UDC 004:351.751.5]:342.5(477)

THE IMPACT OF CENSORING AND FILTERING PRACTICES IN THE UKRAINIAN INTERNET ON UKRAINE'S INTERNATIONAL IMAGE IN CONTEXT OF RUSSIAN MILITARY AGGRESSION

Pervushyn M. M.,
Post-graduate
Vasyl Stus' Donetsk National University

The article presents an attempt to analyze the way international human rights organizations perceive attempts by the Ukrainian government and pseudo-state entities in the occupied territories of the eastern Ukraine to apply mechanisms for censoring and blocking information in the Ukrainian segment of the Internet in the context of an armed conflict between Ukraine and the Russian Federation. The author determines the degree of influence of restrictive measures in cyberspace on the international image of Ukraine and provides practical recommendations for the improvement of such an image.

У статті представлена спроба проаналізувати сприйняття міжнародними правозахисними організаціями спроб уряду України та псевдо-державних утворень на окупованих територіях сходу України застосувати механізми цензурування та блокування інформації в українському сегменті Інтернету в контексті збройного конфлікту між Україною та Російською Федерацією. Автор визначає ступінь впливу обмежувальних заходів в кібер-просторі на міжнародний імідж України та надає практичні рекомендації щодо покращення такого іміджу.

В статье представлена попытка проанализировать восприятие международными правозащитными организациями попыток правительства Украины и псевдо-государственных образований на оккупированных территориях востока Украины применить механизмы цензуры и блокировки информации в украинском сегменте Интернета в контексте вооруженного конфликта между Украиной и Российской Федерацией. Автор определяет степень влияния ограничительных мер в кибер-пространстве на международный имидж Украины и формулирует практические рекомендации по улучшению такого имиджа.

Key words: Internet censorship, informational warfare, Russian-Ukrainian conflict, freedom of expression in the Internet, cyber-security.

Formulation of the problem. The ongoing Russian intervention in Ukraine is widely perceived within Ukrainian scientific community as one of the most prominent modern examples of asymmetrical conflict (See [1], [2, p. 13], [3, p. 11]) because of general disproportion of military power and available resources between the sides of conflict as well as due to the nature of involved actors, such as paramilitary formations, private military corporations and quasi-state structures. The most frequently used means of warfare are also typical for asymmetrical conflict and include terrorist attacks, diversions, disinformation campaigns etc.

There is, however, another kind of asymmetry, which manifests itself most prominently in light of European aspirations of Ukraine. Despite the war, the process of Ukraine's eurointegration continues and puts the country under tight scrutiny of Western think tanks, NGO's and international organizations, concerned with the state of Ukrainian civil society, democratic institutions and support of human rights, especially in the conflict zone. This leads to the situation, where Ukraine has to abide by the international and humanitarian law, while Russia and it's proxies in the conflict zone feel free to disregard the rules, established by international community, whenever they see fit. So far Western monitoring structures showed little leniency and readiness to take into account the realities of military conflict, as can be illustrated, for example, by recent demand of Human Rights Watch, which called for Ukraine to sign the Safe School Declaration [4]. The statement implied that signing of the declaration itself should help to reduce the number of casualties among schoolchildren in the conflict zone, even though it is clear that any declaration can have tangible impact only if all sides of the conflict have agreed to follow its provisions.

Such supervision extends itself beyond physical reality, as restrictive measures applied to Ukrainian cyberspace by Ukrainian authorities and unrecognized "governments" of the occupied territories are also scrutinized by relevant Western institutions, in view of their impact on freedom of speech and accessibility of information for the citizens of Ukraine. Taking into account sheer quantity of censoring and filtering prac-

ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 4 (40) 2018

47

tices that are either proposed or already applied in the UAnet in the last four years, ostensibly with an aim of upholding the national security interests, it is important to analyze the impact that such restrictive measures make on the international image of Ukraine.

