YouTube is not yet regulated by Ukrainian law: Internet regulation in the proposed draft law of

Ukraine on the media

Svitlana Jaroszynski

Florida State University

Abstract

The paper examines how Ukraine's current bill on the media approaches the regulation of foreign-owned content sharing platforms in view of the country's national security interests. A balance between national security interests and freedom of expression is an important issue for Ukraine that has to protect itself against the Russian aggression and abide by principles of a democratic society it is building. Securitization of cyberspace regulation is becoming a standard justification of public policymaking. The paper explores how threats to national security are defined in the current Ukrainian legislation, and how they are addressed in the proposed regulation of online platforms. As the analysis of the Ukrainian bill demonstrates, national security can be used as a ground for restrictive regulations and hinder freedom of expression.

YouTube is not yet regulated by Ukrainian law: Internet regulation in the proposed draft law of

Ukraine on the media

At the beginning of May 2020, a well-known Ukrainian journalist, Dmytro Gordon, posted a YouTube video on his website. In the video, he interviews Natalia Poklonskaya, exprosecutor in the Crimea who, after its annexation in 2014, sided with Russia and eventually became a deputy of the Russian State Duma (Parliament). The interview caused a storm in the Ukrainian media and social networks. The major controversy was about whether Gordon was promoting a traitor or helping to expose her crimes. One of the comments deserves particular attention because of its connection with the Internet regulation. A member of the Journalist Ethics Committee observed that what happens on YouTube was not yet regulated by the Ukrainian legislation but was however a part of the proposed draft law on the media (Ekspert, 2020). This comment may lead one to believe that a new law on the media, if adopted, would not allow for such interview to become public, a troubling implication from the perspective of freedom of speech and expression.

The original draft law on the media was registered with the Parliament of Ukraine

Verkhovna Rada (VR) in December 2019. The future law was intended to replace a number of separate statutes on different types of legacy media and add online resources to the scope of regulation. The bill has been discussed by the public, media representatives, and international organizations, such as the Organization for Security and Co-operation in Europe (OSCE). One of the disputed provisions of the bill is related to the regulation of Internet resources, in particular "content sharing platform providers" that include Facebook, YouTube, Instagram, and others.

Statements made by government officials as well as certain provisions of the bill suggest that these providers may be asked to register in Ukraine and held liable for the content posted on their

platforms. These arrangements, according to the officials, are justified by the on-going Russian aggression against Ukraine and a massive disinformation and propaganda campaign carried out through online resources. Introducing the government's plans to develop a comprehensive media regulation, Minister of Information Policies Volodymyr Borodianskyi assured that legitimizing concepts of "'harmful information,' disinformation,' 'unreliable information'... is very important in the conditions of information war with RF1" (Borodians'kyi, 2020, para. 3). Thus, the interests of national security are used to establish restrictions on the content disseminated through online platforms. The above interview with Natalia Poklonskaya may just fall under these restrictions. After several modifications, a revised bill was approved by the VR in the first reading in July and is currently under further development.

In this paper, I analyze how Ukraine's current bill on the media approaches the regulation of foreign-owned content sharing platforms in view of the country's national security interests. A balance between national security interests and freedom of expression is an important issue for Ukraine that has to protect itself against the Russian aggression and abide by principles of a democratic society it is building. Wigell (2019) admits that hybrid warfare, which includes disinformation spread through online platforms, are especially dangerous for liberal democracies, because liberal democratic values are perceived as "vulnerabilities that can be exploited to drive wedges through democratic societies and undermine governability" (p. 256). Most studies in online content regulation refer to countries that are not involved in an active armed conflict. The analysis of Ukraine's efforts in Internet regulation will complement the existing research by examining a country with an active armed conflict presenting immediate security threats to the state.

¹ Russian Federation

I start with a review of academic literature pertaining to the regulation of online platforms, including definition of online platforms, justification of online content regulation, securitization of Internet regulation, and current approaches to online platforms regulation. A brief history of the proposed legislation is followed by the analysis of its regulatory provisions on online platforms rationalized by national security interests. The paper finishes with a discussion of the proposed regulation and some alternatives to the currently proposed policies.

Literature review

Concepts and definitions

Online platforms that host content generated by users come under different names in academic literature, legislation, and popular use, including "social media services" and "video sharing platforms" (EU Directive 2018/1808, Directive 2010/13/EU), "social media platforms" (Marsdren et al., 2019; Rochenfort, 2020), or "content sharing platforms" (OSCE Legal Analysis, 2020). Rochefort (2020) posits that the term "platforms" is customarily applied "in broad fashion to social media sites like Instagram and YouTube, multifaceted technology companies like Amazon which provide e-commerce and cloud computing services, transportation networks like Uber, and even the housing marketplace Airbnb" (p. 227). However, in a narrower sense, they refer to companies "like Facebook, Twitter and YouTube, that provide Internet-based communication tools affording users the capability to create profiles, connect with other individuals, and build and navigate their list of connections within a bounded network" (p. 228). Transnational online platforms present a particular challenge for regulators because of their association with cyberspace (Diebert & Rohozinsky, 2010; Ünal, 2015).

Ünal (2015) argues that the term "cyberspace" is more inclusive than the Internet, because it implies "a global network of computer processing systems, interdependent

information technology infrastructures and telecommunications networks in which online communication takes place" (p. 175). The term embraces a complex nature of the online space that has physical and informational components to it. Going beyond the boundaries of the Internet is important for the discussion of content sharing platform regulation because ownership and location of the platform providers define regulatory means chosen by the state. If a provider does not fall under the jurisdiction of a regulating state, the state cannot enforce its policies directly as was the case of the U.S. Congress hearing of the top management of social media giants in 2018 (Fiegerman, 2018) or 2020 (Allyn et al., 2020).

