**Studia Bezpieczeństwa Narodowego**
Zeszyt 23 (2022)
ISSN 1508-5430, s. 11-18
DOI: 10.37055/sbn/149509

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

**National Security Studies**
Volume 23 (2022)
ISSN 1508-5430, pp. 11-18
DOI: 10.37055/sbn/149509

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

# CONSTITUTIONALISATION OF CYBER THREATS TO GENERALELECTIONS

# KONSTYTUCJONALIZACJA CYBERZAGROŻEŃ WYBORÓW POWSZECHNYCH

**Paweł Zawadzki**
Uniwersytet w Białymstoku

**Abstract.** Universal suffrage by means of technology can in some cases become essential. Voting by e-mail, text message or information system raises many ethical and legal challenges. Add to this the intensified wave of disinformation during the election campaign period, and a problem of a systemic nature may arise with respect to the question of the necessity of regulating elections by technical means at the constitutional level. Such a need arises from the obligation to maintain statehood both from the perspective of the implementation of elections and the impact on society of harmful disinformation, ending with cyber threats related to vote rigging, identity theft or hacking of election servers. The aim of this paper is to show the legality of disinformation during general elections at the constitutional level. An explanation of disinformation activities and an analysis of cyber attacks in selected countries around the world shows that disinformation and cyber attacks have a significant impact on the final outcome of general elections. In this state of affairs, the key question arises as to whether the good protected directly by the Constitution of the Republic of Poland should be attributed stronger protection of the freedom of speech, which is an individual right expressed in Article 54 of the Constitution of the Republic of Poland, or the assurance of security of the State and its citizens in the form of ensuring democratic elections in a state governed by the rule of law with the help of the criminalization at the constitutional level of disinformation and influence on general elections by technical means. Ensuring security of the State and its citizens is one of the cardinal duties of the Polish State enshrined in Article 5 of the Constitution of the Republic of Poland.
**Keywords:** Polish Constitution, hybrid threats, disinformation, cyber threats, general election
**Abstrakt.** Powszechne prawo wyborcze za pomocą technologii może w niektórych przypadkach stać się niezbędne. Głosowanie przez e-mail, sms czy system informacyjny wiąże się z wieloma wyzwaniami etycznymi i prawnymi. Dodając do tego nasiloną falę dezinformacji w okresie kampanii wyborczej, może powstać problem o charakterze systemowym w związku z koniecznością uregulowania wyborów środkami technicznymi na poziomie konstytucyjnym. Taka potrzeba wynika z obowiązku zachowania

państwowości zarówno z perspektywy przeprowadzenia wyborów, jak i wpływu na społeczeństwo szkodliwej dezinformacji, a skończywszy na zagrożeniach cybernetycznych związanych z fałszowaniem głosów, kradzieżą tożsamości czy włamywaniem się na serwery wyborcze. Celem niniejszego opracowania jest ukazanie legalności dezinformacji podczas wyborów powszechnych na poziomie konstytucyjnym. Wyjaśnienie działań dezinformacyjnych oraz analiza cyberataków w wybranych krajach świata pokazuje, że dezinformacja i cyberataki mają istotny wpływ na ostateczny wynik wyborów powszechnych. W tym stanie rzeczy nasuwa się kluczowe pytanie, czy dobru chronionemu bezpośrednio Konstytucją RP należy przypisać silniejszą ochronę wolności słowa, która jest prawem indywidualnym wyrażonym w art. 54 Konstytucji RP. Rzeczypospolitej Polskiej, czyli zapewnienie bezpieczeństwa państwa i jego obywateli w postaci zapewnienia demokratycznych wyborów w państwie prawa za pomocą kryminalizacji na poziomie konstytucyjnym dezinformacji i wpływu na wybory powszechne przez oznacza.
**Słowa kluczowe:** Konstytucja RP, zagrożenia hybrydowe, dezinformacja, cyberzagrożenia, wybory powszednie

