Over the past years, the phenomenon of external information interference in the electoral process has been gaining increasing representation in political discourse. We are witnessing the emergence of more and more new statements by various countries about the invasion of their national political systems by external actors. A considerable number of scientific works of both Western European and American and Anglo-Saxon scientists are devoted to this problem (Bartos, Mercea, 2019: 28–54; Bessi, Ferrara, 2016; Ferrara, 2017; Baines, Jones, 2018: 12–19; Keller, Klinger, 2018; Pope, 2018: 24–38).

Russia, USA, France, Germany, Great Britain, Spain (Catalonia), Montenegro, Ukraine are only a small part of a long list of states declaring interference in their elections. Nonetheless, considering politics as a system of relations evolving over the conquest, retention, distribution, and realization of power, we note that this kind of relationship always unfolds in public and at the same time highly competitive space. The presence of a significant number of political actors, including shadow ones, consisting of various relationships and interactions, whose complexity levels are steadily increasing, is typical of contemporary national electoral systems.

Given this, the electoral system of the modern state cannot be subject to complete “encapsulation.” Moreover, in the conditions of globalization of the contemporary world, the sovereign policy of the leading states has a significant impact on the political processes in other countries and forms the international political situation. This circumstance also leads us to the question of whether the political (and, in particular, electoral) process of a particular state can be a completely closed system.

An affirmative answer to the question posed would be quite paradoxical because the presence of an environmental impact (in this case, an international political space) is in itself, within the framework of the classical general theory of systems, a characteristic of an open, but not closed, system that will surely and inevitably exposed and the reverse influence of the environment.

In this case, we can talk about the presence of a significant number of political actors representing their interests in the framework of the elections, which, we emphasize once again, are held in conditions of publicity and high competitiveness, as well as systemic openness. These conditions are essential for any contemporary democratic regime, and an attempt to deny this fact is characteristic of authoritarian regimes trying to make their political and electoral systems as close as possible).
As for the online space, it is even more competitive than the traditional public offline space, it actively expresses and promotes its interests a significant number of institutional and non-institutional actors in political activities (Eberwein, Porlezza, Splendone, 2016; Stier, Bleier, Lietz, Strohnaier, 2018: 50–74; Williams, 2017: 207–211; Kreiss, Lawrence, McGregor, 2018: 8–31; Kovic, Rauchfleisch, Sele, Caspar, 2018: 69–85; Lee, 2017: 62–82).

Can political competition be considered interference in elections under such conditions? Can competition in the public political space be classified as an invasion of the sovereign electoral process? Can political actors, having their political interests in specific states, extraterritorially articulate them in the public space of the relevant electoral processes? What characteristics should an interested political person possess so that he can be classified as an “external agent of intervention”? Under the conditions of mutual influence on each other and the formation of international political conglomerations, how should “internal” actors be separated from “external” actors? Can the activity of non-institutional political actors be seen as interference in elections? Are the characteristics of national election campaigns changing in the context of globalization and the intensive evolution of the Internet as an extraterritorial political communications space?

The answers to these questions in many respects can determine the very viability and substantial characteristics of the phenomenon of interference with elections in contemporary conditions.

Unfortunately, today we are only at the stage of raising such questions in the scientific community. The main number of scientific works in this area is devoted to the issues of identifying and analyzing methods, technologies, and consequences of informational interference in the traditional electoral process (see, for example: Hart, Klink, 2017: 97–104; King, Pan, Roberts, 2017: 484–501; Brooking, Singer, 2016).

This state of affairs mainly has objective reasons, since democracies tend to respond rather slowly to crises – their checks and balances, open discussion and public participation do not contribute to quick decision making. However, in our profound conviction, the electoral process will never return to the traditional formats in the conditions of the development of contemporary digital information and communication technologies.

The influence of the Internet, it seems to us, is irreversible and requires a revision of the classical ideas about the electoral system and national information security. Already today, political systems operate in hybrid modes, being subject to significant digital influence both within their own national spaces and outside.

Back in 2006, Benkler pointed out in his work that radical democratization of access to intellectual products and facilitating the distribution of these products thanks to cheap computers and the Internet in a short time can change the political lives of people beyond recognition (Benkler, 2006). At the same time, the initially established information openness and extraterritoriality of the Internet today makes it a global tool for the destruction of traditional value-semantic spaces and the substitution of ideas about the socio-political reality for a significant part of citizens with high political and electoral activity.

In many cases, this leads to the transformation of mass electoral attitudes and models of electoral behavior with an emphasis on the formation of a mass protest potential.

