
Analyzing the Ground Zero.

**What Western Countries can Learn From Ukrainian Experience of
Combating Russian Disinformation**



Kateryna Kruk

Kremlin Watch Special Fellow

Kremlin Watch is a strategic program which aims to expose and confront instruments of Russian influence and disinformation operations focused against Western democracies.

The report analyses different ways in which Ukraine tried to combat Russian information attacks, covering the period from the annexation of Crimea until the end of 2017. It provides the assessment of the effectiveness of the activities of the state and civil society according to the following response areas: putting hostile disinformation efforts on the foreign and security policy agenda, publicly challenging supporters of the Kremlin-sponsored efforts, disclosing disinformation campaigns substance and vehicles, systematically building resilience within free societies (see the table below).

Adoption of the Doctrine of information security was warmly welcomed as an important step to increase information defense capacities. However, so far the implementation of the Doctrine has a limited impact due to the lack of the effective system of efforts coordination among state and civil society actors. Political will to make decisive steps is another important element of the success of disinformation fight. Example of Ukrainian Ministry of Information Policy shows that creating a new government body to fight disinformation only makes sense if there is a sufficient political will and consensus between the leading political actors to ensure that it receives enough staff, budgetary allowances, and proper division of labour with existing institutions.

However controversial, opinion polls indicate that the decision to ban Russian TV channels from the Ukrainian media space was correct. In 2014, 27% of Ukrainians watched Russian TV news, but within two years, this number dropped to 6%. Moreover, Ukraine has witnessed a significant decrease in trust in Russian TV channels. In 2014, 20% of Ukrainians trusted Russian TV channels, in 2017 this figure dropped to only 1%. However, communications campaigns are strongly needed to ensure the proper understanding of the importance of introducing certain limitations. Example of banning Russian social media shows that it can have a short-term effect if people don't understand the logics behind it. After first months success when Ukraine has seen a significant drop in popularity of Russian websites among Ukrainian users, the trend stopped and people started actively returning to certain websites.

The very first NGO organizations that were dealing with fact-checking and detecting fake news, combating Russian manipulating narrative, raising alarm about the disinformation attacks by collecting evidence, appeared already in March 2014, long before Ukrainian state institutions started to act. The report provides an overview of Ukraine's biggest and most successful NGOs that fight Russian disinformation and areas of their activities. It also provides a special case study of the activities of Ukraine Crisis Media Centre which is a unique example of official institutions and NGO joining forces to strengthen communication capacities of the state. Currently, apart of analyzing and disclosing disinformation campaigns, Ukrainian NGOs started to organize workshops and seminars to share their knowledge and increase awareness among Ukrainians.

Brief overview of the analyzed Ukrainians measures according to four response areas.

| Measures overview | Response area one: firmly putting hostile disinformation efforts on the foreign and security policy agenda | Response area two: Publicly challenge supporters of Kremlin-sponsored efforts | Response area three: Disclose disinformation campaigns substance and vehicles | Response area four: Systematically build resilience within free societies |
|----------------------------|--|--|---|---|
| International level | | | International cooperation and exchange of information for prevention of the disinformation and manipulation campaigns | |
| National government | Codifying disinformation efforts to national security documents and updating Doctrine of information security Creating a new governmental institution to deal with disinformation efforts | Banning Russian TV stations, movies, social media, and websites. Reviewing legislation and analyzing the legal framework for countering disinformation and propaganda | | Organizing preventive social and information campaigns |
| Civil society | | Regular public challenging of disinformation narratives | Daily disinformation monitoring, analyzing, and disclosing disinformation campaigns | Strengthen government communication capacities Sharing experience among journalists, civic servants, and individuals |

The following are the main lessons learnt from Ukrainian experience in fighting Russian disinformation:

- Russian disinformation activities should be considered as a threat to the national security and the means of fighting them should be codified in the national security documents.
- When creating a new structure to address information security, it is important to have sufficient political will and consensus between the leading political actors to ensure that it receives enough staff, budgetary allowances, and proper division of labour with existing institutions.
- Coordination of efforts between state institutions, as well between state and civil society is the key to successful fight with disinformation.
- Limiting access to online portals that share disinformation and propaganda, as well as harvest users' personal data, is an effective measure to offset the capabilities of Russian disinformation campaigns to manipulate public opinion with target audiences.
- In countries where television is a primary source of information, banning TV channels that spread propaganda and disinformation is an effective measure to decrease public exposure to manipulation attempts.
- It is important for governments to communicate well not only with their own citizens but with foreign partners as well, especially when it comes to decisions that have potential international repercussions.
- NGOs are more rapid in their reaction, have more flexibility in their budget and have higher creative potential, thus delegating tasks to such organizations, or at least leading close state-NGO cooperation is an important means of counter-propaganda strategy.
- Preventing is always better than reacting, therefore conducting targeted information campaigns is highly recommended.
- Review existing legislature and analyse the legal framework for countering disinformation and propaganda.
- There should be various programs for increasing media literacy and experience sharing about countering disinformation available to journalists, civil servants, and individuals. Moreover, state should provide sufficient financial support for those initiatives.

LESSON LEARNT #1: Codifying fighting with disinformation in the national security documents: Ukraine's information security doctrine

Among many Western states, Russia's disinformation efforts remain a point of controversy. In particular, there is an ongoing tendency to assess Russian disinformation and propaganda in terms of freedom of expression and media pluralism. However, numerous examples prove that Russian disinformation campaigns are a form of hybrid attack on a foreign state.¹ Accordingly, one of the first steps to effectively protect Western states from the threat of Russian information war is an appropriate perception of Russian activities in terms of national security.

Ukraine, the first victim of the full scale of Russia's information war, recognised the gravity of the threat considerably fast. Due to extensive penetration of the Ukrainian media space by Russian media and narratives, the Kremlin's power to manipulate public opinion became evident at the very outset of its aggression against Ukraine. NATO Stratcom experts agree that this information campaign was central to Russia's special operation to take over Crimea².