Literature overview. The main sources of information in the context of this research were reports on Internet Freedom by Western NGO's, such as Freedom House [5] and Whoishostingthis [6]. These and similar reports were also, to some extent, used as objects of analysis, for their perspective reflects general attitude of international community towards the situation in Ukrainian cyber-space. This research takes into account M. Rundle and M. Birdling article that expanded upon the issue of correlation between Internet censorship and international law [7]. Some publications on the informational aspect of Russian-Ukrainian conflict also proved to be useful, such as works authored by G. Pocheptsov [1], I. Bondarenko [2] and T. Andriyevskyy [3]. Finally, some attention to the issue of internet censorship in Ukraine was paid in publications of T. Muzhanova [8] and T. Lokot [9]. However, the topic of restrictions in Ukrainian cyber-space in times of an armed conflict has yet to become a subject of thorough investigation. The absence of publications by English-speaking authors on the subject of informational warfare in the Russian-Ukrainian conflict is also evident.

From methodological standpoint the research is based on conceptual findings of Copenhagen School, in particular a theory of securitization, as defined by Ole Wæver and Barry Buzan [10, c. 25]. The theory of securitization focuses on the process of transformation of an object or phenomenon, which previously wasn't a part of security discourse, but is now being transformed into a matter of national security by a state, facing a real, potential or perceived emergency or threat. In our opinion, current restrictive practices, introduced into Ukrainian cyberspace by states and quasi-state formations, constitute a part of a worldwide phenomenon of securitization and militarization of the Internet, which was originally perceived as, first of all, a medium for communication, and not a security threat. Within the frames of securitization paradigm the author applies a number of methods for data collection and analysis, such as documentary analysis, keywords analysis, event-analysis and case studies, aiming to construct a comprehensive picture of correlation between Ukraine's image and restrictive practices in UAnet on the basis of thorough analysis of the most distinctive cases and relevant legislation.

Thus, the **purpose of the article** is to analyze the way Western Internet freedom watchdogs and international organizations perceive the attempts of Ukrainian authorities to limit the flow of information in the UAnet, as well as similar attempts made by Russian authorities and their proxies in the conflict zone in Ukraine.

Basic material presentation. To be clear, international law leaves some space for imposing certain limitations on freedom of speech. In principle, the ICCPR necessity test should be applied, to determine whether Internet censorship and filtering practices are admissible in a given situation. This test consists of two basic provisions: first of all, the imposed restrictions should be narrow enough to avoid overreaching. Secondly, the state should provide a sufficient explanation for its limitations on freedom of expression in the cyber-space [7, p. 81]. In some cases the national security concerns could indeed serve as a sufficient basis for blocking and filtering of Internet resources. The second provision of necessity test also implies that any restrictive law should be carefully and clearly worded to avoid the possibility of double interpretation. The author hopes to make it clear later on, that most of the regulations introduced by either side of the Russian-Ukrainian conflict are far too extensive and overreaching to pass the abovementioned necessity test.

Moreover, decline of freedom in Ukrainian cyber-space is caused to great extent not only by activity of state organs, but also by similar oppressive measures, introduced by quasi state formations and occupational administration. Indeed, the lists of Ukrainian sites, which are perceived to be dangerous for DPR and LPR and are thus eligible for blocking, have been comprised as early as in 2014 and continue to expand [11]. Activity of separatists also frequently leads to disruptions in connectivity, pressure on providers of Internet services, unlawful prosecutions and detentions of pro-Ukrainian bloggers and reporters [12]. At the same time oppressive measures applied by Crimean occupational authorities towards Ukrainian web-sites often exceed in their severity even those introduced by the infamous Roskomnadzor itself [13]. In context of this research the most important implications of such restrictions are the following:

– First of all, in their desire to restrict access of users to ideologically incorrect material the de-facto rulers of occupied territories don't limit themselves just to the blocking of Ukrainian web-sites, as some of the prominent Western media outlets, such as Radio Free Europe\Radio Liberty, have also been blocked on the territories of self-proclaimed republics [9].

– Secondly, from legal point of view the occupied parts of Donetsk and Luhansk oblasts, as well as Crimea, remain within the jurisdiction of Ukraine. Among other things, this means that while international watchdogs, such as Freedom House, recognize disruptive activity of occupational authorities, their steps towards restriction of freedom of speech online contribute into the decline of Ukraine's own Internet freedom ratings and thus to some extent tarnishes Ukraine's international image.

The most worrying trend is the relatively recent inclination of Ukrainian authorities to copy approaches of their adversaries when it comes to restriction of Internet freedom. While the first attempt to create Ukraine's own blocking list of pro-Russian sites in 2014 had no sufficient legal grounds to support it and

ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 4 (40) 2018

48

was easily repealed thanks to the vocal opposition of Ukrainian activists and international NGO's [13], subsequent measures proved to be more pervasive.