## Introduction

The Constitution of the Republic of Poland has not been revised from the perspective of its relevance to the ongoing changes in society. The past twenty years of the constitution is a fair time for a neutral review. In 1997, elections were won by leaflets, advertisements and newspapers, while votes were cast and counted in person. Today this is not so obvious. Many of the phenomena that arise in connection with the spread of technology will inevitably lead to legal questions of a general nature. The rapid development of computerisation combined with the encroachment of technology in the sphere of election campaigning, the form of voting and the process of conducting elections may lead to an accumulation of normative changes at the lower register of implementation of statutory activities that will force the system to answer the question about the need to regulate disinformation and general elections at the constitutional level. These issues have not received much attention in the legal literature so far, so the article aims primarily to determine, on a preliminary basis, whether disinformation during the campaign period and the computerization of general elections brings constitutional challenges, and if so, what kind of challenges, and what difficulties may arise in the possible normativization of this phenomenon at the systemic level.

## Disinformation as a legal problem

Disinformation is intended to hint to the opponent's intentions and intentions that he will later put them into practice. The disinformer performs this action based on the principle of „leverage, triangle and wire".

Leverage is an action through an intermediary, nowadays the best network of intermediaries is social media, because if you prepare public opinion well, only the effect will be noticed, while the fact of disinformation itself will not be noticed.

The triangle is a spatial activity, which means that disinformation cannot have its source on the disinforming party or on the target party. For example, if Russia wanted to disinform Sweden, it would do it from Canada, so in the triangle it also uses the element of an intermediary.

A wire, as a rule, is an influential person located high up in the social hierarchy, he is never for or against. He does not have the psychological shape to always be against a state depending on the situation.

It is not difficult to imagine what will happen if we deal not with individuals but with masses, and these masses are informed by organisms interested in promoting a particular political ideology. Already before the Second World War Hitler in raping the crowds through political propaganda showed how to use techniques borrowed from experimental psychology to direct public opinion (Volkoff, 1999, p. 8) . A foreign state using disinformation in Poland can in fact influence the electoral outcome in the country in effect a favourable government that can pursue the vital interests of the foreign state. Seeing the effect of disinformation one can refer to Sun Tzu's doctrine: „The highest skill in the art of war is to subdue the enemy without fighting. In war, the best policy is to subdue the enemy state intact (Sun Tzu, 1994, p. 6) . Until the 20th century, the above doctrine did not need to be revised, as there was no fear of nuclear weapons and no mass media. It was only in the 1950s that the „D" department was created in Russia to deal with ideological diversion. In Soviet terminology, diversion means diverting attention by disinformation from hostile activities undertaken to destroy an enemy country. Ideological subversion is an open, legal activity that anyone, if they wish, can carry out because it is in accordance with the laws of Western civilisation, and therefore cannot be prosecuted as a crime. Therefore, for ideological subversion to be successful, it must take place in two directions, and it cannot be done if the opponent actively wants to participate in it. An example is Japan, which until the 20th century was a closed society. Whenever a foreign ship arrived in Japan, the authorities would not allow such a ship into the territory and suggested that it sail away. If the ship's captain did not obey the order, the Japanese army would sink the ship. Such a political line was followed so that culture, ideology, tradition and values would survive. Such a state could not be influenced, as the borders were closed and literature was censored by the authorities. The first condition for ideological upheaval is access, active participation, and Poland fulfils this condition: TV, social media, magazines, etc. Disinformation never goes against the tide, so it usually starts with demoralisation, a process that should take between 15 and 20 years to educate a generation of students. Aspects of life such as religion, the education system, the sphere of social life, state administration, the judiciary and the military are demoralised. As in any democratic state, social movements are formed in different directions, when the right time passes enemy disinformation centralises the demoralised social movements towards a crisis waiting for them to abandon the above values. When the demoralisation in the country reaches its

