of war, where the word „war" was replaced by the word „law". It can be said that lawfare means acts of war conducted using law, legal procedures and remedies. The term is not explicit in its meaning and may be interpreted in various ways, depending on the shift in the focus on specified aspects of using law as a weapon.

An attempt to define lawfare based on the rules of semiotics was taken by Susan W. Tiefenbrun, who wrote in her article entitled „Semiotic Definition of Lawfare" that „[...] lawfare is a weapon designed to destroy the enemy by using, misusing, and abusing the legal system and the media to raise a public outcry against that enemy. The term »lawfare« is also a clever play on words, a pun, and a neologism that needs to be deconstructed in order to explain the linguistic and political power of the term. Semiotic theory can help unpack this play on words, which creates an interesting and shocking equivalence between law and war. Semiotics is the science of signs and involves the exchange between two or more speakers through coded language and convention. Semiotics is the scientific study of communication, meaning, and interpretation. [...] The linkage of law to war is most clearly manifested in the expression of a »just war« and the elaboration of the »laws of war«. Both law and war enjoy power. It is precisely this shared power that constitutes the basis of using lawfare as a weapon of modern asymmetrical warfare. [...] The abuse of the legal system, human rights laws, and humanitarian laws by lawfare undermines the overarching goal of world peace by eroding the integrity of the legal system, and weakening the global establishment and enforcement of the rule of law. The manipulation of Western judicial systems, and the misuse of European and Canadian hate speech laws and libel law procedures, can destroy the very principles of free speech that democracies hold most precious. Lawfare has limited public discussion of radical Islam and created unfair negative publicity against freedom-loving countries. The weapon used is the rule of law itself, which was created not to quiet the speech of the innocent but rather to subdue

dictators and tyrants. Ironically, it is this very same rule of law that is being abused to empower tyrants and to thwart free speech"[1].

An interesting paradox, dating back to antiquity and demonstrating the use of law in an insidious fight against one's adversary, was cited by José Luis Martí, in his article entitled „Lawfare and Democracy. Law as a weapon of war": „One fine day, the Greek sophist Protagoras met a potential student, Euatle, who wanted to take rhetoric lessons with him but had no money to pay. Protagoras reassured him by saying: »Don't worry, Euatle. You learn from me, and when you win your first case in court, you will pay the price you owe me for all the lessons I have given you«. Euatle gladly accepted the proposal and studied with Protagoras for years. After completion of the training, however, time passed, and Euatle did not pay for the classes with Protagoras, arguing that he had not yet won any case. One day, finally, Protagoras sued him. Before entering the trial, when he was at the door, Protagoras said to Euatle: »Whatever happens, you will pay me what you owe me. If I win the lawsuit, you will be sentenced to pay me. And if I lose, you will win your first case and will have to pay me«. Euatle replied to this: »No, master. Whatever happens, I will not pay you what I owe you. If I win, I will be exempted from paying. And if I lose, I won't have won my first case«"[2]. As the above example clearly shows, the strategic or even abusive use of law and the use of law as a weapon, also known as lawfare, is as old as law itself.

As Benjamin Wittes, Jack Goldsmith, and Robert Chesney write in their blog devoted to lawfare, in its contemporary meaning, the term was used as early as the 1950s in the United States, in contexts wholly unrelated to national security[3]. It was used by lawyers, particularly concerning divorce cases where spouses were disputing over property and child care so fiercely that it was justifiable to use the term „warfare", or in relation to other disputes in the courtroom, where the temperature exceeded the accepted standards of cultural behaviour. After World War II, the term was used in the context of the fight against colonialism. It was brought to international organisations, in particular to the UN. The procedures within the UN structures were limited to preparing resolutions condemning colonialism and legitimising national

1 S.W. Tiefenbrun, *Semiotic Definition of Lawfare*, „Case Western Reserve Journal of International Law" 2010, vol. 43, no. 1, p. 28 et seq.

2 J.L. Martí, *Lawfare and Democracy. Law as a weapon of war*, https://revistaidees.cat/en/lawfare-and-democracy-law-as-a-weapon-of-war/?pdf=25050 [access: 10.01.2024].