Ukrainian authorities not only issued special laws and decrees to counter the destructive influence of Russian disinformation campaigns in Ukraine but also amended the National Doctrine on Informational Security to appropriately reflect the threat and codify disinformation efforts in the national security documents. On February 25, 2017, the President of Ukraine signed and effectuated the new Doctrine on Information Security of Ukraine.

The updated Doctrine (originally developed in 2009) presents an interesting precedent for Western countries. In particular, the Doctrine:

- officially recognizes the threat to national security posed by Russia's aggressive informational influence;
- recognizes that Russia is conducting systematic informational war against Ukraine;
- outlines national interests in the informational sphere;
- names the threats to national interests and national security;
- sets the priorities of state policies in the informational sphere;
- outlines mechanisms of realization of the Doctrine;
- provides terminological definitions (e.g., the terms 'strategic communications' and 'governmental communications' have been distinguished, with the former concentrated in the security and defence sector);
- emphasizes the importance of the development of public diplomacy;
- outlines the need for developed instruments to fight propaganda which do not limit the right to free access to information.

¹ Giles, K. (2016). "Handbook of Russian Information Warfare". *NATO Defense College*. November 2016. Available at: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf

² Berzins, J. et al (2015). "Analysis of Russia's Information Campaign against Ukraine". *NATO Strategic Communications Centre of Excellence*. January 2015. Available at: <https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine> >

A key advantage of the Doctrine is its attempt to harmonize the powers of governmental institutions and security bodies to protect the interests of the state in the information sphere and to avoid duplication of efforts. The Doctrine outlines main tasks in the field of information security and state institutions responsible for implementation.

According to the Doctrine, both institutions of civilian administration as well as security and law enforcement bodies are responsible for its fulfilment. The institutions in question are: the Cabinet of Ministers, the Ministry of Information Policy, the Ministry of Foreign Affairs, the Ministry of Culture, the National Television and Radio Council, the State Committee on Television and Radio, the Security Service of Ukraine, intelligence bodies, the state service on secure connection and data protection, and the National Institute of Strategic Studies³.

A risk for the successful implementation of the Doctrine is a **lack of clear coordination between different institutions** mentioned in the Doctrine and the levels of cooperation between them. On the one hand, the Doctrine emphasises the need for a centralization of efforts and algorithms of coordination and control. At the same time, it doesn't outline the concrete mechanisms of this cooperation. For example, the National Council on Security and Defence was chosen as a coordinator of the process of the Doctrine's implementation. However, the National Council lacks certain powers and resources that institutions of the central executive authorities have to make this coordination effective. The same problem of lack of powers and resources is also true for the Ministry of Information Policy, which will be addressed in detail later in this analysis.

Crucially, the Doctrine alone is insufficient for the effective implementation of its provisions. To this end, the adoption of the Doctrine should be followed by the preparation of draft legislation, normative acts, and plans of practical realization. It is important to remember that at this stage, cooperation with the civic sector and organisation of public debates are especially important. The Doctrine's fulfilment will inevitably influence many actors in Ukraine as well as the civilian population. The level of cooperation between institutions responsible for the realization of the Doctrine and civic society is a matter of critique rather than praise.

Lesson to consider:

+ Ukraine appropriately perceives the threat of Russian disinformation as a matter of national security. In Ukraine, institutions that are responsible for dealing with different types of informational threats are: the Ministry of Information Policy, the Ministry of Defence, the Security Service of Ukraine, the Ministry of Interior, the National Council on Security and Defence, etc. Updating the Doctrine of Informational Security in accordance with existing informational threats and recognizing Russia as an aggressor in the informational sphere rightly codifies the threat of disinformation within the national security documents.

Lesson to avoid:

- The Doctrine doesn't provide clear coordination mechanisms for efforts and control of the progress in the realization of Doctrine. This can lead to decentralization of activities, duplication of efforts, and delay in implementation.

³ Presidential decree №47/2017. *President of Ukraine*. February 2017. Available at: <http://www.president.gov.ua/documents/472017-21374> <

LESSON LEARNT #2: Is creating a new institution an effective way to fight disinformation? Analyzing the case study of Ministry of Information Policy of Ukraine

One element of the response to Russia's information warfare against Ukraine was the founding, of a new Ministry of Information Policy in late 2014. The Ministry is based on upholding the principles of freedom of speech and thought, and the protection of citizens' rights to express their views⁴. The key objectives of the MIP are:

- to develop strategies for Ukraine's information policy and the concept of information security;
- to coordinate government agencies in matters of communication and information dissemination;
- counteraction of informational aggression by Russia.

The MIP is primarily engaged in preparing draft laws in the field of information policy based on analyses of the existing legislative framework, working with journalists, raising awareness about informational threats and media literacy, and developing and carrying out social campaigns.

The particular direction of the work of the MIP with respect to increasing internal information security is strengthening the presence of Ukrainian media in the currently occupied territories:

- development of a national television and radio system to provide coverage of Ukrainian media on all territories, including Crimea and Donbas;
- deterring illegal signals to Ukraine from the currently occupied territories, especially in the front-line regions;
- stimulating the production of special content for the currently occupied territories⁵

According to the Doctrine of Information Security, the Ministry of Information Policy is one of its chief implementers, as designated by the number of tasks assigned to it. However, this responsibility raises questions about whether the Ministry has adequate capacities to effectively implement those tasks. First, although the MIP is the main entity responsible for providing information security, it is not a part of the security and defence sector and is not responsible for the fight against terrorism⁶. This means that the MIP lacks access to some classified information or coordination with security bodies. Secondly, in order to effectively implement tasks assigned to the MIP by the Doctrine, the Ministry should be delegated more powers and competence. Thirdly, the Ministry has only 29 employees and a very limited initial

⁴ About the Ministry. *Ministry of Information Policy of Ukraine*. August 2017.. Available at: <<http://mip.gov.ua/en/content/pro-ministerstvo.html>>

⁵ Ministry of Information Policy names three priorities of the internal information security of Ukraine. (2017, November 2). *Detector Media*. Available at: <<http://detector.media/infospace/article/131539/2017-11-02-mininformpolitiki-nazivae-tri-napryamki-vnutrishnoi-informatsiinoi-bezpeki-ukraini/>>

⁶ Popova, T. (2017, February 28). What does the Doctrine of Information Security mean? *Radio Svoboda*. Available at: <<https://www.radiosvoboda.org/a/28337376.html>>

budget of 4 million UAH (approx. €133 thousand)⁷. These weaknesses may indicate a lack of serious political will to further develop the Ministry so that it can ably fulfil its assigned tasks.