Of all the provisions, included in the text of Presidential Decree № 133/2017, which confirmed the introduction of the new sanction package against the Russian Federation, it was the blocking of four leading Russian Internet-corporation that provoked the most heated discussion within Ukrainian civil community. The abovementioned decree also served as a wake-up call for Western watchdogs. Not only it prompted Freedom House to register "a crackdown" on social media in Ukraine [15, p. 912], but also led to unfavorable statements from several international organizations, such as OSCE [15], Council of Europe [16], and Human Rights Watch [18]. All the above mentioned organizations unanimously called for reversion of the ban.

It is worth to note, however, that despite Western rejection the Decree № 133/2017 actually represented an attempt of Ukrainian authorities to imply relatively rational and balanced approach to the issue of censoring of Russian and pro-Russian web-sites. Despite initial mixed reaction within Ukrainian society it was clear, that Russian Internet-giants sooner or later should be targeted by Ukrainian sanctions alongside with their offline counterparts. In general, the experts noted that while there were some doubts concerning the possibility of full-scale implementation of the Decree, it was first and foremost directed at causing economical damage to the leading corporations of Runet, instead of simply blocking access for Ukrainian users in style of Roskomnadzor. Moreover, efforts of civil society to repeal the Decree were partly successful, as decisions of Ukrainian courts confirmed the right of users to access the banned sites through VPN or anonymizer services [19]. This led to emergence of a fairly unique situation, whereupon the Decree carried out its main task of putting economical pressure on Russian enterprises, without any significant breach of Ukrainian Internet users' rights. All in all, this was the first censoring effort, actually backed by more or less solid legal document, which could provide basis for further law-making activity on informational security matters.

However, the very next Presidential Decree № 127/2018 on informational security, which was perceived as "second wave" of blockings by Ukrainian activists [19] signified the return to previously adopted chaotic and overzealous approach to content regulation, while also mirroring the typical Russian practice of comprising extensive lists of prohibited sites. The main point of concern for international watchdogs in relation to this Decree was its inability to finally establish at least a semblance of actual legal basis for restrictions in the Ukrnet [5]. Neither Ukrainian security service nor the Ministry of information policy of Ukraine, on whose recommendations the final list of 192 sites to be blocked in Ukraine was comprised, possess the right to block any resource in the Internet [20]. Thus, any attempt to actually enforce the Decree would lead to severe breach of several Ukrainian laws [20]. To sum up, while presidential Decrees represent a significant upgrade in comparison with early attempts to block Russian influence in the Ukrnet, when proposed restrictions were based solely on a letter of one of the Ukrainian security service departments to the head of Internet Association of Ukraine [21], they still leave a lot to be desired.

It is worth to note, however, that apart from the negative trends international organizations are able to perceive some positive developments related to freedom of speech in Ukrainian web-sphere. For example, in comparison to Freedom house's 2017 report, the latest edition of Freedom on the Net survey pays closer attention to the efforts of Ukrainian activists to repeal the would-be restrictive laws on their draft stage or mitigate their impact after such laws have already been enforced. As was illustrated above, sometimes those efforts prove to be successful. Indeed, civil society of Ukraine remains vigilant and perceptive towards any effort to impose some limitations on spreading of the information in the Internet (see for example [22]).

Freedom House also praises general vibrancy and diversity of Ukrainians' activity on social platforms, as well as growing use of social media by Ukrainian officials [15, p. 910-911]. At the same time, organization expresses concern because of frequent manifestations of negative attitude towards ethnic minorities or members of LGBTI-community in Ukrainian cyber-space [15, p. 915]. It is clear that ongoing military conflict could play its part in provoking such outbreaks of xenophobia.

It should also be noted that not all international watchdogs share critical stance of Freedom House towards Ukrainian authorities' approach to informational security matters. For example, the research by WhoIsHostingThis placed Ukraine in the "white zone" [5], which means that the country is free from Internet censorship and filtering practices. This, however, signifies not difference of attitude, but rather difference of applied methods of research. It is clear that WhoIsHostingThis' research was limited to checking the availability of certain sites on the spot. Failure of this organization to detect significant degree of censoring in the Ukrainian cyber-space means that countless efforts of both Ukrainian and separatists' authorities to regulate the flow of information online have so far proved to be ineffective. At the same time, Freedom House's more grounded and methodical approach takes into account not only visible effects of censoring attempts, but a number of other important factors, such as extra-legal pressure, self-censorship, and potential threat from legislative provisions that have yet to be fully enforced. Such an approach allows constructing of more or less complex and realistic picture, even though Freedom House, as well as most of the others Internet and press freedom watchdogs, often fails to take into account existing pressure on Ukrainian authorities and ordinary citizens, created by ongoing Russian military intervention.

ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 4 (40) 2018

49

Conclusions. It's clear that while some Internet and press freedom watchdogs, such as Freedom House and Reporters Without Borders, try to present a relatively complex and multidimensional view on Internet censorship practices of Ukrainian authorities, other organizations limit themselves to pointless demands. Still, however harsh and judgmental those statements may seem, if Ukraine is to continue its course towards Euro-integration, Ukrainian authorities must do their best to take the recommendations of international community into account and secure their implementation at least to some extent.

To do this, in our opinion, Ukrainian authorities should abandon the «tit for tat» approach and refrain from further engagement into fruitless competition with the Russian authorities and Russian proxies on the occupied territories on "Whose list of blocked sites is bigger?" basis. Overall, Ukrainian government should transform its reactive approach into proactive measures. Extending the cooperation with Western powers on the country's cyber-security and preventing another "NotPetya" attack is far more important than blocking the access to some Russian news portal. It would be wise to limit the actual blocking initiatives to a handful of most prominent Russian Internet-corporations and some of the most infamous Russian pro-paganda outlets, such as Russia Today. Beyond that, the government should delegate the task of putting pressure on Russian and pro-Russian resources to independent Ukrainian hacktivists, whose methods proved to be far more effective than any possible restrictions, imposed by the state organs, whose measures are bound to be either ineffective or expensive.

One of the most important trends is the ability of international watchdogs to recognize and appreciate the attempts of Ukrainian activists to oppose the state-initiated restrictions of freedom of speech in the Internet. Such opposition becomes more and more effective with time. However, the efforts of Ukrainian civil society are more likely to succeed when a restrictive law is only on its draft stage. With that in mind, activists should concentrate their efforts on increasing their participation in discussion of the drafts and projects of the laws.

Finally, as far as international community is concerned, the Crimea and occupied territories on the East of the country are still recognized as parts of Ukraine. Taking this into account, any oppressive measure imposed by self-proclaimed authorities will undoubtedly affect Ukraine's place in the relevant ratings and it's international image overall. With this in mind Ukraine's government should increase its efforts of countering Russian propaganda and raising awareness of inhabitants of the occupied territories concerning possible methods of de-blocking of Ukrainian Internet resources. In other words, the emphasis should be put on promotion of Ukrainian channels of information, instead of restricting access to the Russian ones. In such a way Ukraine should be able to mitigate the negative impact that Russian subversive and restrictive tactics in the cyber space make on the country's international image.

References:
1. Почепцов Г.М. Гібридна війна: інформаційна складова [електронний ресурс]: Детектор Медіа: електрон. аналітичний проект. Дата оновлення: 25.10.2015. URL: https://ms.detector.media/trends/1411978127/gibridna_viyna_informatsiyna_skladova/ (дата звернення: 08.11.2018).
2. Бондаренко І.С. Соціальнокомунікаційні техніки та ресурси у війнах нового покоління. Держава та Регіони. Серія: Соціальні комунікації. 2016. № 3 (27). с. 13–17.
3. Андрієвський Т.Г. Концептуалізація поняття гібридної війни: політологічний вимір. Сучасне суспільство. 2017. Випуск 1 (13). С. 4–15.
4. Raqib S. An opportunity for Ukraine to endorse the Safe Schools Declaration // Human Rights Watch. Дата оновлення: 19.08.2018. URL: https://www.hrw.org/news/2018/06/19/opportunity-ukraine-endorse-safe-schools-declaration (дата звернення: 08.11.2018)
5. Freedom on the Net 2018: Ukraine country report // Freedom House. URL: https://freedomhouse.org/report/freedom-net/2018/ukraine (дата звернення: 08.11.2018).
6. Which Countries Censor the Internet Today? // WhoIsHostingThis. Дата оновлення: 27.02.2017. URL: https://www.whoishostingthis.com/blog/2017/02/27/internet-censorship/ (дата звернення: 08.11.2018).
7. Rundle M., Birdling M. Filtering and the International System: A Question of Commitment [in:] R. Deibert, R. Rohozinski (eds.), Access denied: the practice and policy of global internet filtering, Cambridge: The MIT Press 2008, p. 73-102.
8. Мужанова Т.М. Інтернет-цензура як загроза правам громадян у сфері інформаційної безпеки. Сучасний захист інформації. 2015. № 2. с. 84–88.
9. Lokot T. Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republi' Global Voices. Дата оновлення: 14.01.2016. URL: https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/ (дата звернення: 08.11.2018).
10. Buzan B., Wæver O. Security: A New Framework for analysis, Lynne Rienner Publishers, Boulder, Colorado, 1998. 239 p.

ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 4 (40) 2018

50

11. В «ДНР» ввели цензуру в Интернете // Zn.ua. Дата оновлення: 30.05.2015. URL: https://zn.ua/UKRAINE/v-dnr-vveli-cenzuru-v-internete-177876_.html (дата звернення: 08.11.2018)

12. У Луганську сепаратисти викрали журналіста і пограбували офіс інтернет-сайту. Радіо Свобода. Дата оновлення: 16.07.2014. URL: https://www.radiosvoboda.org/a/25459340.html (дата звернення: 08.11.2018).

13. Eight more mass media to be blocked in Crimea that are absent on lists of Roskomnadzor // QHA Crimean News Agency. Дата оновлення: 18.09.2018. URL: http://qha.com.ua/en/society/eight-more-mass-media-to-be-blocked-in-crimea-that-are-absent-on-lists-of-roskomnadzor/143975/ (дата звернення: 08.11.2018).

14. Ukrainian parliament approves very dangerous draft law on first reading // Reporters Without Borders. Дата оновлення: 20.01.2016. URL: https://rsf.org/en/news/ukrainian-parliament-approves-very-dangerous-draft-law-first-reading (дата звернення: 08.11.2018).

15. Freedom on the Net 2017. Manipulating social media to undermine democracy. Freedom House, 2017. P. 902–916.

16. Talant B. OSCE issues rebuke to Ukraine over draft internet censorship law // Kyiv Post. Дата оновлення: 07.07.2018. URL: https://www.kyivpost.com/ukraine-politics/osce-issues-rebuke-to-ukraine-over-draft-internet-censorship-law.html (дата звернення: 08.11.2018).

17. Arbitrary Internet blocking jeopardizes freedom of expression // Council of Europe. Дата оновлення: 26.09.2017. URL: https://www.coe.int/en/web/commissioner/-/arbitrary-internet-blocking-jeopardises-freedom-of-expression?desktop=true (дата звернення: 08.11.2018).

18. Ukraine: Revoke Ban on Dozens of Russian Web Companies // Human Rights Watch. Дата оновлення: 16.05.2017. URL: https://www.hrw.org/news/2017/05/16/ukraine-revoke-ban-dozens-russian-web-companies (дата звернення: 08.11.2018).

19. Новий перелік заборонених сайтів. Мотиви й наслідки коментує медіа-юрист. Громадське радіо. Дата оновлення: 29.05.2018. URL: https://hromadske.radio/podcasts/kyiv-donbas/novyy-perelik-zaboronenyh-saytiv-motyvy-y-naslidky-komentuye-media-yuryst (дата звернення: 08.11.2018).

20. ІнАУ вимагає відмінити рішення МІП про формування і передачу в СБУ переліку сайтів для блокування. Інтернет Асоціація України. Дата оновлення: 21.06.2017. URL: https://inau.ua/news/inau-vymagaye-vidminyty-rishennya-mip-pro-formuvannya-i-peredachu-v-sbu-pereliku-saytiv-dlya (дата звернення: 08.11.2018).

21. Лист Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки голові Інтернет асоціації України Поповій Т. В. від 18.07.2014. URL: http://ru.scribd.com/doc/235847891 (дата звернення: 08.11.2018).

22. Громадські організації заявляють про неприпустимість встановлення технічних засобів стеження у інтернет-провайдерів. Інтернет Свобода. Дата оновлення: 27.02.2018. URL: https://netfreedom.org.ua/gromadski-organizatsii-zajavliayut-pro-neprypustymist-vstanovlennia/ (дата звернення: 08.11.2018).

ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 4 (40) 2018

51