Diebert and Rohozinsky (2010) outline four characteristics of cyberspace that makes it challenging and elusive for regulation. First, as a communication network, it has a transnational organization outside of the institutions of the state. No single state or individual can be in control of cyberspace, even if they own or operate its element. Second, cyberspace is a combination of private and public networks. As a result, it is governed by different principles and policies from copyright to cyber-crime. Third, unlike other environments in which humans operate, like water or air, "cyberspace is a human-made domain in constant flux based on the ingenuity and participation of users themselves" (p. 16). Cyberspace provides its end users with generative capacities which results in its constant innovation but also in unforeseen security risks. Finally, "cyberspace is comprised of both a material and a virtual realm – a space of things and ideas, structure and content" (p. 16, emphasis in original). This feature makes complete exclusion of content in cyberspace virtually impossible. Once ideas are released into cyberspace, they continue to circulate even if access to them is restricted at certain physical locations. One can deduct from these characteristics why the regulation of online information is difficult. Traditional media can be subject to control of their home states, even if they shift their operation

online and become online media. But online content sharing platforms comprise a constantly changing virtual space, in which users' ideas are circulated, and these platforms are operated by private companies that are out of direct reach for media regulators in most countries. However, Ukraine is only one of the many countries around the world that engage in the regulation of these platforms. Justifications they use to introduce this regulation are discussed in the next section.

Justification of government regulation of content sharing platforms

In democratic countries, freedom of speech and expression are the guiding principles in approaching the media. The number of restrictions that can be applied to the content of information distributed by the traditional media is limited to a few causes. In the United States, the Supreme Court allows restrictions on speech in cases that do not deserve the First Amendment protection, including "fraud, obscenities, defamation, and incitement" (Nuñez, 2020). The International Covenant on Civil and Political Rights (ICCPR) (1966) states in Article 19(3) that any restrictions on the freedom of speech must be established by law and deemed necessary for "respect of the rights or reputation of others [and] for the protection of national security or of public order (ordre public), or of public health or morals."² Article 20 guides that any propaganda of war and "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" must be prohibited by law. The ICCPR also asserts that "[e] veryone shall have the right to hold opinions without interference" (Article 19). One may argue that unlike legacy media that produce disseminated information and are responsible for its content, users who create and share content online are not professional journalists and have a personal right to "hold opinions."

² International Covenant on Civil and Political Rights, art. 19, *adopted* Dec. 16, 1966, **S.** Treaty Doc. No. 95-20, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR]. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Therefore, efforts undertaken by states to regulate content sharing platforms are scrutinized by the international community. The 2017 "Joint declaration on freedom of expression and 'fake news,' disinformation and propaganda" adopted by The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, deplored:

attempts by some governments to suppress dissent and to control public communications through such measures as: repressive rules regarding the establishment and operation of media outlets and/or websites; ...unduly restrictive laws on what content may not be disseminated; ... technical controls over digital technologies such as blocking, filtering, jamming and closing down digital spaces; and efforts to "privatise" control measures by pressuring intermediaries to take action to restrict content. (p. 2)

In other words, according to international conventions, legal restrictions on freedom of expression are recognized as justified when they protect national security. They further specify that incitement to discrimination, hostility, or violence shall be prohibited. At the same time, they emphasize the importance of ensuring freedom to seek and receive information. In this regard, international community warns against applying technical controls over digital spaced and efforts to compel intermediaries to restrict content.

Nevertheless, a growing number of states across the world are engaged in the regulation or development of regulation for content sharing platforms. According to Rochefort (2020), more than half the countries have passed "social media privacy laws, of varying scope and

sophistication, with more bills awaiting consideration" (p. 228). He also reports that Freedom House found in 2018, "at least seventeen countries, located in Europe, the Middle East, South America, Asia and other regions, [that] had passed or proposed laws limiting online content with the stated goal of combating fake news and other problematic digital content" (pp. 228-229). In addition, states engaged in social media regulation indicate the following reasons for limiting online content: protection of minors against harmful content and inappropriate commercial communications, as well as protection against incitement to violence or hatred (AVMDS, 2018), protection against abhorrent violent conduct or behavior (Sharing of Abhorrent Violent Material Act, 2019³), or protection against extremism (Russia, 2013⁴).

As follows from research findings and international documents referenced above, restrictions on freedom of speech are legitimatized when publicly available information threatens public order, moral values, and presents a risk to society. The concepts of risk and threat are emerging as drivers for securitization of cyberspace regulation.

Securitization of the Internet regulation

Ünal (2015) describes security as an absence of threats. Threats to security can be either military or non-military, e.g., related to economic interests of the state. Proceeding from securitization theory developed by Wæever and the Copenhagen School, he further asserts that any concern can be securitized through a set of stages that frame it as a security issue by "creating urgency and setting political priorities, as well as identifying existential threats that justify emergency-politics outside the normal framework of governance" (p. 178). A similar process applies to securitization of cyberspace. According to Ünal (2015), "[I]egitimizing the securitization of cyber space by resorting to a discourse of 'risk to society' has become a routine

³ https://www.legislation.gov.au/Details/C2019A00038

⁴ http://www.consultant.ru/document/cons_doc_LAW_156518/3d0cac60971a511280cbba229d9b6329c07731f7/

matter for 'good' public policy" (p. 179). In other words, cyberspace and content associated with it can be framed as a threat to national security on the basis of risk they present to society, thus leading to legitimization of restrictive measures and increased control of the online content.

The concept of threat is identified with the concept of risk, or anticipation of a catastrophic event based on a prior experience (Beck, 2006). Beck (2006) argues that risk is a "socially constructed phenomenon" visualized through mass media, symbolic forms, and other means for the public (p. 332). In the Ukrainian context, Russian military aggression took place in the regions of the country, which were exposed to an extensive Russian information campaign propagated through Russian media (Valevska, 2019). According to Valevska (2019), shared historical past, family ties between Ukraine and Russia, and similarity of cultures made certain population groups susceptible to Russian propaganda and supportive of Russia's agenda for Ukraine. Consequently, controversial topics related to the country's history and culture became associated with risk to security, in particular with the risk of so called "hybrid warfare."

