ARTYKUŁY

„Polityka i Społeczeństwo" 1(17) / 2019
DOI: 10.15584/polispol.2019.1.7

Taras Gurzhii*

FREEDOM OF THOUGHT VS. NATIONAL SECURITY INTERESTS: THE ISSUES OF HYBRID WARFARE IN UKRAINE

SWOBODA MYŚLI VS. KRAJOWE INTERESY BEZPIECZEŃSTWA: KWESTIE WOJNY HYBRYDOWEJ NA UKRAINIE

Abstrakt

Artykuł omawia perspektywy ukraińskiego prawa informacyjnego w kontekście wojny hybrydowej, która spowodowała powstanie nowych stosunków publicznych określonych przez konfrontację informacji, organizację środków bezpieczeństwa, wprowadzenie reżimów sankcyjnych. Przedstawiono zakres zagrożeń informacyjnych związanych z wojną hybrydową; ich wpływ na analizowaną sferę bezpieczeństwa narodowego. Założono, że w czasie wojny hybrydowej w państwie powstaje szeroki zakres zagrożeń informacyjnych. Ich neutralizacja z jednej strony wymaga zastosowania nadzwyczajnych środków prawnych i administracyjnych, a z drugiej strony może zaprowadzić istotne ograniczenia demokratycznych praw i wolności. Opierając się na dualistycznym charakterze prawa informacyjnego, jako narzędziu ograniczeń gwarancji praw i wolności informacyjnych, argumentuje się, że koncepcja jego rozwoju powinna opierać się na równowadze między interesami bezpieczeństwa narodowego a ideami praworządności.

Słowa kluczowe: wojna hybrydowa, zagrożenia informacyjne, bezpieczeństwo narodowe, prawo informacyjne, prawa i wolności informacyjne

Introduction

It is well known that one of the main aspects of hybrid warfare is information operations. Such operations aim to suppress the resistance of the targeted country, sow panic in society, and, as well, to shape the world political narrative according to the interests of the aggressor. To

* Department of administrative, financial and informational law, Faculty of international trade and law, Kyiv national trade and economics university, Kioto St. 19, Kyiv-156, 02156, Ukraine, e-mail: nosterlex@gmail.com, ORCID ID 0000-0002-3348-8298

do this, various tools are used: the introduction of biased media projects, creation of so-called "troll factories", multiplying "bots", distribution of fake news and many other techniques, contrary to honest journalistic practice.

From year to year, the use of information resources for political purposes becomes more and more organized. During the last decade, militant units for information special operations and information security have been created in most leading countries of the world. Such units officially exist in a few dozen countries, and unofficially – in more than a hundred. Their tasks include espionage, cyberattacks and information wars, including various means of influencing the mood and behavior of the population of the country. Only in Russia, the Forces of Information Operations consist of about 1,000 highly skilled specialists: programmers, engineers, cryptographers, communications specialists, experts in electronic attacks and others. Their annual funding is over $300 million (Dolmatova, 2017).

How harmful and destructive such a well-organized power can be, is evident from the events of the 2016 US presidential campaign (Hillary Clinton email controversy), the attack on computer systems of Organization Security and Co-operation in Europe (OSCE) in the year 2016/2017, and a series of hacker attacks in Ukraine that caused huge problems in the functioning of authorities, state enterprises, institutions and banks (April-June 2017) (Sanger 2017, Justin 2017, Dearden 2017).

Even in peaceful times, such situations determine the need for the development of legal, organizational, technical and other measures aimed at strengthening informational security (Дешко, Бондарєва 2018). As for the period of hybrid warfare, this need becomes of vital importance.

It is widely assumed that hybrid warfare requires a re-balancing of society's needs for liberty and security through mechanisms by which security can be bought only at the price of liberty (Pue W. 2003). But it is also evident that the amount of freedom that can be sacrificed for national security is not infinite. The solution to this dilemma greatly depends on the identity of the targeted state, being democratic and compliant with basic human values.

The past decades have seen enormous changes in the system of threats to privacy and in the perception of security, the causes of insecurity and the measures adopted to address them. Therefore, it is worth evaluating whether the limitations of rights and freedoms are reasonable and necessary in a state in order to achieve certain national security aims (Pranevičienė 2011: 1611).

In the light of the above, the *main aim* of the work is to formulate the conceptual grounds for the development of the state informational policy under conditions of hybrid warfare. This aim implies the need for complex research, based on an analysis of international and informational legislation, law making and law enforcement practice, and modern trends in public administration.

In this context, the hypothesis is based on the assertion that a successful solution of various problems of personal data protection in modern Ukraine is possible only within the framework of integrated policy, grounded in a balance between the interests of national security and human rights protection (Gurzhii T., Gurzhii A., Seliukov V. 2018, Гуржій 2018).