3 See www.lawfareblog.com [access: 14.01.2024].

liberation wars by its bodies, with the Trusteeship Council and the General Assembly in the lead. The term „lawfare" was even used in relation to judicial costs generated intentionally by lawyers to charge them to the opposing party. Currently, growing significance is given to using this term in the context of national security. There has been an agreement that the first time lawfare was referred to in the context of national security and international rivalry was in a military strategy book entitled „Unrestricted Warfare", written in 1999 by two officers of the Chinese People's Liberation Army, Qiao Liang and Wang Xiangsui[4].

They used the term to refer to a nation's use of international institutions to achieve strategic ends. The handbook became the basis for educating military command staff in China. It includes the Chinese plan to dominate the world and take over control through a decades-long strategy entailing corporate sabotage, cyberwarfare, and diplomatic measures. The plan also includes circumventing international standards in the sphere of intellectual property laws and taking over control of international financial markets[5].

The changing trends in international rivalry were noted by the Chief of General Staff of the Russian Federation, General Valery Gerasimov. He published an article entitled „The Value of Science in Foresight" in the „Military & Industrial Courier" weekly in February 2013, outlining a new strategy for conducting war operations. It consisted of more behind-the-scenes influence on the adversary's society than in open-armed activities. He noted that the rules of war had changed most of all in that the role of non-military methods for reaching political and strategic objectives was becoming increasingly significant, as in many cases, they turned out to be more effective than military power. This way, he expressed a new Russian doctrine of information warfare, hybrid warfare, or permanent warfare continuously taking place in the international setting. It seemed at the time that the world needed to prepare for new and unknown threats and manipulation in the sphere of propaganda, disinformation, and artificial intelligence algorithms, profiling individual users based on their online activities. On the one hand, it was disturbing. On the

4 Some share the opinion that the notion of lawfare in the context of an armed conflict was first used in mid-1970s by John Carlson and Neville Yeomans in their publication entitled *Whither Goeth the Law – Humanity or Barbarity*?, *The Way Out - Radical Alternatives in Australia*, eds. M. Smith, D. Crossley, Melbourne 1975.

5 See *Wojna bez zasad. Chiński plan dominacji nad światem*, https://historia.dorzeczy.pl/historia-wspolczesna/359164/wojna-bez-zasad-chinski-plan-dominacji-nad-swiatem.html [access: 14.01.2024].

other hand, it moved away from the threat of open military confrontation with the use of weapons of mass destruction, artillery and rocket shelling, with civilian casualties, bombarded cities and trenches drowning in mud, something we know very well from World War I and World War II.

The aggression of the Russian Federation against Ukraine in 2014, and its further staging in 2022, demonstrated that covert and subliminal actions based on social engineering methods have been set aside. Again, we are witnessing brutal, abrupt military violence on the part of the Russian armed forces. However, this does not mean that the Gerasimov doctrine of 2013 has lost its significance. On the contrary, its purpose was to throw Western states and their societies off guard, as they were not expecting the events that took place in Ukraine, particularly the full-scale open military aggression that started in February 2022.

In the West, the term „lawfare" was popularised thanks to a paper written by General Charles Dunlap in 2001[6]. In his article, Dunlap, as a professional soldier, focused on the restrictions for military operations conducted by the USA that arose from international humanitarian law in armed conflicts. He discussed the issue of whether contemporary humanitarian law constituted an obstacle to reaching strategic goals of military operations. He pointed to the significance and position of military lawyers and humanitarian law advisers who played a key role in planning and deploying military operations, participating in the targeting process and providing opinions on attack orders. In his essay, Dunlap declared that he would intentionally use the term „law of armed conflict" rather than the „international humanitarian law" prevailing in the international law doctrine. This was to serve as an expression of his limited trust in excessively restrictive humanitarian law standards in contemporary armed conflicts.

In his deliberations, Dunlap noted that law was not – and could never be – the vehicle to ameliorate the horror of war to the extent its advocates seem to expect. He also pointed to, in his view, the dangerous role of humanitarian law and lawyers in American military interventions. He stated that the role was surprisingly pervasive. In his opinion, the fulfilment of military objectives was each time counterpoised by altruistic, human rights-oriented reasons. He also assessed that the applicable rules of humanitarian law that affect the

6 C.J. Dunlap, *Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts*, https://people.duke.edu/~pfeaver/dunlap.pdf [access: 15.12.2023].

planning and deployment of armed conflict were often ill-informed by the realities of contemporary military strategy and available technologies. Finally, he pointed to the fact that there was disturbing evidence that the rule of law was being hijacked into just another way of fighting (lawfare) to the detriment of humanitarian values and the law itself.