According to Wigell (2019), threats of "hybrid interference" (or "hybrid warfare") are among the top threats on the western security agenda. Hybrid interference consists in the use of both military and non-military means of interference. Non-military means, according to Wigell, include clandestine diplomacy, geoeconomics, and disinformation. The purpose of hybrid interference is to intervene "in domestic politics by seeking to shape perceptions... to incline targets to voluntarily take steps that further the agent's agenda, or, failing that, to paralyse its decision-making capacity" (p. 262). Wigell argues that disinformation that was traditionally spread through newspapers and broadcasting is now reinforced by Internet technologies. He states, "[s]everal studies show how exploiting the hyperconnected nature of cyberspace has been critical to the recent Russian successes in planting, disseminating and lending credibility to

disinformation" (p. 266). Ukraine, which has an armed conflict on its territory prompted by hybrid interference from Russia, sees cyberspace, including content sharing platforms, as a catalyzer for the current conflict.

Ukrainian scholars also consider that information space including the Internet becomes a battle ground in a modern warfare. Smola (2016) argues that "electronic media have destroyed existing state borders," allowing for more interaction but also shaping the reality for their users and affecting their worldview (pp. 49-50). She concludes that influence on the information resources of the state "has become one of the sources of threats to the national security of any country, regardless of its level of development and influence" (p. 51). Tsebynoha and Tsebynoha (2018) suggest that measures of combatting the threats of hybrid interference should include development and implementation of a state policy in the information sphere. Thus, state regulation of the information resources, including electronic media, becomes a necessity grounded in the security interests of the state facing the reality of hybrid interference.

Approaches to content sharing platform regulation

Rochefort (2020) offers an analysis of regulatory efforts undertaken by the United States and western Europe that covers both acting policies and laws, and proposed government legislation. Rochenfort discusses three types of regulatory policies: industry self-regulation, limited government regulation, and comprehensive government regulation. Self-regulation provides for the minimum government involvement, instead, "private social media organizations are encouraged to oversee their own operations and rectify their own shortcomings and transgressions" (pp. 234-235). Examples of industry self-regulation include Facebook Advertising Policies and Google "Be Internet Awesome" media literacy initiative. Limited government regulation encompasses targeted standards for industry behavior formulated by

public authorities. Examples of limited government regulation are most regulations of the online content at the state level and 2017 Federal Honest Ads Act in the United States, as well as 2017 German Network Enforcement Act (NetzDG). Comprehensive government regulation widely applies government authority over online platforms. Rochenfort (2020) states that overall, "such reform attempts to reorganize an entire industry or organization with the goal of remedying the causes of dysfunction, not just mitigating the symptoms" (p. 236). The 2018 European Union (EU) regulation GDPR and the proposed Public Utility Regulation and Break Up Platforms initiatives in the United States are examples of the comprehensive government regulation.

Senden (2005) discusses a co-regulation approach adopted in the European Union along with self-regulation. She describes co-regulation mechanism as a prior establishment of a general regulatory framework by a legislative authority that "leaves the further execution and implementation of this framework to the various private actors in the field concerned" (p. 27). According to Senden, co-regulation essentially complements legislation, in contrast to industry self-regulation that occurs outside the legislative framework.

National security considerations can be a decisive factor in selecting an approach to online platform regulation. Disinformation, as noted above, can be one of the forms of hybrid interference and thus present a threat to national security. Marsden, Meyer, and Brown (2020) discuss a number of ways an issue of online disinformation is tackled by members of the European Union. It can be regulated through policies against defamation, incitement to hatred and violence, or ban on misleading advertising techniques. In reference to disinformation that may present a threat to national security, the authors note that EU initiatives, like proposed Regulation on Prevention of Dissemination of Terrorist Content Online, envisage requiring online intermediaries to promptly remove terrorist content upon notification. Marsden et al.

conclude that the most effective way to combat disinformation is "through media pluralism and literacy initiatives, as these allow diversity of expression and choice" (p. 16).

This conclusion is supported by Nuñez (2020), who states that "legislation that is aimed at increasing people's digital media literacy and access to information on social media platforms is in line with freedom of expression principles and could reduce the impact of disinformation" (p. 785). At the same time, Nuñez admits that marketplace of ideas cannot prevent dissemination of disinformation because its underlying principles have been compromised. Marketplace of ideas is based on the principle that "falsehoods compete with truth until truth prevails" (p. 787), but when false ideas are disseminated knowingly with no interest in uncovering the truth, the state may need to intervene to ensure that the truth is revealed. He warns that because some of the largest providers of global social media platforms are based in the United States, "the legislation that regulates them should account for its legal implications both in the United States and abroad so as not to overly burden the platforms with inconsistent and sometimes contradicting policies" (p. 789). Finally, the scholar voices a concern that governments hostile towards the media may use online platform regulation to silence dissent. In finding a balance between unduly restrictive legislation and serious negative implications of unchecked disinformation, Nuñez recommends to "determine what legislators can do to stop the spread of disinformation while not infringing on the human right of freedom of opinion and expression" (p. 792). In other words, the state regulation countering disinformation is justified when disinformation is spread with malicious intent, but regulators should not restrict free exchange of opinion and avoid overburdening online intermediaries with restrictions, in particular if they are not based in the country of regulation.

To summarize, content sharing platforms, or social media platforms, that offer their users a space to produce, disseminate and consume content present a problem for regulators because of their transnational nature and lack of responsibility for the content created by users. Content regulation is limited in legacy media and online due to considerations of freedom of speech and expression. Therefore, government control has to be established by law and well justified. Threats to national security are often cited by states as the reason for introducing content sharing platforms regulation. Threats to security are formulated by countries based on the perception of risks grounded in prior experience of catastrophic events. Modern tactics of hybrid warfare, or interference, actively use disinformation to influence populations. Online platforms multiply the spread of disinformation, thus presenting a risk to national security and justifying government intervention. Approaches to content sharing platform regulation differ from industry selfregulation to limited government regulation or co-regulation to comprehensive government regulation. Scholars argue that media literacy and transparency are the most effective way to manage risks associated with disseminated disinformation because they support the free speech principle. However, when disinformation threatens national security, government intervention may be necessary. Academic literature reflects a concern that governments hostile to media may use platform regulation to suppress opposition.

Ukraine faces threats to national security related to the hybrid interference of Russia. It is undertaking to counter these threats by developing a policy to regulate its information space including online platforms. In order to determine whether these policies will be able to effectively mitigate threats to national security without restricting freedom of expression, this study will analyze Ukraine's draft laws on the media based on the following research questions:

RQ1: How are threats to national security defined in the current Ukrainian legislation?