climax, destabilisation occurs, where the field of action narrows to radicalisation of all aspects of social life. Social groups become radicalised demanding rights for an ideology that used to be called a disease. This leads to the next stage called crisis, when the legal authorities in the state cease to function. At this point, various foreign bodies are introduced into the state in the form of various self-appointed colleges or, alternatively, revolutionary committees suddenly appear, as happened in Iran. The society sees that the state is not functioning properly and looks for a „saviour", naturally such a revolutionary committee knows how to restore the original state by taking over the legislative, executive and judicial authorities (Wolton, 1986, p. 6). Such cases took place for example in Lebanon or Afghanistan, after the seizure of power, the final phase called normalisation took place. The above presentation of the process of ideological subversion by means of disinformation was necessary in order to show what can happen if disinformation, i.e. activity to the detriment of others, is not criminalised on a constitutional level.

## Cyber threats to the general election

The 2016 US presidential election highlighted the cyber threats of interference by hostile states in democratic processes. A wealth of evidence has emerged showing how Russian agents hacked the Democratic National Convention and leaked confidential documents to undermine voter confidence, spread disinformation and propaganda to polarise and divide US citizens, and suppressed voters through targeted advertising and paid trolls. Hostile interference is a global threat, however, and there are lessons to be learned from the US election that will enable governments around the world to respond more quickly and effectively (May, 2016). In France, Emmanuel Macron's election campaign was disrupted by disclosures on the Pastebin platform (Pastebin - a web application that allows people to paste text and share it with others by following a relevant link. This service is particularly useful when longer text or source code needs to be sent via instant messaging or IRC channels, for example), and 9GB of data and 21,000 messages were stolen from the candidate's mailbox. The attacks lasted from October to May 2016. In April 2016, the referendum on the EU-Ukraine Trade Agreement was disrupted by the publication of a crafted video showing Ukrainian militants threatening the Netherlands with terrorist attacks. In the context of these events, the Dutch intelligence agency AIVD in mid-2014, undertook investigations into the activities of pro-Russian groups that could have a negative impact on the March 2017 parliamentary elections. During the 2015 Bundestag elections, the systems of the CDU Party, the Ministry of Finance and the Ministry of Foreign Affairs were hacked. According to information provided by the Federal Office for ICT Security and the Federal Office for the Protection of the Constitution, the APT 28 grouping was behind the attacks (APT28 - (STRONTIUM, Sofacy or

Fancy Bear) are names given by analysts to describe unknown perpetrators linked to a number of high-profile hacks and computer attacks). A few days before the elections in Ukraine, hackers removed some of the files responsible for the proper functioning of the voting system. The government confirmed the next day that the system had already been repaired. On the day of the elections, a virus installed on the computers of the Central Election Commission with the aim of publishing false results was eliminated. The announcement of correct election results was disrupted by DDoS attacks (DDoS is an attack on a computer system or network service to make it inoperable by seizing all available resources, carried out simultaneously from multiple computers. A DDoS attack is a variation of a DoS attack that involves attacking the victim from multiple locations simultaneously). Experts from the University of Edinburgh have shown that Russian troll farms produced 156,000 Twitter accounts. The posts were mainly shared in the days leading up to the referendum on Brexit with more than 45,000 tweets with a number of impressions reaching several hundred million, while the St Petersburg RIA produced 419 accounts from which 3468 tweets flowed. Mainly on Brexit and topics that arouse anti-Muslim sentiment (National Research Institute, 2018).

Cyber threats that are real in future elections in Poland could come in the form of:

1. manipulation of voting machines in the form of hacks into the computers of the institution conducting the elections and an attack on critical infrastructure;
2. attack of election-related systems in the form of redirection: sms, email, electronic vote, vote swapping and resending to the destination;
3. leakage of voting data to create chaos;
4. disinformation that will call into question whether the elections were held in a democratic manner.