Charles Dunlap understood the notion of lawfare in narrow terms, only concerning international humanitarian laws in armed conflicts, as a factor limiting the freedom of conflicting parties to select the measures and methods to harm their opponents and engage in armed combat. It seems that such an understanding of lawfare is currently the dominating one. Numerous studies and publications focus on the analysis of legal actions taken in the sphere of international relations that are aimed at constraining the possibility for states to operate freely in armed conflicts, including as part of the war against terrorism. Democratic states, where societies adhere to high standards in human rights protection, are particularly susceptible to such attacks.

Another example of using an international legal procedure to strike against the adversary was the resolution of the UN Security Council establishing a no-fly zone over Libya in 2011 (Resolution no. 1973 of 17 March 2011). In the Resolution, the Security Council expressed grave concern at the escalation of violence and the heavy civilian casualties, condemned the gross and systematic violation of human rights, including arbitrary detentions, enforced disappearances, torture and summary executions, as well as acts of violence and intimidation committed by the Libyan authorities against journalists, media professionals and associated personnel, and urged these authorities to comply with their obligations under international humanitarian law. On these grounds, the UN Security Council established a ban on all flights in the airspace of the Libyan Arab Jamahiriya in order to help protect civilians. At the same time, it authorised Member States, acting nationally or through regional organisations or arrangements, to take all necessary measures to enforce compliance with the ban on flights imposed by the Council. As a result, a military operation was commenced against Libyan armed forces loyal to Muammar Gaddafi. The United States conducted Operation Oddysey Dawn, France deployed Operation Harmattan, and the United Kingdom commenced operation under the code-name Ellamy. Canada also provided its military contingent. In late March 2011, NATO took over the military operation in Libya (Operation Unified Protector). Although, officially, the Security Council's Resolution No. 1973/2022 was aimed at protecting Libyan civilians exposed to shelling by Libyan air forces fighting against rebels, it struck the operational

capabilities of the Libyan air force to counteract the armed rebellion across its territory. It should be stressed that the rebels did not have any air force back then, so the ban on combat flights over Libya did not apply to them. The resolution provided the legal basis for bombarding Libyan forces loyal to Muammar Gaddafi and consequently for supporting the anti-government rebellion in Libya.

In this study, lawfare is understood in broad terms, similar to the meaning of Chinese unrestricted warfare or Russian information warfare in the Gerasimov Doctrine. Lawfare will be understood as social engineering measures aimed at shaping the domestic legal order of the opponent state to weaken its military, economic, and cultural potential in global or regional rivalry. More specifically, this paper refers to actions and operations conducted in cyberspace, on the Internet, on social media, engaging influencers and fake accounts, and so-called troll farms. The activities are to shape public opinion, create convictions about the need to introduce specified legal solutions or repeal existing standards or restrictions, provoke conflicts, antagonise the adversary's society internally and stir up social unrest.

Lawfare – activities in cyberspace

Social engineering measures (methods) can be overt or covert. Lawfare, as a hostile shaping of the opponent's legal order, includes several measures that ultimately lead public authorities to adopt unfavourable legal solutions under the pressure of public opinion, although in compliance with constitutional procedures. As such, it is about covert action characterised by false intent aimed at misinforming the public about the seeming benefits of the proposed solutions or imaginary threats.

Such measures may compromise national security and result in

- interference in military security structures,
- interference in political security structures,
- interference in social security structures,
- interference in health security structures,
- interference in energy security structures,
- interference in economic security structures.

As a rule, lawfare is based on covert and confidential actions. Hence, it is difficult to precisely indicate examples of social engineering methods being used in the course of shaping the opponent's legal or political order in a hostile

manner. However, an attempt can be made to point to the potential destructive capabilities of social engineering methods in the sphere of lawfare.

One of the more recent examples of using social engineering methods in international relations, affecting the legal and political order of states, includes presidential elections in the USA in 2016 – support for Donald Trump on his way to the White House and Russian intelligence's assessment that he would play a considerable role in reaching the strategic goals of Russia's foreign policy.