The extraterritorial formation of alternative and, as a rule, protest models of worldview and behavior, the substitution of cultural codes and values make it possible to exert pressure on the political regimes operating in the states, undermine the stability of their functioning, transform the electoral space and have a significant impact on the electoral process with an emphasis on the legitimization of existing power institutions, which is one of the main challenges to the entire system of sovereign political governance of contemporary state (Ruijgrok, 2017: 498–520; Wagner, Gainous, 2013: 261–275).

Contemporary political practice demonstrates the presence of a significant number of global policymakers associated with attempts to dominate the national political spaces of the target countries and monopolize the information and communication infrastructure of the Internet as one of the key platforms for external information invasion. As a result, today there is a situation in which modern states are in a state of intense informational confrontation, which provides access to the core of electoral processes in the countries of the opponents.

At the same time, in addition to such subjects of information confrontation as a state, various non-institutional and neo-institutional subjects should be singled out, for example, international terrorist organizations that actively carry out their own propaganda activities on a global scale. A significant number of works are devoted to this problem, which emphasizes the high urgency of the problem of the penetration of terrorist structures into the network space (Innes, Dobreva, Innes, 2019; Shirinyants, Gutorov, 2017: 277–293; Shirinyants, Gutorov, 2018: 235–247; Styszyński, 2016: 193–201; Holt, Stonhouse, Freilich, Chermak, 2019).

Also, in this informational confrontation, the advantages will be gained by the states possessing the most diverse arsenal of means, methods, and technologies for conducting the struggle in the information space as compared with their opponents. The struggle for the possibility of influencing the mass consciousness in the right direction, the formation of profitable models of political behavior, the creation or destruction of values, the introduction of the “correct” political stereotypes and attitudes into the public consciousness. The struggle for the possibility of communication impact on public consciousness, access to the “molecular core” of national consciousness for the destruction of traditional value-semantic orientations, the introduction of beneficial stereotypes, attitudes, models of ideas about socio-political reality throughout the country becomes key in contemporary political practice.

These opportunities for information and communication impact determine the potential and effectiveness of processes aimed, as a rule, at undermining the stability of the current political regimes of opponents and redistributing power from national political elites to representatives of the “new government” in the processes of interference with the electoral process. In this regard, the creation of information and communication infrastructure, the development of methods of information work in the Internet space, as well as the development and use of effective communication technologies in the network is a critical task for any modern state.

In the absence of its own communication infrastructure and skills to use it for information work with its population, any state exposes itself to the risk of losing control
over the national information space, which in the context of globalization of the world is fraught with severe consequences.\(^1\)

The presence of a developed communication infrastructure across the country and the active (and at the same time, diverse and effective) its use in state-political management are today one of the essential conditions for ensuring political stability and information security of the state as such.

The problem of information security and the sovereignty of the modern state on the Internet is becoming one of the most pressing in the context of the rapid development of information and communication technologies. An opposition to external information expansion is becoming one of the most important tasks of modern political governance at the state level in order to preserve the sovereignty of the national political communication space, including the national segments of the Internet (Verrall, Mason, 2018: 20–28).

It is evident that the emphasis in external interference processes in the sovereign electoral process today is shifting towards the online space, which has become a principal source of information for crucial politically active electoral groups, including young people, considered today by external interested parties as the primary carrier of protest potential in the implementation of Regime Change projects.

At the same time, the transformation of the online space into a tool of global information confrontation generates a response – a growing fragmentation of the Internet into national segments, protected by each state, ensuring its own information security and trying to resist active attempts to exert external influence on public consciousness, including the electoral process.

Many countries are actively using contemporary digital communication technologies in the network space in their own political interests. For example, after a series of anti-corruption protests in Turkey and critical media coverage in the international media, the Turkish government hired thousands of professional trolls in the attempt to create an army in social networks. In Venezuela, authorities used pro-government bots on Twitter to manipulate one of the few news sources not yet controlled by the state; The fake Twitter followers of Venezuelan President Nicolas Maduro were so loyal that he became the third most retweeted public figure in the world, second only to the King of Saudi Arabia and the Pope of Rome (Brooking, Singer, 2016).

Besides, today we can observe from many states an activity aimed at preventing the possibilities of broad access by their population to external Internet resources broadcasting value, semantic and ideological models alien to a particular society that could adversely affect the stability of functioning political regimes and election results.

In addition to countering the information and communication impact on public consciousness by external resources, many states also pursue a policy of protecting their own national network resources and preventing them from falling under the control of external interested parties.