Apart from the MIP's limited powers and resources, many experts in Ukraine question the very idea of its creation. Indeed, the reaction of both experts and civic society was mostly critical. Some feared that the MIP will introduce censorship or limitations on freedom of press and expression⁸. These fear primarily derived from a lack of information and understanding about the responsibilities of the new ministry. The Minister of Information Policy was appointed in December 2014, but the Ministry itself was approved by the Cabinet of Ministers only in January 2015. At the time of the Ministry's creation, there was no clear division of functions between the MIP and other existing bodies responsible for Ukraine's information policy, such as the State Committee for Television and Radio Broadcasting, the state informational agency Ukrinform, and the State Tele-Radio Broadcasting Company (later transformed into the National Public Broadcasting Company of Ukraine). Moreover, several journalist organizations announced their concern over the fact that the Ministry was created without consultations with leading journalist organizations and associations⁹. In general, journalist circles and media experts have a rather critical attitude towards the Ministry, often referring to it in Orwellian terms as the "Ministry of Truth".

At the same time, however, there is a consensus among experts and civil society alike that the state should actively protect its information security and counter Russia's aggression in information space. The jury is still out whether creating a new bureaucratic body is the right strategy to this end. History has shown that in cases of disinformation or propaganda attacks, the civic sector responds much more quickly due to the absence of normative restrictions and bureaucratic decision-making procedures.

Lesson to consider:

+ Better coordination of information security efforts by state institutions is a good approach. When facing a disinformation attack, a state must be able to provide an effective and quick response in national defence.

Lesson to avoid:

- However, creating a specialised ministry to that end may not be the right decision, since the new bureaucratic structure may not be an expedient format for responding to the threats posed by constant disinformation attacks. When creating a new structure to address information security, it is important to have sufficient political will and consensus between the leading political actors to ensure that it receives enough staff, budgetary allowances, and proper division of labour with existing institutions.

⁷ Tax payers will pay 4 mln hryvnias for the Ministry of Information Policy of Ukraine. (2014, December 10). *Independent Media Union of Ukraine*. Available at: <<http://nmpu.org.ua/2014/12/ministerstvo-informpolityky-koshtuvatyme-platnykam-podatkiv-4-mln-hrn/>>

⁸ Ratsyborska, Y. (2014, December 5). Is Ministry of Information Policy is a big state "temnik"? *Radio Svoboda*. Available at: <<https://www.radiosvoboda.org/a/26726492.html>>

⁹ Media Union is expressing regret regarding the methods of creation of the Ministry of Information Policy of Ukraine. (2014, December 3). *Independent Media Union of Ukraine*. Available at: <<http://nmpu.org.ua/2014/12/media-profspiilka-vyslovyuje-zhal-cherez-metody-stvorenniya-ministerstva-informpolityky/>>

LESSON LEARNT #3: Coordination of efforts is a key to success

Weak coordination of efforts is not only a problem for state institutions responsible for the fulfilment of the Doctrine on Information Security – there is a notable lack of coordination and cooperation between state structures and civil society. In Ukraine, some of the most prominent NGOs¹⁰ were founded to increase Ukraine's resistance against Russian disinformation. Notably, all these organizations began working before the Ministry of Information Policy was created and the Doctrine on Information Security adopted. In a sense, these **NGOs took over certain responsibilities and spheres of state work when the government was too weak or unready to perform them**. These organizations still possess invaluable expertise in combatting Russian disinformation and run major national and international projects.

Coordination of efforts with the civic sector is important for several reasons:

- using the experience and expertise of the civic sector in preparing fulfilment approaches of the strategic documents on countering Russian disinformation;
- the civic sector could be effectively engaged in the realization of certain provisions in the Doctrine;
- feedback from civil society organizations about the plans of combatting Russian disinformation is important to maintain the balance between security actions and democratic freedoms (i.e., while countering Russian disinformation, Ukraine shouldn't turn into an authoritarian state itself);
- coordination platform with NGOs can be used as an analytical hub that provides analytics about Russian disinformation efforts and propaganda methods;
- NGOs are generally faster and more flexible in their response to disinformation and propaganda. By coordinating response efforts to disinformation campaigns between state and civil society, their effectiveness can increase significantly.

What is the profile of the biggest Ukrainian organizations countering Russian disinformation?

- **StopFake**,¹¹ a fact-checking website, was launched on 2 March 2014, right at the outset of Russia's takeover operation in Crimea. Originally, the project aimed to check news and refute disinformation and propaganda about events in Ukraine. Since then, the project has developed into an informational hub analysing different aspects of Kremlin propaganda not only in Ukraine but also in the EU and former Soviet states. StopFake translates their reports into 11 languages. StopFake and IREX recently conducted a pilot media literacy project in Ukraine called Learn to Discern¹². The goal was to equip Ukrainian citizens to both identify misinformation and demand better quality information. Results from the evaluation were extremely promising: people became more skillful in separating fact from fiction, and they shared what they learned with their family and friends.