As Marcin A. Piotrowski, an analyst from the Polish Institute of International Affairs, proved in his analysis: „Available materials and reports by the U.S. intelligence community confirm the influence of the active measures undertaken by Russian intelligence on the recent presidential campaign and Trump's success. These activities represented significant interference in the political process in the United States. It is hard to obtain an objective measure of their direct impact on the electoral preferences of American voters. Nevertheless, even the incomplete information and general estimates currently available suggest one of the most sophisticated and ambitious operations carried out by Russian intelligence"[7]. The disclosed and published materials by U.S. intelligence confirmed the interference of the Russian Federation's special services in the course of the presidential campaign in 2016. The interference consisted of carrying out several cyberattacks targeting the databases of Hillary Clinton's electoral staff (Trump's opponent in electoral elections), obtaining classified materials and documents discrediting the former U.S. Secretary of State, and disclosing them to the public in the USA. The documents discrediting Hillary Clinton obtained and published by cyber operations contributed to her defeat in the presidential elections and allowed Donald Trump to succeed.

Another factor that played a major role in the 2016 USA presidential elections was using new voter profiling methods based on the analysis of big data. Huge data sets were analysed using artificial intelligence algorithms. Support to Donald Trump's electoral staff was offered by Cambridge Analytica, a British company that was infamous for illegally obtaining data of 50 million American Facebook users to profile them for electoral campaign purposes. As Infoshareacademy.com reports: „Cambridge Analytica is a UK-based

7 M.A. Piotrowski, *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*, https://pism.pl/publikacje/Ameryka_skie_oceny_dotycz_ce_ingerencji_Rosji_w_przebieg_wybor_w_prezydenckich_w_USA_ [access: 21.01.2024].

company providing political consulting services. The company purchased data of unaware Facebook users and used them to create targeted advertisements addressed to specified audiences. Such a message had a huge impact on the public sentiment of the decisive group of voters. It offered its services, among others, to Donald Trump's staff during the 2016 presidential elections"[8].

In the context of Brexit and the UK European Union membership referendum of 2016, intentional and intelligence-supported Brexit tendencies in the United Kingdom were suggested by applying social engineering techniques and big data to weaken the European Union and break its cohesion. Cambridge Analytica was also shown as providing analyses to support political circles of Brexit advocates and, at the same time, an entity having connections with Russian services. However, as was ultimately concluded by the UK data protection authority, Cambridge Analytica's activities did not influence the UK's EU membership referendum results. After three years of inquiry into the impact of Cambridge Analytica's operations on the Brexit referendum, the British Information Commissioner's Office announced that they had not found any evidence which would confirm the impact of the company's activities on the voting results. The investigation only confirmed that Cambridge Analytica had held several preliminary consultations with UKIP (United Kingdom Independence Party) which was calling for Brexit.

As reported by Cyberdefence24.pl, „Elizabeth Denham, Information Commissioner, commenting on the conclusion of the proceedings conducted by her office, stated that the investigation had revealed systemic vulnerabilities of the democratic system in the UK. As she noted, the investigation allowed a new understanding of the role of personal data use in the context of contemporary politics and introduced profound changes to the way the data are used for political purposes worldwide. Referring to the issue of whether the 2016 Brexit referendum was fair, Denham stressed that no major abuse of privacy and electronic marketing regulations had been found in personal data protection laws. Both the campaign groups opting for the UK to remain in the EU and those encouraging the citizens to leave the Community met the formal criteria marked out by the regulatory framework, said the Commissioner"[9].

8 *Jak dzięki Data Science wpłynąć na wybór prezydenta USA*, https://infoshareacademy.com/blog/2021/01/26/jak-dzieki-data-science-zmanipulowac-wyborami-na-najpotezniejszego-czlowieka-swiata/ [access: 28.12.2023].

9 *Wlk. Brytania: działania Cambridge Analytica nie miały wpływu na brexit*, https://cyberdefence24.pl/polityka-i-prawo/wlk-brytania-dzialania-cambridge-analytica-nie-mialy-wplywu-na-brexit [access: 5.01.2024].