\(^1\) According to the law of the required diversity of Ashby, according to which one variety can be conquered by a large variety. An entity with a more diverse arsenal of means for communicating with target audiences has a clear advantage when working in the information space as compared with a subject limited in the choice of means, channels and communication technologies, which undoubtedly represents a certain threat from the point of view of ensuring information security on a scale a whole state that does not develop modern communication technologies.
In this regard, in countries such as Germany, Canada, China, Italy, Iran, South Korea, Turkey, Australia, Thailand, Belarus, Azerbaijan, Denmark, Algeria, Bahrain, Belgium, Burma, Vietnam, Egypt, India, Jordan, Iraq, Kazakhstan, Kyrgyzstan, Cuba, Malaysia, the United Arab Emirates, Pakistan, Saudi Arabia, North Korea, Singapore, Syria, Tunisia, Turkmenistan, Uzbekistan and others have seen the introduction of state control over the network space into political practice.

In contrast to the openness and globality of the Internet space declared and supported by a significant number of Western countries, many modern states are striving to manage their own national online segments. For this, technologies such as content filtering, user authorization and the prohibition of anonymous use of Internet resources, restricting access to external and internal Internet sources of information are actively used. In Russia, recently, the blocking of Internet resources introduced at the legislative level, which pose a threat from the standpoint of ensuring national information security, has also been practiced. In the case of the implementation of this scenario, the Internet with a high degree of probability can turn into an aggregate of closed national online spaces, the exchange of information between and within which will be under state control.

At the same time, the problem of ensuring the freedom of the Internet from the growth of digital authoritarianism is actualized and acquires new meaning. Modern information and communication technologies should allow citizens to make their own political choices without coercion or hidden manipulations. However, if anti-democratic structures effectively seize the Internet, citizens will be denied a forum for formulating common values, discussing political issues and resolving intra-social disputes peacefully.

For democracy to survive the digital age, technology companies, governments, and civil society must work together to find real solutions to the problems of social media manipulation and illegal data collection.

In the meantime, the Internet is becoming less and less free in many countries, and democratic regimes themselves are under pressure from its influence. For example, when the last presidential elections were held in Venezuela, designed to consolidate the authoritarian rule of Nicholas Maduro, the government accepted the law, which provided for harsh prison sentences for inciting “hatred” on the Internet. The introduction of the “Map of the Fatherland” – an electronic identification system used to direct social assistance – has raised suspicions that the data collected using the device can be used to monitor and put pressure on voters. On the eve of the July 2018 general election, Cambodia experienced a surge in arrests and prison sentences for speaking on the Internet, as the government sought to expand the arsenal of crimes used to suppress dissent, including a new law prohibiting insults to the monarchy.

There are quite a few such examples, and they all show that in a number of countries, under the pretext of protecting the sovereign information space, there is a movement towards digital authoritarianism using models of extensive censorship and automated surveillance systems. Only in 2017, the tactics of manipulation and misinformation in the Internet space played an important role in elections in at least 17 other countries, which undermined the ability of citizens to choose their leaders based on actual news and genuine debate (Freedom on the Net 2017). In 2018, as a result of these trends,
according to Freedom on the Net, global Internet freedom also continued to decline for the eighth consecutive year (Shahbaz, 2018).

In essence, this is about the disintegration of the Internet empire in its traditional democratic understanding and the creation of a number of independent and sometimes quite authoritarian virtual territories with fragile information and communication links among themselves. Moreover, in the event of aggravation of foreign policy relations, in the context of possible global and interstate crises, links between national segments of the online space can be blocked entirely by states to ensure their own cybersecurity. At the same time, the parties involved in the information confrontation will make ongoing attempts to “hack” someone else’s communication space in order to gain the possibility of broadcasting their own content to the public consciousness of the population of the adversary state, including periods of election campaigns.

The Russian approach to understanding the Internet space assumes recognition of the presence of national online segments with issues of international and national information security arising from this position. The draft Concept of the Foreign Policy of the Russian Federation enshrines contemporary realities, according to which Russia acts as an independent subject of forming a state system of counteracting information threats in the sphere of political and public security at the national level, including protection from external information interference in the internal affairs of Russia (The Concept of foreign policy of the Russian Federation).

In this regard, at the level of various state and intergovernmental institutions, Russia actively participates in shaping the concept of information security, taking into account the possibilities of using the Internet to implement information interventions. Remarkably, discussions about cybersecurity in Russia, as well as in the countries of North America and Western Europe increasingly resemble each other in terms of the issues under consideration (Pigman, 2018).