Threats to democracy primarily concern the internal space of democratic states: the information system, the political system. Such attacks strike at institutions, constitutional principles and norms, values and procedures, destabilising the ability of a democratic state to function (Kruglashov, 2020, p. 81) . However, recent technological developments and growing interconnectedness have enabled some states to find ways to challenge the West through the use of so-called hybrid threats. This mode of warfare involves the synchronised use of a wide range of instruments that are designed to fall below the threshold of detection, attribution and retaliation. The combination of these (relatively cheap) threats with conventional threats confronts liberal democracies with difficult choices in defence budget allocation. While the stability of the conventional and nuclear arms race leads to a peaceful stalemate, this article shows that adding hybrid threats to the spectrum of state power projection leads to a gradual shift in the balance of power. While hybrid threats have been

widely analysed in the military literature, this article presents a paradigm-shifting study of hybrid threats from the perspective of democratically held general elections.

## Constitutionalisation of cyber security

The definition of the national interests of the state is directly stated in Article 5 of the Constitution of the Republic of Poland. „The Republic of Poland shall safeguard the independence and inviolability of its territory, ensure freedom and human and civil rights and the security of its citizens, safeguard the national heritage and ensure environmental protection, guided by the principle of sustainable development" (Constitution of the Republic of Poland of 2 April 1997). Separation of legal language from colloquial language does not mean lack of coherence between them, on the contrary - colloquial language corresponds to legal language giving foundations to classical formal logic, since legal language is not always strictly logical. A legal regulation in relation to a legal norm is a completely different conceptual category. As Lech Jamróz notes, „a legal regulation is a technical unit of a normative act. It is assumed that it can be identified with a linguistic phrase contained in a legal text and constituting an elementary part of this act, singled out by the legislator, e.g. in the form of an article or a paragraph. A legal norm, on the other hand, is a statement which is constructed on the basis of legal regulations, it is a rule of conduct containing the necessary directive elements (Jamróz, 2011, p. 129).

A rule of law is a legal norm of special importance. In the hierarchy it is superior to ordinary legal norms and is usually placed directly in the Constitution. As in the case of legal norms, they are the result of a logical cause and effect relationship. As a rule, they have primacy over ordinary legal norms in the case of a legal conflict. A legal principle may be legally binding if the norm in question is coherently recognised by doctrine and applied in practice, as a universally recognised principle of law (Leszczyński and Maroń, 2013, p. 81).

The „Constitutional principle of security of the state and citizens" was extracted from Article 5 of the Constitution of the Republic of Poland. As not every principle should have sanctions each principle should contain a hypothesis and dispositions that will create a logical whole. The construction of this legal principle requires linguistic, functional and systemic interpretation in order to show the abstract hypothesis, which by defining the prerequisites, through their occurrence in an actual situation, requires the application of the disposition. It should be noted, however, that the addressee of a legal principle, its characteristics, status, etc., should first be determined. The Republic of Poland guards the independence and inviolability of its territory, thus the State is the subjective element of the hypothesis comprising the legal principle. The hypothesis also includes an objective

element - i.e. premises defining situations, states, phenomena or events. The behaviour of the addressee of a legal principle depends on the occurrence of the premises. Also in this case, the good protected by law in the form of „security of the state and citizens" is specified. The disposition, on the other hand, is the word „protect". The above principle has a hypothesis and a disposition, and the fact that it is enshrined in the Constitution gives it the status of a constitutional principle. This is an innovative principle, since in jurisprudence we distinguish three types of dispositions, and with them legal norms - they occur in the imperative, prohibitory and permissive modes, of course, if there is a premise for it. However, in the case of this principle the disposition - to guard is realised as long as the subject of the hypothesis exists, in this case it is the Republic of Poland. It is not required that there be a threat to the security of the state and its citizens; as long as the state exists, it has a duty to protect this good protected by law.