Furthermore, there is no evidence of direct cooperation between Cambridge Analytica and the Russian services. The only Russian thread in this matter is related to Aleksandr Kogan, a psychologist born in 1986 in the then Moldavian Soviet Socialist Republic (part of the Soviet Union) who emigrated with his parents to the USA at the age of 7. Kogan, working as a lecturer at the University of Cambridge, created an app that collects data concerning the online activity of Facebook users (an app called „thisisyourdigitallife"). Using this app, UK-based Cambridge Analytica acquired data that later allowed the company to analyse the profiles of 50 million American voters who took part in the 2016 presidential election.

Another example of the potential use of destructive capabilities of social engineering methods in the sphere of lawfare is the so-called Wind Turbine Act, which was adopted in Poland in May 2016 and effectively blocked the development of the wind energy sector for many years. The situation lasted until the outbreak of war in Ukraine in February 2022 (on 5 July 2022, the Council of Ministers adopted a draft amendment to the Act on Wind Farm Projects, which liberalised the possibility of building new wind farms in relation to the need to intensify the use of renewable energy sources).

The Act on Wind Farm Projects of 20 May 2016, colloquially known as the Wind Turbine Act (or even the Anti-wind Turbine Act), was adopted by the Sejm, the lower house of the Polish Parliament, with votes from the ruling coalition. As stated in the justification for the draft act which was brought to the Sejm in 2016, it was possible to observe an immensely rapid development of the wind energy sector in Poland since 2009. „Unfortunately, no sufficient legal framework to regulate the location, construction and operation of wind farms has been provided thus far. The consequence of this situation is the location of the systems in places that are too close to residential buildings. This became the reason for numerous conflicts between dissatisfied residents and local authorities, as such devices are responsible for noise emissions and infrasound undetectable to the human ear. They cause vibration and shadow flicker, as well as may pose a direct threat to human life or health in the event of failure, plus the turbine blades may ice over in the winter. The situation resulted in numerous claims by citizens and associations (established specifically to counteract the construction of wind farms in specified locations/communes) addressed directly to Members of the Parliament or to the Council of Ministers who are requested to withhold the construction of wind farms. So far, around 50 claims and interpellations and 23 petitions have been submitted,

including 20 claims filed by associations[10]". In the bill, it was proposed that the distance between the wind farm and residential buildings (or valuable nature conservation areas) was at least ten times the total height of a wind turbine, meaning height measured from the ground level to the highest point of the structure, including the technical elements, i.e., the blades of the wind turbine. Such a solution was ultimately adopted in the Act. Assuming that the average height of a single turbine is approximately 150 metres, the distance of the structure from the nearest buildings could not be smaller than 1,5 kilometre. In practice, it meant that it was extremely difficult to find the right location for a wind farm in the territory of Poland. The development of wind energy as a renewable energy source (RES) was hindered by, on the one hand, public pressure from the aforementioned groups of protesting commune residents concerned about their lives and health, and by the political influence of the mining lobby producing coal, the core energy source for the Polish economy, on the other hand. The ruling coalition of conservative and national parties did not hide their sentiment towards traditional power supply sources and the mining circles, demonstrating their distrust of alternative, wind and solar energy sources. This approach was revised in the face of Russian aggression against Ukraine in February 2022, which sparked the energy crisis related to the sanctions imposed by the European Union on energy raw materials (coal, oil, and natural gas) from Russia. It instantly turned out that renewable energy sources may, on the one hand, ensure the state's energy independence in the face of limited supplies of energy raw materials from the east, and on the other hand, wind and photovoltaic farms distributed across the country might better secure energy supplies during a potential armed conflict when the enemy could effectively attack large coal-fired or nuclear power plants concentrated over a small area and cut off electricity supplies across the country, as could be observed in Ukraine.

There are currently no grounds to search for foreign interference, in particular on the part of Russian services in the process of enacting the said Act in the Polish Parliament, although in practice, it effectively blocked the growth of the wind energy sector in Poland for several years, in the times of the Russian aggression against Ukraine. It seems that it was enacted as a result of the Polish policy to support coal mining and pressure from the

10 *Druk nr 315, Poselski projekt ustawy o inwestycjach w zakresie elektrowni wiatrowych. Uzasadnienie*, https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=315 [access: 16.01.2024].

protesting residents of rural communes, concerned about the negative impact of wind turbines on their health, general well-being and landscape features. Nonetheless, such a situation might potentially serve as an example of the influence of public opinion on the operations of law-making bodies, whilst it is also possible that public opinion could be manipulated by disinformation on the negative impact of wind turbines on the health and well-being of people living nearby. The effective use of troll farms, fake social media accounts posing as actual users, and spreading false information on the adverse effects of infrasound and vibrations moving along the ground as a result of working wind turbines could produce a false sense of threat among the residents of communes where the construction of wind farms was being planned.