¹⁰ Dutsyk, D et al. (2015). "How to counteract Russian information aggression". *Telekrytyka*. December 2015. Available at: <https://issuu.com/irf_ua/docs/telekritika_how_to_couneract_rf_agg>

¹¹ About StopFake. Available at: <<https://www.stopfake.org>>

¹² Susman-Peña, T. (2017, June 12). Ukrainians' self-defense against disinformation: What we learned from Learn to Discern. *IREX*. Available at: <<https://www.irex.org/insight/ukrainians-self-defense-against-disinformation-what-we-learned-learn-discern>>

- **Ukraine Crisis Media Centre** was founded in March 2014 by leading Ukrainian communications, PR, and international relations experts. UCMC aims to provide reliable information about developments in Ukraine. UCMC has recently grown into a large NGO that is active in different fields: e.g., providing a platform for briefings and roundtables with simultaneous translation into English, preparing newsletters for more than five thousand international subscribers, supporting reform of governmental communications by delegating its experts to key state institutions, running a media centre for communicating and explaining reforms occurring in Ukraine, developing public cultural diplomacy, and providing a platform for coordinating national audiences.
- **Informnapalm** InformNapalm volunteer initiative emerged as a response to the Russian aggression in Ukraine in March 2014¹³. Now it unites the efforts of more than 30 volunteers from over 10 countries. Their investigations are available for the readers in more than 20 languages. Informnapalm issued a handbook of Russian aggression in Ukraine “Donbas in Flames. Guide to the Conflict Zone”. This guide is particularly useful to journalists, researchers, war experts, diplomats and general readers seeking information on the war in Donbas.
- **Euromaidan Press** is an online English-language independent newspaper launched in 2014 by Ukrainian volunteers. EP focuses on covering events in Ukraine and provides translations of Ukrainian news and expert analysis as well as independent research. Euromaidan Press releases weekly newsletters from the Friends of Ukraine network, covering projects in support of Ukraine. Jointly with Euromaidan SOS, Euromaidan Press launched and runs the site letmypeoplego.org.ua for the #LetMyPeopleGo campaign, aimed to free Ukrainian political prisoners and hostages illegally held in Russia¹⁴.
- **Informacijnyi Sprotyv (Informational Resistance)** was launched in March 2014. IR is a non-governmental project that aims to counteract external threats to Ukraine’s information space in the main areas of military, economic, and energy, as well as the sphere of informational security. IR provides analytical materials prepared by in-house experts (Center for Military and Political Studies), as well as Ukrainian and foreign experts from non governmental and government agencies to counter informational challenges in the military, economic, political, and security spheres¹⁵.
- **Likbez. Historic Front** was founded in spring 2014 by Ukrainian historians as a reaction to growing Russian revisionism about Ukraine’s past and the domination of Kremlin narratives in Western historical discourse¹⁶. The project runs its web pages in Ukrainian, Russian and English, organizes public lectures and historical reconstructions, cooperates with the military and studies the history of the Ukrainian Armed Forces, and publishes brochures about Ukrainian history.
- **Boycott Russia Today** is a Facebook page that regularly provides propaganda-debunking stories. It also runs a campaign to ban Russian Today in the U.S. if the channel refuses to stop broadcasting anti-Ukrainian propaganda¹⁷.

¹³ About us. Available at: < <http://informnapalm.rocks> >

¹⁴ About EuromaidanPress. Available at: <<http://euromaidanpress.com/about/>>

¹⁵ About us. Available at: <<http://sprotyv.info/en/about-us>>

¹⁶ Meta proektu. Available at: <<http://likbez.org.ua/ua/meta-proektu>>

¹⁷ Boycott Russia Today. Available at: <<https://www.facebook.com/boycottrussiatoday/>>

- **Ukrainski Kiber Wijska (Ukrainian Cyber Forces)** is a network of Ukrainian IT specialists working together to carry out both offensive and defensive operations in Ukrainian cyberspace. “White hackers”, as they call themselves, block the banking accounts of terrorists, block web pages that share anti-Ukrainian propaganda, and collect evidence of the presence of Russian military equipment in Ukraine. The network collects data and information about separatists and shares them with the Ukrainian Security Service¹⁸.
- **TrolleyBust**, a website established in 2015, aims to expose and block internet trolls who share anti-Ukrainian propaganda. TrolleyBust comprises a network of volunteers who share information about trolls and collectively send complaints about the accounts to the relevant social media platform(s)¹⁹.

Working with opinion leaders is another important sphere that requires coordination and proper communication from state. Each of influential public figures has a loyal community of followers. By reaching out to opinion leaders or respected figures in different spheres and explaining the rationale behind certain decisions, state can gain additional partners and supporters. People tend to trust respected figures more than state institutions.

Lesson to consider:

+ Civic action by NGOs and activists can be a very quick and effective way to counter disinformation and propaganda. So far, **the most effective and successful campaigns of exposing Russian disinformation and raising domestic and international awareness about it are the ones initiated by the civil society**. The NGO sector should therefore be treated as a trustworthy partner in informational security efforts and engaged in the realization of state-level counter disinformation activities.

Lesson to avoid:

- A lack of coordination between different projects and state structures renders the disinformation response more decentralized and weaker than it could be. In Ukraine, most of the NGOs devoted to countering propaganda are supported by their constituent members or alternatively by international foundations, foreign embassies, or international organizations, which makes continuity and sustainability of certain projects problematic. The state should therefore provide support to NGOs and projects working in the field of informational security.

¹⁸ Dutsyk, D et al. (2015). “How to counteract Russian information aggression”. *Telekrytyka*. December 2015. Available at: <https://issuu.com/irf_ua/docs/telekritika_how_to_couneract_rf_agg >

¹⁹ Trolleybust main page. Available at: <<https://trolleybust.com> >

LESSON LEARNT #4: To ban or not to ban? Measuring the effectiveness of Ukrainian decision to ban Russian websites and social media

Audience access, data collection, and behavioural analysis of reactions are crucial to the success of any type of informational campaign. The ability to pursue these targets renders actors more potent at exerting influence on their target audience. Under the conditions of information war waged by a foreign state, the protection of civic information space and citizens' personal data are matters of national security that require decisive defensive action.

In Russia, according to the infamous Yarovaya law, all companies listed in the register of information disseminators **are required to provide their users' personal data to the FSB**, namely:

- user's login;
- real name and surname;
- passport data;
- residence address;
- languages that are spoken by a user;
- user's network;
- information about the accounts in other services;
- IP address²⁰.