As a result of the collision of two conflicting paradigms (the Internet is a global information and communication space, and the Internet is a set of national online segments), a scenario of the development of the Internet space is formed, within which the outlines of two main groups of countries that adhere Internet as a space for political communications.

On the one hand, we can observe a group of technologically advanced countries headed by the United States that do not recognize national segments of the online space and view the Internet beyond national borders, which provides them with opportunities to promote democratic values and ensure freedom of speech and the right to access information (Aaronson, 2017: 232–254; Seo, Thorson, 2017: 141–155; Bildt, Smith, 2016: 142–156; Perez, Ben-David, 2012: 293–310; Adami, 2014: 163–180; Chandler, 2007: 283–298; Christou, Simpson, 2011: 241–257).

As US Secretary of State Hillary Clinton stated back in 2010, the United States will ensure freedom of speech and the right to access information in the Internet space, including foreign countries. In this case, it is primarily about providing access to US global resources, such as Google, Facebook, Twitter, Wikipedia. Any attempts to manage their own national segments of the online space by states are considered and will be viewed by the American authorities as a violation of democracy and a restriction of human rights. According to Clinton, authorities in some countries use the topic of
Internet governance as a cover for plans to limit human rights online. They want to remove civil society and business from network management, to erect national barriers in cyberspace, wanting to replace an effectively functioning repressive system (Chernenko, 2013: 162–170).

On the other hand, an increasingly numerous alternative group of countries is emerging that recognize the presence of national segments of online space and the right of states to exercise control over their own information space, including limiting external information and communication influence on public consciousness within their borders (Shen, 2016: 304–324; Safshekan, 2017: 266–284; Jiang, 2016: 202–220; Akhavan, 2013: 131–133).

This kind of global division of countries into fundamentally different in terms of approaches to understanding the essence of Internet space blocks can pose new global challenges in contemporary conditions of social development, lead to a revision of the very concept of open space, and also translate the information confrontation to a fundamentally different level of content and scale. What will be meant by interference in the electoral process in the interpretation of representatives of the designated blocks, and to what extent the positions of these blocks will be incompatible – this in itself ensures the formation of a potential global conflict between states in the field of national information security.

Anyway, today we can state the need to revise existing ideas about the Internet and its main characteristics due to the ambiguity of current approaches to its understanding. As the intensity of the information confrontation between leading states is steadily increasing, uncertainty, ambivalence of approaches to understanding the Internet space will increasingly influence the formation of interstate political conflicts, and also act as a factor in destabilizing the international political situation, as well as a pretext for imposing economic sanctions on strategic competitors on the world stage.

Moreover, in our opinion, the struggle to consolidate a precise understanding of the essence of the Internet space in the framework of international law will be the primary strategic task of the leading powers in the field of global politics. The international regulatory framework can largely determine the possibilities and nature of the information influence of states in the Internet space, as well as influence the global processes of contemporary politics. However, in the current conditions of the ambiguity of understanding whether the Internet is a single space, or within its borders there are separate national segments, discussions about interference in the electoral process of certain states seem to us incorrect, requiring the formation of a specific international convention.

At the same time, given the ambiguity and unsettled nature of the issue, the very phenomenon of interference in elections becomes not so much an objective process as an instrument of the information struggle, mass political propaganda and discredit of political opponents, a manipulative tool of international scope. As Benkler rightly writes in this connection, “the fundamental driver of disinformation in American politics of the past three years has not been Russia, but Fox News and the insular right-wing media ecosystem it anchors. All the Russians did was jump on the right-wing propaganda bandwagon: Their efforts were small in scope, relative to homegrown media efforts. And what propaganda victories the Russians achieved occurred only
when the right-wing media machine picked up stories and, often, embellished them” (Benkler, 2018).

The formation of international institutions for managing the global online space as a unified communication environment, in which all states have collective responsibility and obligations to maintain the openness and transparency of the Internet, can be a useful tool for solving this problem. This scenario seems to be the most optimal from the standpoint of international information security and the possibility of avoiding the transformation of Internet space into an instrument of total information pressure from one or more political forces to the detriment of most other states. Minimizing the risks of unmanaged political conflicts related to the topic of interference in the elections of a state also seems to be a realizable task under such a scenario. International management of the Internet space potentially allows for equal opportunities for political participation of various countries in information activities at the global level.