RQ2: How does the media bill address threats to national security in the proposed regulation of online platforms?

I will first describe the legal and media environment in which the proposed laws on the media emerged and Ukraine's legislation defining national security.

Legal environment surrounding proposed laws on the media History of the bills

The first draft law on the media was registered with the Verkhovna Rada (VR),

Parliament of Ukraine, in December 2019 under No. 2693. A group of bill's authors and initiators was headed by Olexander Tkachenko, MP⁵ from the ruling "Servant of the People" party and then chair of the Parliamentary Committee on Humanitarian and Information Policy.

The Explanatory Note to the bill stated that the current legislation in the field of mass media, adopted in 1993-2006, was outdated and did not account for the modern level of technological development in the media industry. According to the authors, the goal of the bill was to establish a unified, orderly, and balanced system of legal norms aimed at regulating legal relations in the field of the media. This goal was to be achieved through

ensuring the realization of the right to freedom of expression, the right to receive comprehensive, reliable and operational information, to ensure pluralism of opinion and free dissemination of information, to protect the national interests of Ukraine and the rights of media users, to regulate media activities in accordance with the principles of transparency, fairness and impartiality, stimulating the competitive environment, equality and independence of the media" (p. 2).

⁵ Member of Parliament

Thus, declared goals of the bill and ways of their accomplishment were aimed at protecting both freedom of expression and national interests of the country. This approach meets the guidance of the ICCPR regarding legitimate efforts of the countries to restrict media content if it necessary to protect national interests provided that freedom of speech and opinions is secured.

The bill was submitted for public discussion and review of international organizations, such as the Organization for Security and Co-operation in Europe (OSCE), Counsel of Europe, and others. Ukrainian media community and public organizations raised concerns regarding attempts to extend the requirements of the Ukrainian regulator to all players in the modern media market that includes social media and video platforms. Commenting on the proposed regulation of foreign online platforms, Detector Media wrote, "Make your predictions of what such requirements may lead to. Will international players perform them? Will they be ignored? Will they leave Ukraine? Will prices increase for Ukraine? Your options?" (Petrenko, 2020). In an interview to Radio Liberty, Executive Director of the NGO Ukrainian Institute of Media and Communication Diana Dutsyk posited that although it is good that the law outlines measures related to the armed aggression, it does not specify the criteria for identifying content that threatens information security. She admitted that the criteria should be developed by the National Council and the regulatory body, and as "always in such matters, everything will depend on the composition of the National Council and this co-regulatory body. And here, too, there is a certain risk" (Shtorgin, 2020). Composition of the National Council presents a risk, in Ms. Dudsyk's opinion, because it is determined by the government: half of the members are appointed by the president and half by the VR. With the majority of the VR held by the President's party, the National Council may consist only of representatives appointed by the ruling party. The ruling

party and President Zelensky have "complicated" relationship with the media. Even as a running candidate, he ignored the national media and preferred communicating with voters through social networks without "mediators." The problem, however, is that this choice was explained by desire to avoid criticism. According to Ukrainskaya Pravda, "People close to the president have repeatedly said that he closely follows the publications in the media, where his name appears, and painfully perceives criticism" (Zelenskyi, 2019, para. 54). Having means to restrict the content of the media may give politicians the power to decide what information is allowed to become public. International reviewers also raised a number of concerns regarding regulation of online platforms, in particular, restrictions on dissemination of certain content and vague definitions of reasons for banning content in "situations affecting national security" (Legal analysis, 2020, p. 4). As underlined by Nuñez (2020), these are valid concerns related to the introduction of restrictions on media content. Legitimate nature of restrictions can be determined by analyzing whether a proposed law can effectively mitigate the risks presented by certain information.

While the bill was undergoing discussion, another group of VR members, led by Mykola Kniazhytskyi from the ex-president's "European Solidarity" party, developed an alternative bill that was registered with the VR in May 2020 under No. 2693-1. Only about one-third of the second bill differed from the original draft, but it contained some clarifications and additions to the text of the December bill. Both drafts went through VR committees' reviews and were revised and resubmitted to the VR. On July 1, 2020, the VR accepted the revised December bill as the basis for the future law and rejected the May bill. As a result, as of September 1, a draft law titled, "On the Media," is registered under No. 2693-d and is being prepared for second reading by a group of MPs led by Mr. Poturayev, the current chair of the Parliamentary

Committee on Humanitarian and Information Policy. The current bill retained provisions on online platforms that pertain to the threats to national security. Part IX of the bill specifically establishes restrictions in relation to the on-going armed aggression. It is therefore important to understand how national security is defined in Ukrainian legislation, what is presented as threats to national security and what restrictions related to national security are applied to the media content.

RQ 1: How are threats to national security defined in the current Ukrainian legislation?

Threats to the national security of Ukraine are detailed in Ukraine's Strategy of National Security adopted in 2015. According to the statute, Ukraine's national security lies in the defense of "its fundamental values, defined by the Constitution and laws of Ukraine - independence, territorial integrity and sovereignty, dignity, democracy, human rights and freedoms, rule of law, welfare, peace and security" (Article 1, para. 4). Whereas the previous revisions of the national security strategy viewed post-Soviet political and economic legacy and international terrorism as the main threats to Ukraine's national security, the approach changed after 2014. The Revolution of Dignity of November 2013 - February 2014 that secured Ukraine's orientation towards a Western-type democracy over its alliance with Russia caused aggression on the part of the Russian government. As stated in the National Security Strategy, Russia occupied the Crimea, a part of Ukraine, and started a military aggression in the east of the country (Pro stratehiyu, Article 1, para. 2). The Strategy specifies that Russian aggression has a long-term nature and in addition to military actions, takes the form of "information and psychological warfare, belittlement of the Ukrainian language and culture, falsification of Ukrainian history, formation of alternative reality, [and] distorted information picture of the world by the Russian mass

media" (Article 3, para. 3.2). The Strategy, therefore, recognizes that disinformation as a form of Russian aggression presents a threat to national security by intentionally targeting controversial issues. These provisions confirm Beck's (2006) argument that threats are identified based on prior experiences and anticipation of future disastrous events. Nuñez (2020) posits that state intervention is necessary to ensure truth is revealed in case of intentional disinformation campaigns. This is important because it separates malicious disinformation from opinions held on controversial issues, which must be protected under the freedom of speech principle (ICCPR, 1966).