Companies including Vkontakte, Odnoklassniki, Yandex, and Mail.ru all appear on this register²¹. These are precisely the Russian websites that were recently banned in Ukraine²². The President of Ukraine commented on this decision: "Currently, we shouldn't distinguish cybersecurity and Russia's interference in the democratic processes around the world from its propaganda actions, which Russia conducts using Russian social media among others".²³

Despite the obvious security logic behind this decision, the reaction to it was very mixed, both in Ukraine and abroad. Many accused Ukraine of limiting free speech and Internet freedom²⁴. There were even several protests outside the Presidential Administration in Kyiv requesting retraction of the decision.

Ukraine's experience with banning Russian websites and social media exemplifies how poor communication can compromise an important security decision. All strategically important and consequential issues should be introduced only after the necessary communication has taken place.

The decision to ban Russian websites came in the third year of Russian aggression against Ukraine. Moreover, there was no specific incident that could be used to justify this ban. The President's decision

²⁰ Brysgalova, E. (2017, August 13). FSB will get an access to the personal data of the user's of social media that are allowed to work in Russia. *Vedomosti*. Available at: <<https://www.vedomosti.ru/technology/articles/2017/08/14/729199-fsb-dannim-polzovatelei>>

²¹ Registry of information disseminating websites. *Roscomsvoboda*. Available at: <<https://reestr.rublacklist.net/distributors/>>

²² On special personal and economic sanctions. Presidential decree №133/2017. *National Security and Defense Council*. April 2017. Available at: <<http://www.rnbo.gov.ua/documents/445.html>>

²³ President explained the reason of blocking Russian websites. (2017, May 17). *TSN*. Available at: <<https://tsn.ua/politika/poroshenko-poyasniv-prichinu-blokuvannya-rosiyskih-saytiv-930853.html>>

²⁴ Ukraine bans Russian Social Media Networks. (2017, May 16). *Hromadske International*. Available at: <<https://en.hromadske.ua/posts/poroshenko-signs-decree-blocking-russian-social-media-and-email-service-in-ukraine>>

therefore had an element of public surprise. Moreover, according to the author's own sources, the decision surprised even the government and people who were previously engaged in drafting the proposal for the President.

In the weeks following the ban, Ukrainian authorities spent much time and effort explaining and justifying the ban: they came from a defensive position, trying to shift the narrative away from concerns about freedom of expression to security instead. This complication could have been avoided if Ukrainian authorities had prepared a proper public communication campaign to inform the country of their intentions. Such consequential decisions cannot be introduced without prior explanation to domestic and international audiences.

Suitable communications are not only needed to avoid subsequent criticism but, above all, to convey the gravity of the threat and the value of the proposed changes. For example, in Ukraine, many debates revolved around the question whether the ban can be considered a restriction of free speech and internet freedom. The frame of discussion was whether or not *Ukraine* did something wrong rather than about the depth of FSB penetration of Russian websites. Unfortunately, Ukrainian authorities also failed to provide concrete examples FSB data espionage. At the end of the day, Ukrainian authorities appeared to be those pushing the limits of a democratic state, rather than those who take active precautions to safeguard the security of their citizens.

The lack of an adequate public communications campaign conveying the seriousness of the issue is confirmed by user numbers of certain websites in Ukraine. On the one hand, just a few months after the ban, V Kontakte – which had previously been the most popular website in Ukraine – no longer made the top 10 most visited websites in the country²⁵. Ukraine has instead seen significant usage growth with Facebook, Instagram, and Snapchat. At the same time, Ukrainians are actively using VPN services to overcome the ban and continue using V Kontakte. Numbers show that although V Kontakte has left the top 10 most visited websites, it hasn't lost its audience and still experiences slight increases in usage (data from June and July 2017²⁶). This proves that many Ukrainians still don't understand the seriousness of the threat and the potential implications of using websites to which the FSB has full access. Thus, although the ban had a major public impact, it has not solved the problem due to the lack of a strong educational and awareness campaign that would change public attitudes.

Lesson to consider:

+ limiting access to online portals that share disinformation and propaganda, as well as harvest users' personal data, is an effective measure to offset the capabilities of Russian disinformation campaigns to manipulate public opinion with target audiences.

Lesson to avoid:

- However, without a proper public communication campaign (both in the country and abroad), well-intended yet controversial government moves are likely to be criticized and resisted. Explaining the logic behind such moves is key to their acceptance.

²⁵ VK is out of top-10 most visited websites in Ukraine, Facebook is third most popular website. (2017, August 8). TSN. Available at: <<https://tsn.ua/ukrayina/vpliv-blokuvannya-rosiyskih-socmerezh-vk-vibuv-z-top-saytiv-v-ukrayini-a-facebook-uviyshov-do-triyki-972925.html>>

²⁶ Ibid

LESSON LEARNT #5: Ball cartridges of the propaganda: Russian TV stations, films and TV series. How Ukraine has effectively decreased their influence on public opinion

Before the beginning of the war, Ukraine's media space was deeply connected to Russia's. Although the biggest and most popular TV stations in the country were Ukrainian and owned by Ukrainians, the majority of broadcasted products originated in Russia. It was common to buy Russian programs, TV series, and movies instead of producing original content.

Russian TV content always contained highly charged narratives: e.g., the myth of the great Russian nation, the unity of the "Russian world", the similarities between Ukrainians and Russians who together form "one big nation", and the heroism of the Russian army and special forces that "fearlessly fight evil". These messages were often conveyed subtly, not in the straightforward political discussions but rather in the form of entertainment via concerts, TV series, and movies.

The situation changed with the beginning of Maidan and the war in eastern Ukraine. Ideologically charged Russian media took a highly offensive position towards Ukraine and events taking place in Kyiv. Russian media circulated conspiracy theories about Euromaidan, glorified the occupation of Crimea, denied Russia's involvement in the crisis in eastern Ukraine (soon followed by the invasion of Russian troops), and accused Kyiv of the failure of the Minsk process. Apart from a habit of falsifying news, Russian media continued to push the ideological narrative that Ukrainians and Russians are one nation divided by the fascist authorities in Kyiv. Taking into account that television in Ukraine remains the most popular source of information, with 61% of Ukrainians receiving their daily news this way²⁷, it was impossible to ignore the security implications of a continued Russian media presence in Ukraine. Starting on 24 July 2014, the National Television and Radio Council of Ukraine banned several Russian TV channels that were notorious for spreading false information and manipulating public opinion.