Knowledge acquisitions of the study. The dialectical method provided a comprehensive consideration of the issues of national security in the face of information threats posed by the hybrid warfare. With the deductive method, the genesis of information policy of Ukraine is overviewed. The use of the inductive method allowed the issues of realization informational rights and freedoms on the example of certain practical casestobe highlighted. The method of analysis was used to examine modern scientific research, as well as to study the main trends of scientific thought. Through the prism of the systematic approach, information policy considered as the integral unity of national security and human rightprotection activities.

Among scientists who explored information relations in the context of hybrid war, the works of Nissen (2015), Svetoka (2016), Vračar, Radin (2017), Ćurčić (2018) should be outlined.

The theoretical basis for this work is a theory of a "Balance between Human Rights and National Security", according to which resolving the conflict arising between the need for national security and human rights should be based on the doctrine of proportionality (Godler, Williams 2006, Arden 2015).

1. Information as a tool of hybrid warfare

The experts distinguish at least six ways of using mass media for hybrid warfare: – intelligence collection; – targeting; – psychological influence; – cyber operations; – defense; – command and control. All of these activities, regardless of whether they have online or offline effects, can be conducted through social networking media. They are mutually supportive, being used in concert with physical actions (Nissen 2015: 72).

In particular, intelligence gathering is focused on searching, storage and analysis of information from social media networks and profiles, including content and conversations. There are several approaches to analyzing social media for intelligence collection (e.g. trend, network, sentiment, geo-, content, behavioral, systemic, and information analysis). All of these forms of analysis can contribute to target audience analysis and support psychological warfare or the selection of targets for operations both on- and offline.

Targeting implies the use of social media to identify potential targets for military actions in the physical domain (based on geo-tagged pictures or on-going conversations in social media), as well as to attack social media accounts by hacking or defacing them.

Psychologic influence refers to the dissemination of information to influence a target audience's values, belief system, perceptions, emotions, motivation, reasoning, and behavior. The use of social media in this case would seek to achieve certain military effects in the cognitive domain – shape, inform, influence, manipulate, expose, diminish, promote, deceive, coerce, deter, mobilize, convince (Nissen 2015: 63). The methods of influence used on social media can be overt, such as the creation of official accounts, channels, websites, comments by opinion leaders etc., or covert, such as fake identities, botnets, and trolling. They can be used in any combination for information operations on social media.

Cyber Operations – targeting social media platforms and accounts to breach password-protected spaces, alter the content of a profile, or render a website completely unusable. Cyber operations can be offensive or defensive, however most social media cyber-ops are offensive in nature. They can include attacks on websites, the breaching (hacking) of password protected chat sites, e-mails or cell-phones, with the purpose of later exposing the content; intrusion on news agencies' cable news and altering news stories; or altering content and imagery on, e.g., a Facebook profile, etc.; or stealing identity information like usernames and passwords. It can also be intrusion into, e.g., databases in order to, undetected, extract information for intelligence purposes, also known as "computer network exploitation".

Defense provides the protection of social media platforms, sites, profiles and accounts at the technical or system level. Defensive activities can include the use of encryption, anti-tracking, and/or IP-concealing software in connection with social network media (Svetoka. 2015: 14–17).

Management and control are carried out by using social media for internal communication, information sharing, coordination, and synchronization of actions. The use of social media for Command and Control

purposes is important for non-state actors such as insurgent groups, particularly if these groups lack formal structure or are dispersed over large geographical areas; social media can provide a means of communication and a way to coordinate their activities. However, the use of social media exposes the activities of insurgent groups to intelligence services.

Being combined, the above listed methods comprehensively impact on society, reducing its ability to resist and defend. Without effective counteraction, such information activities can cause catastrophic consequences. In the light of this, the targeted state is compelled to set various informational restrictions (Nissen 2015: 62–66, 90–94).

Under conditions of hybrid warfare, the limitation of informational rights and freedoms is unavoidable. It is vitally important for the survival of the country and the nation. Informational restrictions are desperately needed to protect the state from the flaw of sensitive data, to ensure functioning of electronic systems and, of course, to protect society from disinformation and enemy propaganda. For this purposes, strict informational restrictions can be imposed on any media which is used as an information weapon of hybrid warfare. And this is an objective necessity.

However, this necessity raises a number of very difficult questions. For example: "At what principles information restrictions should be applied?", "On the principle of jurisdictional belonging to country-aggressor or on the principle of informational harm?", "By which criteria such harm should be identified?", "Is it fair to block social networks and searching systems?" and so on.