Similar phenomena could be observed during the COVID-19 pandemic that paralysed the world in 2019–2022. The exceptionally intense spread of the unknown virus and the severe course of infection, resulting in some of the patients' deaths, compelled the governments of numerous countries to announce temporary lockdowns, consisting of the obligatory closure of schools, workplaces, cultural institutions, and even ordering the residents to stay at home in fear of the spreading COVID-19 infections. It turned out that the only effective methods to combat the disease were masks protecting the airways from the virus, social distancing, enhanced personal hygiene and vaccinations. The latter, given their mass administration in the society, guaranteed a mild disease course and the end to the pandemic.

Vaccinations against various infectious diseases are, without doubt, one of the most important human inventions of the last centuries (starting from the late 18th century when a British physician, Edward Jenner, administered the cowpox virus to James Phippsow, an 8-year-old boy. Before the experiment, Jenner had observed that persons working with cattle did not fall ill with smallpox or their displease symptoms were mild. It was the first case of administering a vaccine and a breakthrough discovery, as smallpox, also referred to as black pox, had been a deadly threat to the world's population for years. The invention of vaccines, and their obligatory mass application in children and adults, provided people with tools to eliminate the epidemics of plague, smallpox, cholera, tuberculosis, diphtheria, pertussis, tetanus, typhus fever, yellow fever, measles, mumps, rubella, chickenpox, hepatitis B, and hepatitis A.

Knowledge of vaccines and preventive vaccinations has been widespread worldwide for nearly two hundred years. Their beneficial actions, potential side effects and threats to some patients are well-known. Injecting a foreign

substance into a human body, in other words, a vaccination, is a medical procedure which, as with every such method, involves the risk of failure or adverse effects. However, this does not change the fact that vaccination, as a medical procedure tested on a mass scale for two centuries, is one of the safest and most effective means to ensure the health and safety of large human populations.

Despite this knowledge, in the times of the COVID-19 pandemic, anti-vaccine movements have become active, particularly on the Internet, spreading disinformation on social media on the deadly effects of vaccines against the SARS-CoV-2 virus and exaggerating their negative consequences. On the one hand, the anti-vaccine movement could be a natural consequence of engaging people concerned about their lives and health, whereas, on the other hand, these anti-vaccine trends in specified countries could be intentionally fuelled by special services interfering in the health safety of a given country's population. There is no clear evidence to prove this type of special service operations, all the more so that the pandemic, as the name suggests, constituted a global threat and could easily spread from one country to another despite the travel restrictions in place. This means that actions compromising the health safety in one country could effortlessly bring negative consequences across the entire region or the globe, affecting the population of the state where such disinformation is generated using support from special services. Nonetheless, this type of a potential disinformation threat to the health safety of human populations is worth noting.

In addition to anti-vaccine movements during the COVID-19 pandemic, we could also observe public resistance to administrative restrictions of social and professional activities, so-called lockdown. On the one hand, such opposition was understandable, as individuals wanted to continue living and working normally. On the other hand, questioning the existence of the pandemic and ignoring bans on social contacts could contribute to the spread of the virus, and an increased number of infections and deaths. Again, accounts calling for social disobedience and evoking a sense of public resistance against decisions of public authorities became active on the Internet and in social media. In this case, it is also not possible to indicate clear-cut evidence that this type of public resistance was artificially generated by the special services of hostile states trying to affect the decisions of public authorities (including decisions in the sphere of legislation). However, such a potential threat in the times of the information revolution we are experiencing should be duly noted.