Opinion polls indicate that the decision to ban Russian TV channels from the Ukrainian media space was correct. **In 2014, 27% of Ukrainians watched Russian TV news, but within two years, this number dropped to 6%**²⁸. Moreover, Ukraine has witnessed a significant decrease in trust in Russian TV channels.

²⁷ Ukrainian media lose trust, the attitude to the Russian media has critically deteriorated even at East. (2015, July, 1). *Osvita. Media Sapiens.* Available at: http://osvita.mediasapiens.ua/mediaprosvita/research/ukrainski_zmi_vtrachayut_doviru_ale_stavlennya_do_rosiyskikh_zmi_kritichno_pogirshilos_navit_na_skhodi_sotsopituvannya/ >

²⁸ Ukrainian media popularity in 2016. (2016, September, 17). *Osvita. Media Sapiens.* Available at: http://osvita.mediasapiens.ua/mediaprosvita/research/spozhivannya_zmi_v_ukraini_2016_roku_populyarnist_facebok_zrostae_dovira_do_rosiyskikh_media_znizhuetsya/ >

The trend speaks for itself:

- in 2014, 20% of Ukrainians trusted Russian TV channels;
- in 2016, 4%²⁹;
- in 2017, only 1%³⁰.

Another important study on the influence of Russian propaganda in Ukraine was conducted in 2015 by Kyiv's International Institute of Sociology³¹. Remarkably, the results show that none of the Russian propaganda narratives about events on Maidan or in eastern Ukraine received significant support among Ukrainians. Based on the polls, an absolute majority of Ukrainians agreed with the following statements:

- In Donbas, the Ukrainian army is fighting against Russia and Russia-backed terrorists;
- most of the difficulties that Ukraine is currently facing are the result of Russian aggression;
- Events that took place in Kyiv in 2014 were a people's revolution.

The following statements received the lowest support:

- In Ukraine, ethnic Russians and the Russian-speaking population are persecuted;
- In Donbas, the Ukrainian army is fighting against its own people;
- The Donbas referendum reflected real aspirations of the locals citizens.

Accordingly, the case of banning Russian TV stations in Ukraine demonstrates that this measure has effectively inoculated Ukrainians from Russian propaganda and almost fully eliminated the possibility of Russian media to manipulate Ukrainian public opinion regarding the war in Donbas and Euromaidan. Ukrainians are fully aware that Russia is waging war against Ukraine.

Lesson to consider:

+ In countries where television is a primary source of information, banning TV channels that spread propaganda and disinformation is an effective measure to decrease public exposure to manipulation attempts.

Lesson to avoid:

- This measure may have a limited effect in countries where penetration by Russian media and pro-Russian narratives is insignificant or is only limited to the Russian-speaking population.

²⁹ Ibid

³⁰ During last year trust in Ukrainian TV stations and internet media has deteriorated. (2017, September 5). *Osvita. Media Sapiens*. Available at: http://osvita.mediasapiens.ua/mediaprosvita/research/za_rik_znizilas_dovira_ukraintsiv_do_telekanaliv_ta_internetz_mi_doslidzhennya_internews/ >

³¹ Russian narrative about Maidan and Donbas is not popular in Ukraine. (2015, July 2). *Osvita. Media Sapiens*. Available at: http://osvita.mediasapiens.ua/mediaprosvita/research/rosiyskiy_poglyad_na_maydan_ta_viynu_na_donbasi_v_ukrai_ni_ne_prizhivsya_sotsopituvannya/ >

LESSON LEARNT #6: “Make them fight with each other”. Can we prevent Russian disinformation activities from creating tensions between states?

Russia uses disinformation and influence campaigns not only to destabilize certain countries from within but also to create tensions and conflicts internationally between countries. Russia’s manipulation attempts regarding recently passed educational reform in Ukraine is a good example of such efforts.

In passing education reform, Ukraine has taken a step towards building a new system of education that would replace the previously existing Soviet model. Unlike this original system, the current reform takes into account international pacts and treaties, for example regarding the rights of parents to choose the educational format, the territorial accessibility of education, and the rights of children with disabilities.

However, some provisions in this reform regarding the languages of national minorities have been the subject of controversy. Previously, the whole course of secondary education could be taught in the native language of certain minorities. Now, under the new law, members of national minorities can obtain preschool and elementary education in their native languages, while secondary education is to be provided in the state language, with the native language taught separately³².

Russian media rapidly caught on to this issue and produced a number of fake and misleading reports about the reform, such as:

- national minorities in Ukraine are discriminated;
- provisions of the new law undermine the Ukrainian Constitution;
- the law on education bans the Russian language in Ukraine;
- schools of the national minorities will be closed;
- teachers teaching in the language of the minority will be fired³³.

Soon thereafter, these messages also reached Hungary. Unlike in Ukraine, however, they soon reached the mainstream media and were even repeated by politicians and members of government. Some representatives of Hungarian authorities claimed that if Ukraine won’t withdraw the law in question, Hungary will block every potential euro integration prospect for Ukraine. Hungarians also raised this issue at the parliamentary assembly of the Council of Europe, accusing Ukraine of discriminating against minority rights.

Tensions between the two countries were alleviated when the Ukrainian Ministers of Education and Foreign Affairs went to Budapest and met with their Hungarian colleagues. Once the provisions of the law were fully explained and a compromise for the Hungarian community in Ukraine was agreed, Hungary eased its position.