According to the Strategy, a lack of comprehensive state communication policy and an "insufficient level of media culture in the society" also have a negative impact on national security (Article 3, para. 3.6). To address these threats, the Strategy outlines priority protective measures to mitigate the threats that include combatting information campaigns against Ukraine which manipulate public consciousness and disseminate distorted information, protecting national values and strengthening the unity of the Ukrainian society, and introducing national educational programs to improve media culture.

Doctrine of information security of Ukraine (2017) sees policymaking priorities in establishing

legislative regulation of the mechanism of detection, fixation, blocking and removal from the information space of the state, in particular from the Ukrainian segment of the Internet, information that threatens the life, health of citizens of Ukraine, promotes war, national and religious enmity, change of the constitutional order by force or violation of the territorial integrity of Ukraine, threatens state sovereignty, promotes communist

and/or National Socialist (Nazi) totalitarian regimes and their symbols. (Article 5, para.

5)

To sum, threats to national security are defined in the National Security Strategy. The primary threat is associated with the Russian aggression, its military actions and information warfare. National security, according to the Strategy, is assured by protecting Ukraine's national interests that include territorial integrity and sovereignty as well as democracy and human rights. Information threats related to the hybrid interference of Russia present threat to national security by intentionally targeting controversial issues, such as language, culture and history of Ukraine. This threat can be mitigated by combatting Russian information campaigns, protecting national values and introducing media literacy education. Doctrine of Information Security calls for establishing legal mechanisms for identifying and removing from the Ukrainian segment of the Internet information that threatens life and health of Ukrainian citizens, promotes war and violation of territorial integrity. The next section describes how the draft law addresses threats to national security in the regulation of online platforms.

RQ 2: How does the media bill address threats to national security in the proposed regulation of online platforms?

Definition and status of online platforms

It is important to see how the bill defines online platforms in order to understand the scope of the proposed legislation and whether platforms are treated differently from other online content, as well as how their ownership shapes their responsibilities. The bill separates online media from online platforms based on the presence of editorial control over the published content. Article 1 defines online media as the media which distribute information in an electronic format on their own website or on their page at the information sharing platform. Online

platforms are called "information sharing platforms" or "video sharing platforms" and are defined in Article 1 as follows:

Information sharing platform - a service to provide users with the ability to download and store information, including audiovisual programs, user videos and other user information for viewing and use by an unlimited number of persons, over which the owner of the information sharing platform does not exercise editorial control; in addition, the organization of the posted programs and user information is carried out by such provider with the use of automatic means and algorithms, in particular concerning sequence of display and systematization. (pp. 6-7)

Although it is recognized in the definition that platform providers do not exercise editorial control over the content, it is not stated whether they are responsible for the circulated content. Diebert and Rohozinsky (2010) emphasized that cyberspace provides its end users with generative capacities which limits intermediaries control over them. Besides, once ideas are released in cyberspace, control of a certain physical location cannot prevent them from spreading. These specifics are not reflected in the definition.

According to the revised draft, platforms will not be regulated by the law unless their providers, their parent company or a company in the provider's group are located in Ukraine (Article 2, para. 12). Another provision specifies that a foreign media entity does not fall under the jurisdiction of Ukraine, but if its activities affect the rights and interests of citizens of Ukraine, a competent government body is obliged to take all possible measures to establish a mechanism of co-regulation with such an entity by concluding an appropriate memorandum or

⁶ Online platforms were called "information sharing platforms" in the earlier drafts but were later renamed to "video sharing platforms" to correspond to the terminology used in the European Union. See, for example, Directive 2010/13/EU of the European Parliament and the Council. Although the terms are sometimes used interchangeably in the text of the document, their general definition is provided in Article 1.

agreement (Article 2, para. 15). In Part II, the bill names providers of the video sharing platforms subjects in the field of the media who would be responsible for the actions prescribed by the law. In other words, if Dmytro Gordon, a Ukrainian journalist, posts his interview with Natalia Poklonskaya on YouTube under his personal account, it is YouTube as a provider who would be responding to Ukraine's competent authority. If Gordon posts it on his newspaper's website, Gordon.ua, he would be responsible for the interview's content as a media owner.

Individuals who do not act as a media outlet, according to the bill, are not held accountable for the content of information they post. Thus, it is proposed that foreign-owned video sharing platforms would not be regulated by the future law, and individuals sharing information on these platforms would not be held responsible for its content. However, if the posted content affects "rights and interests of the citizens of Ukraine," a platform provider will be contacted by a competent Ukrainian authority regarding the posted information.

Consequently, if the bill is adopted in its current form, YouTube will be responsible for removing content identified by Ukrainian authorities. While leaving the decision on whether specific information falls under restrictions prescribed by the law with the country authorities relieves intermediaries of the burden to inspect posted content, it also allows the authorities to decide whether the content affects interests of the Ukrainian citizens. In other words, establishing clear criteria for evaluating threat presented by information to the interests of Ukraine is critical for ensuring that freedom of speech is not violated.

Requirements for platform providers related to national security

The Explanatory Note to the bill states that one of the goals of the proposed law is to ensure legislative consolidation and

compliance with the requirements and restrictions in the field of the media on the territory of Ukraine in order to protect the national media space of Ukraine and build an information environment capable of confronting the current realities of hybrid warfare, and information security threats. (p. 2)

Article 23 of the bill specifies requirements for providers of video sharing platforms in regard to enforcing restrictions on information. Providers are expected to include in the conditions for using the service a ban on dissemination of user's content that violates the terms of Article 36 of the bill. Article 36 titled, "Restrictions on the content of information," forbids disseminating information containing "calls for forcible change, overthrow of the constitutional order of Ukraine, unleashing or conduct of aggressive war or military conflict, violation of the territorial integrity of Ukraine, materials or information that justify or promote such actions" (p. 38). In addition, the bill requires a platform provider to give users an effective mechanism for reporting and filing complaints against content restricted by the law and have in place a procedure for refuting and correcting inaccurate information.