2. Ukrainian information policy under conditions of hybrid war

Ukraine has been trying to find answers since 2014. The history of this search can be divided into three stages:

Stage I (2014–2015) – the stage of political "shock" – characterized by total unpreparedness for the informational invasion. National legislation did not provide grounds and criteria for information restrictions. As a result, for a long time, the subversive activity of Russian media met with no resistance. National and local providers continued to broadcast propagandistic channels of Russia. Russian-controlled print media and internet resources freely disseminated anti-Ukrainian materials to justify aggression, annexation of territories and separatist activities. At this stage, freedom of speech and the right to information were practically unlimited, but national security interests were defenseless against information aggression.

Stage II (2015–2017) – the stage of legislative conceptualization. At this stage, the Ukrainian state recovered from the "informational tsunami" launched by Russia, and finally began to develop the legal foundation for information resistance. Special laws were adopted, setting the grounds for prohibition of anti-Ukrainian information products. Additionally, the criteria for recognizing media activities as hostile and harmful to national interests were defined.

In particular, all information activities were restricted, intended to promote or spread the propaganda of aggressor-state, its authorities and representatives, as well as their actions; or creating a positive image of the aggressor, justifying or recognizing the occupation of Ukrainian territory *(Law of Ukraine dated 05.02.2015 № 159-VIII "On amendments to certain laws of Ukraine on the protection of the information television and radio space of Ukraine", Law of Ukraine dated 08.12.2016 № 1780-VIII "On amendments to some laws of Ukraine restricting access to the Ukrainian market of foreign printed materials with anti-Ukrainian content").*

Stage III (2017-present time) – the stage of propagating restrictions (and, accordingly, the curtailment of information rights and freedoms). From the spring of 2017, information restrictions in Ukraine have become tighter and tighter. Prohibitions on Russian media are made not only due to their "hostility", but also – due to their residence. Many of them are prohibited not because they are unfriendly, but because they are Russian

3. Informational rights on the slaughter of security

As a result, the issue of "collision" between interests of national security and guarantees of democratic rights and freedoms (including freedom of information activity) has been rasied.

An exemplary example is the Decree of the President of Ukraine dated May 15, 2017 № 133/2017 "On the ... Application of Personal Special Economic and Other Restrictive Measures (Sanctions)", which introduced a blockade of many popular Russian Internet services (Kaspersky Lab, Doctor Web, Yandex, Mail.Ru, Vkontakte). This document provoked a sharp polemic both in Ukraine and at an international level (Decree of May 15, 2017 № 133/2017).

The supporters of such restrictions insist that listed Internet services occupy a dominant place in Ukrainian information market and are simultaneously under the tight control of Russian special services, which can use them for destabilization of the political, social and

economic situation, collecting confidential data, unfair competition and other hostile purposes. At the international level, blocking of Russian websites was supported by NATO Secretary General Jens Stoltenberg, who considers it "... a matter of security, but not a freedom of speech" (Stoltenberg 2017).

At the same time, there are numerous voices "against" such activity. Many public figures and organizations are convinced that such restrictions have no factual basis (in essence, they are aimed against purely hypothetical threats), have no legal justification, are contrary to the Constitution, and violate democratic rights and freedoms. For example, the chairman of the Verkhovna Rada Committee, Viktoria Syumar, noted that the decision about blocking Russian social networks is out of the legal framework. International organization Reporters Without Borders considers this step as a „non-symmetric measure that significantly restricts the right to information and freedom of thought (Syumar 2017, RSF, 2017).

Without attempting to arbitrate where freedom of speech ends and national security begins, we are deeply convinced that in any case informational restrictions should be individual and should concern only those media that made concrete hostile actions or are obviously dangerous to the state and society.

It seems unreasonable and unlawful to apply sanctions on the principle of state affiliation, when all information services without exception are blocking, regardless of their activity, content or thematic direction (Gurzhii 2017). In this sense, Ukrainian experience is very instructive. Of the hundreds (105) of Internet resources blocked in accordance with the Decree of the President of Ukraine dated May 15, 2017. 133/2017 "On the ... application of personal special economic and other restrictive measures (sanctions)", more than a quarter (27%) – have reference, entertaining or everyday character and are unlikely to be an effective weapon of hybrid warfare. Among them are the sites: "www.kinopoisk.ru", "www.auto.ru", "www.translate.yandex.ua" and others. Their prohibition cannot be justified by security interests, and even more – it is seemed to be unacceptable limitation of information rights and freedoms.

Conclusion

Summarizing above, we can state the following. Under conditions of hybrid warfare, the targeted state faces a wide range of information threats, neutralization of which, on the one hand, requires the application of extraordinary restrictive measures, and, on the other hand, may be

accompanied by substantial limiting of democratic rights and freedoms. The search for a balance between the interests of national security and the ideas of the rule of law is a strategically important task of the state.