³² What do you need to know about education reform in Ukraine. (2017, October, 6). *Ukraine Crisis Media Centre*. Available at: <<http://uacrisis.org/61084-education-reform-ukraine>>

³³ Fake: Education law contradicts the Constitution and bans Russian language in Ukraine. (2017, September 29). *Stop Fake*. Available at: <<https://www.stopfake.org/fejk-zakon-ob-obrazovanii-protivorechit-konstitutsii-ukrainy-i-zapreshhaet-russkij-yazyk/>>

Lesson to avoid:

- It is important for governments to communicate well not only with their own citizens but with foreign partners as well, especially when it comes to decisions that have potential international repercussions. Ukraine didn't provide sufficient explanation for the rationale behind certain provisions of the education reform law. This oversight was quickly exploited by Russia and used as leverage to pressure the country. Ukraine reacted only after the issue became an international crisis and Hungary made very strong statements condemning the law. Importantly, monitoring the media and public space of foreign countries can help spot and pre-empt potential hurdles in the first place, before they devolve into international tensions, after which it is harder to find a compromise or steady the debate. Countries should therefore be aware of informational challenges in the foreign media space just as much as within their domestic context.

LESSON LEARNT #7: Leave it to professionals: why working with Ukraine Crisis Media Centre was probably the best step to strengthen state's communications capacities

Ukraine's Revolution of Dignity resulted in the formation of an entirely new government, following the ouster of President Yanukovich. In late February 2014, when the first "little green men" started appearing in Crimea, Kyiv witnessing a total change of power. Thus, for several weeks while the new government was being formed, Ukraine had a very limited capacity to react to Russian propaganda about Euromaidan and to the growing amount of disinformation about developments in Crimea. A group of most prominent Ukrainian strategic communications, PR, and foreign relations experts, recognising the seriousness of the challenge, founded the Ukraine Crisis Media Centre (UCMC). The chief aim of the UCMC was to create a trustworthy platform for sharing news from Ukraine, provide quality translations and support for foreign journalists, and fight Russian disinformation³⁴.

The UCMC began as a civic initiative aimed at strengthening Ukraine's communications capacities when state structures weren't able to respond to growing Russian propaganda activities. The organization's activities proved to be effective for several reasons:

- rapidity in reacting to disinformation campaigns or urgent events;
- reaching out to a very wide audience thanks to network merging and the founders' contacts;
- independence from political parties or state institutions that enhanced the trustworthiness of the platform;
- professional background and expertise of the members;
- flexibility in the realization of projects and their financing.

³⁴ About Ukraine Crisis Media Centre. Available at: <<http://uacrisis.org/ua/about>>

In first eight months of the UCMC's work – covering the period of the Crimean annexation, beginning unrest in eastern Ukraine, shooting down of MH17, and invasion of Ukraine by the Russian army – UCMC conducted almost one thousand briefings and six international campaigns abroad.

By the time the Ukrainian government became fully operational and able to react to informational threats, the UCMC started developing new projects within and outside Ukraine. After compensating for low governmental communications during the initial period of operation, the UCMC has since conducted work in several different areas. Nevertheless, its aim is to provide communications support to the state as needed has remained the same.

One of the most successful examples of cooperation between the UCMC and Ukrainian state institutions is the One Voice Policy project³⁵. In order to strengthen the communications of key governmental resorts, the UCMC delegated its experts to work within the Ministry of Defence, the General Staff, the Ministry of Finance, the Ministry of Economic Development and Trade, the Presidential Administration, and the Ukrainian Parliament. The One Voice Policy aimed at strengthening the communications capacities of governmental institutions, increase the effectiveness of communications efforts, and let key institutions speak with one voice about key topics. UCMC experts were also involved in reforming communications departments in the ministries and sharing their experience with public servants to ensure the sustainability of the changes.

For instance, the UCMC initiated daily briefings for the representative of the Anti-Terrorist Operation Staff to provide information about developments in eastern Ukraine. In periods of high escalation, ATO briefings were a reliable source of information that helped avoid media hysteria and reveal Russian disinformation aimed at demoralizing Ukrainians³⁶. The UCMC initiated and lobbied for this idea in the Ministry of Defence. It was also the UCMC's idea to provide the Ministry of Defence with an English-speaking spokesperson who could deliver briefings to foreign journalists³⁷.

The UCMC works closely with other organizations and state institutions to respond quickly to disinformation activities and fight manipulative Kremlin narratives about Ukraine. For instance, the UCMC and the Ukraine Institute of National Memory jointly create visual materials for the public about Ukrainian history and Soviet atrocities. For some time, the UCMC also worked closely with StopFake, another prominent Ukrainian NGO working to debunk Russian disinformation (see section 3), to disseminate StopFake's reports. The UCMC also runs a website, Ukraine Under Attack,³⁸ that provides comprehensive updates about the war in Ukraine for both domestic and foreign audiences, including investigations, infographics, documentaries, and audiovisual content.

³⁵ Ringis, A. (2014, December 12). Speaking one language with the world. How does the volunteer “ministry of information” work? *Ukrainska Pravda*. Available at: <<http://life.pravda.com.ua/volunteers/2014/12/12/185772/>>

³⁶ Ministry of defense spokesperson for the ATO. Available at: <<http://uacrisis.org/tag/rechnik-ministerstva-oboroni-z-pitan-ato>>

³⁷ Ministry of defense spokesperson for the ATO. Available at: <[http://www.mil.gov.ua/en/news/2017/07/24/topic-russian-military-aggression-in-eastern-ukraine-vilyen-pidgornyy-mod-spokesperson-\(video\)](http://www.mil.gov.ua/en/news/2017/07/24/topic-russian-military-aggression-in-eastern-ukraine-vilyen-pidgornyy-mod-spokesperson-(video))>

³⁸ Ukraine Under Attack. Available at: <<http://ukraineunderattack.org/en/>>

Lesson to consider:

+ **The case of the UCMC illustrates how, in some cases, civic society initiatives can react more nimbly and effectively to disinformation challenges.** NGOs have more flexibility in their budget and have higher creative potential. They are also more time flexible and unlike state institutions, are not constrained by a complicated and bureaucratic decision-making process. Delegating tasks to such organizations, or at least leading close state-NGO cooperation, is thus an important means of counter-propaganda strategy.