In addition to Article 36 that describes general restrictions including restrictions related to national security listed above, there is a dedicated section of the bill, Part IX, that focuses on restrictions related to the armed aggression. The temporary nature of this section is explained in Article 118. The restrictions are in place from the time when the VR identifies a certain country as an "aggressor state" until this status is revoked. Article 119 establishes types of content that cannot be distributed through media because of the armed conflict. The banned content includes:

1) materials containing popularization or propaganda of the bodies of the aggressor state (occupant state), its officials, persons and organizations controlled by the aggressor state (occupant state), and their individual actions that justify or recognize legitimate armed

aggression, annexation, occupation of the territory of Ukraine, including public denial of these actions;

- 2) unreliable materials on armed aggression and actions of the aggressor state (occupant state), its officials, persons and organizations controlled by the aggressor state (occupant state), if this results in incitement of hostility and hatred or appeals to violent change, overthrow of the constitutional order or violation of territorial integrity or constitutional order;
- 3) programs and materials (except for informational or analytical), among the participants of which there are persons included in the List of Persons Who Pose a Threat to the National Media Space of Ukraine, approved by the National Council in accordance with Article 126 of this Law. (p. 131)

Paragraph 2 of the article specifies that it is possible to cover the activities of the aggressor state, but only in a critical light, at the same time requiring that information be provided "in accordance with the principles of reliability and balance" (p. 131). This requirement seems contradictory because it established by default that reliable and balanced information will be critical of the aggressor state. What is problematic in this provision is that rather than exposing the source of "unreliable materials" demonstrating that it is a part of the Russian information warfare, it bans content related to the armed aggression based on a broad definition of being "unreliable" or associated with a list approved by the National Council. Open discussion of controversial issues is necessary to develop media literacy. At the same time, media literacy is only mentioned three times in the bill – as a definition and as one of the tasks of the National Council. The legislation acts as a prescriptive and disciplinary mechanism in the use of information.

Addressing restrictions related to the armed aggressions, independent media freedom expert Dr. Joan Borata Mir wrote in the 2020 OSCE analysis of the original bill that some of the banned subjects covered "legitimate political opinions and discussions, related to matters of public interest in Ukraine, particularly regarding its territorial integrity" (p. 4). She argued that according to international standards, "only direct calls to the commission of crimes or to engage in forms of violence, discrimination of hostility can be limited by the legislator or any other State authority" (p. 4). The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression also asserts that "advocacy of hatred on the basis of national, racial or religious grounds is not an offence in itself. ...[it] becomes an offence only when it also constitutes incitement to discrimination, hostility or violence" (p. 12).

Returning to the example of an interview with Natalia Porklonskaya by Dmytro Gordon brought up in the introduction – following Article 119 of the bill, Gordon's interview would be banned from dissemination because Poklonskalya justifies the annexation of Crimea. Ukrainian journalists spoke against such prohibitions. Svitlana Ostapa, a member of the Ukraine's Commission on Journalist Ethics, stated, "Gordon constantly justifies the Revolution of Dignity when Poklonskaya says it is a coup. He emphasizes the annexation of Crimea - that it was illegal, that the referendum was illegal, as well as everything that is happening there now" (Ekspert, 2020, para. 4). The expert pointed out that there are historical examples of journalists interviewing war criminals. Gordon himself explained that he was interested in the interview because for him, Natalia Poklonskaya was "a symbol of betrayal, which in 2014 became powerful, massive. I never expected that so many government officials, top officials up to the commander of the fleet would betray Ukraine" (Dlia mene, 2020, para. 3). As clear from the motive, this topic is extremely important and relevant for the present-day situation in Ukraine. It

would be more damaging to the national security of Ukraine to avoid discussing such topics than to let them open for a public debate.

In addition, enforcing legislation on platform providers is problematic as underlined by Diebert & Rohozinsky (2010) and Ünal (2015), because these entities are located outside of the country and jurisdiction of its state authorities. The bill proposes to address this issue through voluntary registration and co-regulation.

Regulatory mechanisms and enforcement measures applicable to foreign online platform providers

To introduce a means of coordinating content restrictions with platform providers, the bill in Article 63 encourages providers to voluntarily register in Ukraine. In this case, they will need to communicate information on their output data, technology used to provide the service and the territory on which the service is provided. Registrants will be required to pay a registration fee.

The other option proposed by the bill is co-regulation outlined in Part VII. Co-regulation, as defined in Article 92, will combine functions and means of state regulation and industry self-regulation in order to "ensure the participation of media entities in the development and definition of requirements for the content of information disseminated by the media, and to prevent censorship and abuse of freedom of speech" (p. 103). The bill proposes to achieve this goal by setting up requirements for the dissemination of information based on the statute's provisions through the adoption of codes (rules) for the creation and dissemination of such information. Media entities would voluntarily undertake to comply with these requirements, and the National Council would recognize that these requirements are sufficient to ensure the public interest. One of the items to be regulated by the codes/rules includes the criteria for information banned from dissemination in Ukraine by the future law. Parties to the co-regulation agreement

will create a public association registered in Ukraine. Based on the provided instructions, registration looks like an easier option than co-regulation that will involve a lot of efforts heavily regulated by the bill.

Both options described above are presented as voluntary and will not provide the regulator with direct means to enforce restrictions on content. Therefore, the bill includes provisions outlining responsibilities for violating its requirements. Thus, Article 114 states that the National Council will have the right to impose sanctions on providers of video-sharing platforms for significant violations of the law. Significant violations include failure to provide information to the National Council upon a substantiated request, violation of Article 23 of the law (notifying users of content restrictions in Ukraine and having a procedure for banning, reporting and refuting prohibited content), and violation of registration terms in case of voluntary registration. For these violations, providers of video-sharing platforms will be "fined between 10 and 50 times the minimum wage on the day the violation is committed" (p. 127). If signs of violation of part two of Article 237 by the platform provider are detected, the National Council will transmit relevant information to law enforcement agencies and the VR. There is no clear indication of how the sanctions will be applied to foreign providers of online platforms who will be neither registered, nor in the co-regulation agreement with the Ukrainian regulator.