Another manifestation of special service activities is the potential online support for political formations whose political agenda is favourable to the strategic objectives of the interfering state that uses false propaganda to achieve them. The state which intends to pursue hostile propaganda activities can use social media to affect voters' sentiments and thus influence the results of presidential, parliamentary, and local elections, and referenda. Such a state may conduct an intelligence-supported evaluation of a given country, selecting parties that might contribute to fulfilling the strategic objectives set as part of the foreign policy of the interfering state or simply weaken the potential of the state being under attack. Regarding possible activities on the part of the Russian Federation, this would mean support for national, conservative, anti-EU and anti-western political formations. At the same time, as the war in Ukraine is taking place, it is also possible that the Russian Federation might support liberal and left-wing circles in the European Union, as they are perceived to be pacifist, against war, and afraid of the spread of the Russian aggression across other European countries, and hence more willing to make concessions to Russia at the cost of Ukraine.

The above-mentioned goals can also be achieved by influencing the shape of the electoral system in the target country to maintain the desired political formations in power. The target of the attack might be the electoral legislation, the vote-counting system, the reach of constituencies, etc.

The list of threats related to hostile activities based on social engineering tools, aimed at shaping the adversary's legal and political system, is not exhaustive. In the era of an information revolution, there are limitless possibilities to affect the legal and political systems of the opposing state in cyberspace. As shown by one of the most thoroughly examined examples of the US presidential election in 2016, the combination of intelligence operations, consisting of the theft and dissemination of sensitive data with propaganda, disinformation and profiling potential voters with the use of big data algorithms constitutes a tool that allows the fulfilment of any strategic objectives.

It is vital from the perspective of protecting the state's strategic interest to note these threats in cyberspace and counteract them effectively. This study only includes the analysis of examples of potential threats and indicates vulnerable areas of state security. It does not provide ready-made solutions or countermeasures. Proposed measures to counteract lawfare-related cyberthreats constitute the subject matter requiring in-depth analysis, in particular, on the part of services responsible for the protection of state security.

Bibliography

Dunlap C.J., *Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts*, https://people.duke.edu/~pfeaver/dunlap.pdf [access: 15.12.2023].

Jak dzięki Data Science wpłynąć na wybór prezydenta USA, https://infoshareacademy.com/blog/2021/01/26/jak-dzieki-data-science-zmanipulowac-wyborami-na-najpotezniejszego-czlowieka-swiata/ [access: 28.12.2023].

Martí J.L., *Lawfare and Democracy. Law as a weapon of war*, https://revistaidees.cat/en/lawfare-and-democracy-law-as-a-weapon-of-war/?pdf=25050 [access: 10.01.2024].

Piotrowski M.A., *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*, https://pism.pl/publikacje/Ameryka_skie_oceny_dotycz_ce_ingerencji_Rosji_w_przebieg_wybor_w_prezydenckich_w_USA_ [access: 21.01.2024].

Spalding R., *Wojna bez zasad. Chiński plan dominacji nad światem*, Warszawa 2022.

Tiefenbrun S.W., *Semiotic Definition of Lawfare*, „Case Western Reserve Journal of International Law" 2010, vol. 43, no. 1.

Wlk. Brytania: działania Cambridge Analytica nie miały wpływu na brexit, https://cyberdefence24.pl/polityka-i-prawo/wlk-brytania-dzialania-cambridge-analytica-nie-mialy-wplywu-na-brexit [access: 5.01.2024].

Wojna bez zasad. Chiński plan dominacji nad światem, https://historia.dorzeczy.pl/historia-wspolczesna/359164/wojna-bez-zasad-chinski-plan-dominacji-nad-swiatem.html [access: 14.01.2024].

Lawfare – wrogie kształtowanie systemu prawnego państwa poprzez działania w cyberprzestrzeni

Streszczenie

Autor analizuje ważne i aktualne zagadnienia dotyczące wykorzystania nowoczesnych technologii informacyjnych we wrogich działaniach przeciwko państwu w środowisku międzynarodowym. W pierwszej kolejności zdefiniował pojęcie „lawfare" jako metodę prowadzenia wojny informacyjnej. Następnie skoncentrował się na jej potencjalnych przejawach w cyberprzestrzeni, wskazał możliwe luki w systemie bezpieczeństwa informacyjnego państwa i wrażliwe obszary, podatne na metody wrogiego kształtowania systemu prawnego państwa.

Słowa kluczowe: lawfare, inżynieria społeczna, wojna informacyjna, cyberprzestrzeń