At the same time, the formation of international Internet governance institutions provides ample opportunities to resolve information conflicts between states, including those associated with interference with elections. In our opinion, it is necessary to form united international institutions-regulators capable of preventing and regulating information conflicts in the Internet space, similar to the existing UN peacekeeping forces ensuring the prevention and settlement of military conflicts. Such a solution is mainly capable of reducing global political risks (including risks associated with potential interference in the electoral process of sovereign states) arising from the implementation of other scenarios for the development of the Internet in the contemporary world, forming the collective responsibility of countries in the framework of the Internet.

REFERENCES


Adami R. (2014), Human rights for more than one voice: rethinking political space beyond the global/local divide, “Ethics & Global Politics”, Vol. 7, No. 4.


The article analyzes the phenomenon of digital interference with national political systems in the conditions of the modern information society and the evolution of the Internet as a space of political communications. It is shown that digital intervention is relevant but at the same time a complex multidimensional phenomenon of contemporary politics. In many respects, the potential of the digital interference phenomenon is closely related to the substantive and functional features of the functioning and transformation of the contemporary Internet, which has been actively used when changing political regimes in many countries. The initiatives of countries to form the sovereign national segments of the Internet space are, on the one hand, an attempt to protect their political systems from external influence and invasion, to ensure their own political stability, and on the other hand, they pose risks to the democratic potential of the Internet. The article substantiates the thesis that the phenomenon of interference with elections in actual practice often becomes not so much an objective process as an instrument of information warfare,

ABSTRACT


mass political propaganda and discredit of political opponents, a manipulative tool that can be actively used not only by authoritarian regimes with a low level of democratic development. It is noted that differences in understanding and defining the essence of the Internet by various countries give rise to a significant potential for political conflicts on a global scale. This leads the author to conclude that it is necessary to form institutions that are able to prevent and regulate information conflicts in the Internet space, as well as reduce global political risks (including risks associated with potential interference in the electoral process of sovereign states), forming a collective responsibility in the functioning of the global Internet.

**Keywords:** Internet communications, digital interference, informational confrontation, political system, electoral process

---

**INTERWENCJA CYFROWA W KRAJOWYCH SYSTEMACH POLITYCZNYCH W WARUNKACH WSPÓŁCZESNEGO SPOŁECZEŃSTWA INFORMACYJNEGO**

**STRESZCZENIE**

Artykuł analizuje zjawisko ingerencji cyfrowej w krajowe systemy polityczne w warunkach współczesnego społeczeństwa informacyjnego oraz ewolucję Internetu jako przestrzeni komunikacji politycznej. Wykazano, że interwencja cyfrowa to istotne i jednocześnie złożone, wielowymiarowe zjawisko współczesnej polityki. Pod wieloma względami potencjał zjawiska zakłóceń cyfrowych jest ściśle związany z merytorycznymi i funkcjonalnymi cechami działania i transformacji współczesnego Internetu, który jest aktywnie wykorzystywany przy zmianie ustrojów politycznych w wielu krajach. Inicjatywy krajów zmierzające do utworzenia suwerennych krajowych segmentów przestrzeni internetowej są – z jednej strony – podejmowaną w celu zapewnienia sobie stabilności politycznej próbą ochrony swoich systemów politycznych przed wpływami zewnętrznych i inwazją, a z drugiej strony, stanowią ryzyko dla demokratycznego potencjału Internetu. Artykuł uzasadnia tezę, że w praktyce zjawisko ingerencji w wybory często staje się nie tyle obiektywnym procesem, co narzędziem wojny informacyjnej, masowej propagandy politycznej i dyskredytacji przeciwników politycznych oraz narzędziem manipulacji, które może być aktywnie wykorzystywane nie tylko przez reżimy autorytarne o niskim poziomie rozwoju demokratycznego. Podkreślono, że różnice w rozumieniu i definiowaniu istoty Internetu przez różne kraje powodują znaczny potencjał konfliktów politycznych w skali globalnej. Prowadzi to autora do wniosku, że konieczne jest utworzenie instytucji zdolnych do zapobiegania konfliktom informacyjnym w przestrzeni internetowej i ich regulowania, a także do ograniczania globalnego ryzyka politycznego (w tym ryzyka związanego z potencjalną ingerencją w proces wyborczy suwerennych państw) i formowania zbiorowej odpowiedzialności za funkcjonowanie globalnego Internetu.

**Słowa kluczowe:** komunikacja internetowa, ingerencja cyfrowa, konfrontacja informacyjna, system polityczny, proces wyborczy