Discussion and policy recommendations

This study undertook to examine a proposed Ukraine's bill on the media in terms of its effectiveness in addressing threats to national security associated with online platforms.

Answering the first research question on how national security threats associated with online

⁷ "to provide in the conditions of using the service of the video access sharing platform for banning the dissemination of user information, which violates the requirements of Article 36 of this Law, as well as the requirements of copyright and related rights legislation" (p. 24)

platforms are defined in the current Ukrainian regulation, the analysis showed that the Strategy of National Security and the Doctrine of Information Security name Russian aggression, its military actions and information warfare as the primary threat to Ukraine's national security. Disinformation campaigns originating in Russia and often disseminated through the Internet using social media platforms address issues of territorial integrity and sovereignty of Ukraine. They became a part of hybrid interference that builds its effects on falsifying the picture of reality in the minds of targeted population. Among measures that can mitigate these threats to national security, the above Ukrainian legislation identifies combatting Russian information campaigns, protecting national values, and introducing media literacy education. The Doctrine also calls for establishing legal mechanisms for identifying and removing from the Ukrainian segment of the Internet information that threatens life and health of Ukrainian citizens, promotes war and violation of territorial integrity.

The second question was related to the ways the identified threats to national security associated with online platforms are addressed in the proposed regulation. The bill addresses the threats by establishing extensive restrictions on the information that can be distributed by online platforms and requiring platform providers to introduce mechanisms for reporting and removing content identified by the national regulator. Criteria for prohibited information are often vague and subject to interpretation. Although the bill states that platforms will not be regulated by the proposed law, it establishes ways for making platform providers responsible for abiding by the law by providing in addition to voluntary options, a system of sanctions for failure to fulfil the requirements. On the one hand, the bill meets the guidance of the Doctrine of Information Security on establishing mechanism for removing harmful information from the information

space of the state. On the other hand, it prevents discussion of important issues related to loyalty and love to your country, as demonstrated by the example with Gordon's interview.

As underlined by Ünal (2015), cyberspace embraces a complex system of physical and informational components, which makes it difficult to regulate it. In addition, the regulation involves foreign companies outside the jurisdiction of Ukraine. Information circulating through online platforms that provide users access for producing, disseminating, and consuming content constitute ideas and opinions protected by the freedom of expression. International communities in democratic countries warn against attempts to suppress dissent and control public discourse (ACHPR, 2017). Online platforms regulation is new for Ukraine, as it is for many countries throughout the world due to constantly developing technologies. Media policymaking in Ukraine is also young. In three centuries of country journalism, the first media law in Ukraine was the Law of the USSR "On Press and Other Mass Media" adopted on June 12, 1990 (Protsenko, 2012). Therefore, it is important to involve as much legal and journalist expertise and public input in the discussion of media laws.

Taking these considerations into account, it would be reasonable to approach threats to the national security on a case-by-case basis and justify them using a thorough process. Article 10 of the European Convention on Human Rights (ECHR) suggests using a three-part test to verify whether specific content should be banned. The test consists in ensuring the following three conditions are met:

1) any interference must be provided by law, 2) the interference must pursue a legitimate aim included in such provision, and 3) the restriction must be strictly needed, within the context of a democratic society, in order to adequately protect one of those aims, according to the idea of proportionality. (Legal analysis, 2020, pp. 11-12)

When these conditions are met, steps set up in the regulation can be taken to mitigate the identified threat.

The current bill places a responsibility on platform providers to identify and respond to the content prohibited by Ukraine. If foreign providers do not register in Ukraine or sign a coregulation agreement, it will be hard to enforce these responsibilities that also create an extra burden for providers. It may be advisable to consider approach taken in a proposed Regulation on Prevention of Dissemination of Terrorist Content Online, according to which national authorities notify online intermediaries of the harmful content and ask to promptly remove it (Marsden et al., 2020). Regarding co-regulation, reviewers noted that the process outlined in the bill is overly prescriptive and basically requires a provider to follow the rules established by the regulator. Nooren et al. (2018) suggested that principles-based regulation would be more effective than rule-based regulation in dealing with digital economy because it gives regulators room to decide whether a certain event should trigger an action based on a broad set of standards. Rule-based regulation is also more prescriptive and limiting (cited in Rochefort, 2020).

Finally, lack of media literacy is listed as one of the threats to the national security in the National Security Strategy of Ukraine, and it should be more prominently addressed in the law on the media. As underlined by scholars of media regulation, "legislation that is aimed at increasing people's digital media literacy and access to information on social media platforms is in line with freedom of expression principles and could reduce the impact of disinformation" (Nuñez, 2020, p. 785).

References

- Allyn, B., Bond, S., and Selyukh, A. (2020, July 29). Heads of Amazon, Apple, Facebook And Google Testify On Big Tech's Power. NPR. Retrieved from https://www.npr.org/2020/07/29/894802424/watch-heads-of-amazon-apple-facebook-and-google-testify-on-big-techs-power
- Beck, U. (2006). Living in the world risk society. Economy and Society, 35(3), 329-345.
- Borodians'kyi, V. (2019, November 10). Ne zbyralys I ne zbyraemos regulyuvatu standarty novyn [Did not plan and do not plan to regulate news standards]. *Ukrinform*. Retrieved from https://www.ukrinform.ua/rubric-society/2815241-ne-zbiralis-i-ne-zbiraemos-regulyuvati-standarti-novin.html
- Diebert, R. J., and Rohozinsky, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International political sociology*, 4, 15–32.
- Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. (2018). *EUR-Lex*. Retrieved from https://eur-lex.europa.eu/eli/dir/2018/1808/oj
- Directive 2010/13/EU of the European Parliament and the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). (2010). EOR-lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013&from=EN

- "Dlia mene Poklonskaia symvol zrady", Godon pro intervju ["For me, Poklonskaya is a symbol of betrayal" Gordon on the interview]. (2020, May 14). *Espreso.tv*. Retrieved from https://espreso.tv/news/2020/05/14/quotdlya_mene_poklonska_symvol_zradyquot_gord on_pro_intervyu
- Doktryna infromatsiyinoyi bezpeku Ukrayiny [Doctrine of information security of Ukrane].