This task can be solved only if the principles, criteria and mechanisms of information restrictions are clearly defined in legislation. The starting point for such restrictions should be the Constitution and fundamental acts on information rights and national security. Limiting of information rights and freedoms should have a personal character. It should applied according to the criteria of hostility, not to state affiliation of media. And, of course, it should not bring into the question the democratic choice of society.

Then and only then will the informational policy of the state be provided in legal frames, and only then, even in the most difficult times, will it be able to guard democratic values, without betraying them.

References

Дешко Л, Бондарєва К. 2018, Кібербезпека в Україні: національна стратегія та міжнародне співробітництво, "Порівняльно-аналітичне право", 2.

Arden M. 2015, Human Rights and European Law: Building New Legal Orders. Oxford: Oxford Univ. Press. DOI: 10.1093/acprof:oso/9780198728573.001.0001

Dearden Lizzy, Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers. The Independent http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-co mpany-airport-rozenko-pavlo-cabinet-a7810471.html (1.06.2017).

Golder B., Williams G. 2006, Balancing national security and human rights: Assessing the legal response of common law nations to the threat of terrorism, "Journal of Comparative Policy Analysis", 8(1). DOI: https://doi.org/10.1080/13876980500513335

Gurzhii T., Gurzhii A., Seliukov V. 2018, Public administration of personal data protection in modern Ukraine, "Politické Vedy", 2.

Gurzhii A. 2017, The Decision-Making Process in Administrative Cases. "Rocznik Administracji Publicznej", 3.

Gurzhii A. 2018, The system of public administration in the field of personal data protection. In: Development of National Law in the Context of Integration Into the European Legal Space, Warsaw : BMT Eridia Sp. z o.o. Wydawnictwo Erida.

Decree № 133/2017 of the President of Ukraine of 15.05.2017 № 133/2017 "On the decision of the Council of National Security and Defense of Ukraine dated April 28, 2017 "On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions)"„. Official web portal of Verkhovna Rada of Ukraine http://zakon3.rada.gov.ua/laws/show/133/2017 [in Ukrainian].

Dolmatova M., Russian mass media: falling incomes of Russians and paradoxical optimism. BBC Russian Service http://www.bbc.com/russian/features-38566253 (10.01. 2017).

Huggler J., Germany accuses Russia of cyber attack on Ukraine peace monitors, as Kremlin dismisses US intelligence claims as a "witch hunt". The Telegraph

http://www.telegraph.co.uk/news/2017/01/09/germany-accuses-russia-cyber-attack-ukraine-peace-monitors-kremlin/ (9.01.2017).

Law of Ukraine from 05.02.2015 № 159-VIII "On Making Amendments to Some Laws of Ukraine on the Protection of the Information Television and Radio Broadcasting of Ukraine". Parliament of Ukraine (February 2015). Official web portal of Verkhovna Rada of Ukraine http://zakon3.rada.gov.ua/laws/show/159-19 [in Ukrainian].

Law of Ukraine of 08.12.2016 № 1780-VIII "On Making Amendments to Some Laws of Ukraine Concerning Restriction of Anti-Ukrainian Content to the Ukrainian Market for Foreign Printed Products. Parliament of Ukraine". Official web portal of Verkhovna Rada of Ukraine http://zakon2.rada.gov.ua/laws/show/1780-19 [in Ukrainian].

Nissen T. 2015, The Weaponisation of Social Media. Characteristic of Contemporary Conflicts. Copenhagen: Royal Danish Defense College.

Pranevičienė B. 2011, Limiting of the Right to Privacy in the Context of Protection of National Security, "Jurisprudencija", 2011.Wesley Pue W. 2003, The War on Terror: Constitutional Governance in a Stateof Permanent Warfare?, "Osgoode Hall Law Journal", 41.

RSF urges Ukraine to scrap ban on Russian social media sites. Reporters Without Borders https://rsf.org/en/news/rsf-urges-ukraine-scrap-ban-russian-social-media-sites (23.05.2017).

Sanger David, Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says. The New Yourk Times https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html (6.01.2017).

Syumar V. Inetrwiev by The head of the Committee on Freedom of Speech and Information Policy. Information agency ZIK http://zik.ua/tv/video/83547 (May 2017) [in Ukrainian].

Stoltenberg J. Press conference by NATO Secretary General Jens Stoltenberg ahead of the Meeting of NATO Heads of State and Government. Official site of NATO http://www.nato.int/cps/en/natohq/opinions_144081.htm?selectedLocale=en (May 2017).

Svetoka S. 2016, Social media as a tool of hybrid warfare, Riga: NATO Strategic Communications Centre of Excellence.

Data przekazania tekstu: 23.01.2019 r.; data zaakceptowania tekstu: 4.04.2019 r.