Cyber security of elections is a constitutional challenge, as normativisation of this phenomenon at the level of the political system reveals legal conflicts. Thus, the question arises: how to ensure cyber security in the form of legal prevention of disinformation and hacking attacks on election systems in juxtaposition with Article 54 of the Polish Constitution, which provides that: „everyone shall be guaranteed the freedom to express his or her opinions and to acquire and disseminate information in addition, preventive censorship of social media and press licensing shall be prohibited" (Constitution of the Republic of Poland of 2 April 1997) . And in accordance with Article 14 of the Constitution of the Republic of Poland, the Republic of Poland shall ensure freedom of the press and other means of social communication (Nowińska, 2007, p. 33) . The jurisprudence emphasises that Article 54 (1) of the Constitution of the Republic of Poland expresses three separate but inherent freedoms: to express views, to obtain information and to disseminate information (Judgment of the Supreme Court of 2.7.2013, III SK 42/12). These freedoms constitute individual rights. The Constitutional Tribunal also notes that all forms of expression are subject to constitutional protection, and at the same time, freedom of expression is connected primarily with the expression of one's own views and is not limited only to facts (Judgment of the Constitutional Tribunal of 20 February 2007, ref. P 1/06).

In this state of affairs the key question arises, whether the good directly protected by the Constitution of the Republic of Poland should be attributed stronger protection of the freedom of speech, which is an individual right expressed in Article 54 of the Constitution of the Republic of Poland, or the assurance of security of the State and its citizens in the form of ensuring democratic elections in a state governed by the rule of law by means of criminalising disinformation at the constitutional level and influence on general elections by technical means.

## Conclusions

The main challenge to measures to protect electoral integrity is that they can, paradoxically, also have the effect of eroding basic democratic and constitutional rights. The first issue is whether restrictions on the influence of disinformation are constitutional. On the other hand, what will constitutional correctness give to the state if an anti-Polish grouping whose aim is to dismantle the state wins the general election? The constitution is the supreme expression of statehood, so it was enacted for ‚ever', not for a few years. Therefore, it would seem that ensuring security in the broad sense is indispensable for individuals to feel free in their own state, as the state is made for citizens. Constitutional law is one of those branches of law that develops dynamically, but it should not be limited to changes that have already been made. In cardinal matters for the state, the law should anticipate potential problems that may arise in the forthcoming general elections. The state should have the ability and the right to react, and perhaps criminalising activities that may serve to disrupt the peaceful existence of the state and are carried out with such intent, especially hybrid warfare or subversive activities, would resolve the constitutional impasse.

BIBLIOGRAFIA

[1] Jamróz, L.A., 2011. *SKARGA KONSTYTUCYJNA. Wstępne Rozpoznanie*, Temida 2.

[2] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).

[3] Kruglashov, A., 2020. *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*, East of Europe vol 6, 2/2020.

[4] Leszczyński, L. i Maroń, M., 2013. *Pojęcie i treść zasad prawa oraz generalnych klauzul odsyłających. Uwagi porównawcze*, Annales Universitat is Mariare – Skłodowska, Lublin in – Polonia, VOL. LX, 1, SECTIO G 2013.

[5] Maj, M., 2016. *Zagrożenie cyberatakami wyborów prezydenckich w USA*[online]. Dostępne pod adresem: https://www.cybsecurity.org/pl/zagrozenie-cyberatakami-wyborow-prezydenckich-w-usa/ [dostęp: 12 marca 2022].

[6] Nowińska, E., 2007. *Wolność wypowiedzi prasowej*, Warszawa.

[7] Państwowy Instytut Badawczy, 2018. *Cyberzagrożenia w czasie kampanii wyborczych* [online]. Dostępne pod adresem: https://bezpiecznewybory.pl/baza-wiedzy/cyberzagrozenia-w-czasie--kampanii-wyborczych [dostęp: 12.03.2022].

[8] Sun Tzu,. 1994. *Sztuka Wojny*, wydawnictwo Przedświt, Warszawa, ISBN 83-7057-025-9.

[9] Volkoff, V., 1999. *Psychosocjotechnika, dezinformacja – oręż wojny*, Komorów.

[10] Wolton, T., 1986. *Le KGB en France*, Paryż.

[11] Wyrok Trybunału Konstytucyjnego z dnia 20 lutego 2007 r. sygn. akt P 1/06, (Dz.U. 2007 nr 36 poz. 234).