 (2017). Verkhovna Rada Ukrayiny. Retrieved from

 https://zakon.rada.gov.ua/laws/show/47/2017#Text
- Dutzyk. D., & Dyczok, M. (2020, February 10). Ukraine's New Media Laws: Fighting

 Disinformation or Targeting Freedom of Speech? Wilson Center. Retrieved from:

 https://www.wilsoncenter.org/blog-post/ukraines-new-media-laws-fighting-disinformation-or-targeting-freedom-speech
- Ekspert pro interv'yu Gordona z Poklons'koyu: YouTube nashim zakonodavstvom ne reguliuyetsia [Expert about Gordon's interview with Poklonskaya: YouTube is not regulated by our legislation]. (2020, May 12). *Ukrinform*. Retrieved from https://www.ukrinform.ua/rubric-society/3023791-u-komisii-z-zirnalistskoi-etiki-prokomentuvali-intervu-gordona-z-poklonskou.html
- Fiegerman, S. (2018, April 12). Congress grilled Facebook's Mark Zuckerberg for nearly 10 hours. What's next? CNN Business. Retrieved from https://money.cnn.com/2018/04/12/technology/facebook-hearing-what-next/index.html
- International Covenant on Civil and Political Rights. (1966). S. Treaty Doc. No. 95-20, 999
 U.N.T.S. 171. Retrieved from

https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

- Joint declaration on freedom of expression and "fake news", disinformation and propaganda. (2017). Organization for Security and Co-operation in Europe. Retrieved from https://www.osce.org/fom/302796.
- Legal analysis of the draft law of Ukraine "On Media." (2020). Organization for Security and Co-operation in Europe. The Representative on Freedom of the Media. Retrieved from https://www.osce.org/representative-on-freedom-of-media/447508.
- Marsden, C., Meyer, T., and Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation? *Computer law and security review*, *36*, 1-18.
- Nuñez, F. (2020). Disinformation Legislation and Freedom of Expression. *University of California, Irvine Law Review*, 10(2), 783-797.
- Petrenko, H. (2020, January 14). Zakonodavtsi zvazhylysia na rehulyuvannia Neflix ta Facebook v Ukrayini. Shcho tse oznachaye? [Lawmakers have decided to regulate Netflix and Facebook in Ukraine. What does it mean?]. *Detector Media*. Retrieved from https://detector.media/infospace/article/173879/2020-01-14-zakonodavtsi-zvazhilisya-na-regulyuvannya-netflix-ta-facebook-v-ukraini-shcho-tse-oznachae/
- Proekt Zakonu pro media [Draft law on the media], No. 2693. (2019). *Verkhovna Rada Ukrayiny*. Retrieved from https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812
- Proekt Zakonu pro media [Draft law on the media], No. 2693-d. (2020). *Verkhovna Rada Ukrayiny*. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

- Proekt Zakonu pro media v Ukrayini [Draft law on the media in Ukraine], No. 2693-2. (2020). *Verkhovna Rada Ukrayiny*. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68970
- Pro stratehiyu natsionalnoyi bezpeky Ukrayiny [On the Strategy of National Security of Ukraine]

 (2015). Verkhovna Rada Ukrayiny. Retrieved from

 https://zakon.rada.gov.ua/laws/show/105/2007#Text
- Protsenko D. V. (2012). Rozvytok zakonodavstva Ukrayiny u sferi rehulyuvannia diyalnosti ZMI

 [Development of the mass media regulation in Ukraine]. Naukovi zapysky NaUKM

 [NaUKMA Research Papers]. Law, 129, 88-92. Retrieved from

 http://ekmair.ukma.edu.ua/bitstream/handle/123456789/2208/Protsenko_Rozvytok_zako

 nodavstva_Ukrainy.pdf?sequence=1&is Allowed=y
- Rochenfort, A. (2020). Regulating social media platforms: A comparative policy analysis.

 Communication law and policy, 25(2), 225-260.
- Senden, L. (2005). Soft law, self-regulation and co-regulation in European law: Where do they meet? *Electronic Journal of Comparative Law*, 9(1), 1-27.
- Smola, L. E. (2016). Aspekty vedennia informatsiyinoyi ta hibrydnoyi viyiny v konteksti zastosuvannia komunikatsiyinykh tekhnolohiy [Aspects of information and hybrid war in the context of application of communication technologies]. *S.P.A.C.E.*, *1*, 48-53. Retrieved from http://dspace.onua.edu.ua/handle/11300/7303
- Shtorgin, I. (2020, June 15). "Zakon pro media": Chotki pravyla dlia usikh chu nastup na svobody slova yi internet [The Media Law: clear rules for all or an attack on freedom of speech and the Internet]. Radio Svoboda. Retrieved from:

 https://www.radiosvoboda.org/a/zakon-pro-media-krytyka/30670314.html

- Ünal, S. (2015). Legitimizing securitization of cyberspace by using "risk" discourse. In Baybars-Hawks, B. (Ed.). *New media politics: Rethinking activism and national security in cyberspace*. Cambridge scholars publisher.
- Valevska, I. A. (2019). Sotsioculturni peredumovy rozpovsyudzhennya informatsiyinykh vplyviv rosiyiskoyi propagandy [Social and cultural prerequisites for dissemination of information influences of Russian propaganda]. In Smirnova, O. V. (Ed.). Proceedings of the international scientific-practical conference "Deocupation and reintegration of the information space of Crimea: International law." Institute of International Relations, Kyiv: Ukraine.
- Wigell, M. (2019). Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*, 95(2) (2019), 255–275.
- Zelenskiy vs zhurnalisty. Pochemu ne vse initsiativy prezidenta poleznye [Zelensky vs journalists. Why not all the president's initiatives are useful]. (2019, November 12).

 Ukrainskaia Pravda. Retrieved from

 https://www.pravda.com.ua/rus/articles/2019/11/12/7231754/