LESSON LEARNT #8: Preventing is always better than reacting: conduct targeted information campaigns

Russia's information war is characterized by a high number of targeted disinformation and influence campaigns. Since the beginning of the war, Ukraine witnessed numerous such campaigns against authorities, political and public figures, and institutions. Perhaps the longest and most intensive of these was a disinformation campaign against Ukraine's armed forces, closely related to the Kremlin's attempts to demoralize Ukrainians en masse. Key narratives in this campaign included the following:

- The leadership of your army is weak and must be fired;
- Service conditions in your army are terrible;
- Your President betrayed you in the Minsk negotiations – he and his generals are traitors;
- The West doesn't care about you, you are doomed;
- You can always escape from the army by going to Russia or Donetsk;
- Don't be fooled by your illegal government³⁹

Russians exploited low levels of trust in Ukraine's armed forces prior to the conflict. Since the collapse of the Soviet Union, in which the glorification of the Soviet army was one of the most prominent strategic narratives, Ukrainians witnessed a significant decrease in levels of trust and prestige of the army. An opinion poll⁴⁰ measuring the attitude of Ukrainians towards serving in the armed forces shows that in 2011, almost half of respondents (47.9%) perceived the army as a waste of time. Moreover, 68% of respondents said they don't condemn young men who evade service in the army. While describing the army, people often complained that they don't trust in its military capability, find it unprofessional, unreformed, and badly equipped.

At the beginning of the war, Russians began exploiting these existing negative perceptions about the army. The situation began to change with the escalation of the conflict in eastern Ukraine. Civilian volunteer battalions were the first to defend Ukraine's territorial integrity in the east. The Ukrainian armed forces were strongly supported by volunteers who started many nationwide campaigns to collect money for soldiers' needs. Due to the high number of soldiers and civilians engaged in fighting in the east, most

³⁹ According to Ukraine Crisis Media Centre

⁴⁰ Attitude of Ukrainians towards serving in the military. (2011, September 21). *UNIAN*. Available at: < <https://www.unian.ua/politics/544807-yak-ukrajintsi-stavlyatsya-do-slujbi-v-armiji-opituvannya.html> >

Ukrainians soon had a personal contact with someone who was fighting on the ground. Furthermore, Ukrainian news coverage of developments in the east, together with the ban on Russian TV channels, and information provided by the spokespersons of the Anti-Terrorist Operation Staff, increased public awareness that the Ukrainian army is fighting Russian aggression and Russia-backed terrorists in Donbas. In combination, these factors significantly increased public trust in the Ukrainian armed forces.

At the same time, there was a need to fight back against targeted disinformation campaigns regarding particular issues or persons. For instance, although support and trust for the Ukrainian army were growing, media coverage about its leadership was predominantly negative. In 2015, 63% of messages were negative. By undermining the leadership of the armed forces, propaganda messaging called for disobedience in the army and questioned the validity of orders issued by the leadership. This dissonance could potentially lead to serious disciplinary problems within the army.

The Ukraine Crisis Media Centre's activities to improve perceptions of the armed forces leadership presents a valuable case study. As mentioned, Ukraine experienced extensive Russian propaganda that exploited previously existing negative viewpoints of the Ukrainian army. But the problem was exacerbated by the weak communication capacities of the armed forces themselves and by structural weaknesses of Ukraine's media space (oligarch ownership of media outlets influences its positions; the Ukrainian media space is therefore also vulnerable to fake news).

To address this problem, the Ukraine Crisis Media Centre began cooperation with the Ukrainian Ministry of Defence and the General Staff of the Armed Forces of Ukraine. Its activities mainly aimed at providing Ukrainians with more official information from the armed forces and improving perceptions of its leadership and the validity of its orders. The UCMC took the following steps:

- Give voice on Ukrainian TV channels to military commanders from the front line at the battalion and brigade level;
- Put the Chief of Armed Forces in the spotlight;
- Provide information about the location of Russian army units and their soldiers and officers who were captured in Ukraine;
- Launch advertising campaigns about the prestige of service in the army.

Thanks to communications experts from the civic sector, both the General Staff and the Ministry of Defence improved their crisis communications capacities. Unlike before, both entities were providing constant updates and in case of escalation in the East, actively communicated with media and civilians.

Another important activity was the provision of more information about the activities of the armed forces and the situation in the east. To this end, the Ministry of Defence started producing infographics with daily updates in the east, explaining past military operations and the way they were conducted, and providing more information about the composition of the armed forces and particular divisions. Social media campaigns were also launched, including patriotic videos about the army⁴¹ and advertising the

⁴¹ Social campaign about the Armed Ground Forces of Ukraine. Available at: <https://www.youtube.com/watch?v=HZlyOmsDjew> >

contract army⁴². These activities proved highly successful: in a five month period, the percentage of negative coverage of the armed forces in the Ukrainian media was only 0.7%, while public trust in the Ukrainian armed forces rose to 53.1%, and continues to grow.

Lesson to consider:

+ It is vital to raise public trust and support for key state institutions, especially those responsible for public order and security. Developing civilian pride in the armed forces and the state's democratic institutions is essential to social stability.

Lesson to avoid:

- There is no need to wait for war or an armed conflict to begin fostering trust in the armed forces. Campaigns promoting respect for the army and sustaining its prestige should be a constant practice.

LESSON LEARNT #9: Deactivate Trojan horses. Review existing legislature and analyse the legal framework for countering disinformation and propaganda

Although the concept of information warfare is not new, the intensity of Russia's activities in this domain and their potential threat due to the ubiquity of the internet demand a serious counter approach. According to Russian scholars, the goal of information warfare is "*achieving political or diplomatic ends, and influencing the leadership and public opinion of foreign states, as well as international and regional organizations*"⁴³.

Information itself is not always the most important element of information warfare. What matters most is how this information is used against the enemy. This requires not only accurate analysis of one's target audience in order to make precise predictions about behaviour and reactions, but also comprehensive knowledge of the political, cultural, social, economic, legal background of the country. Elements of the political, cultural, social, and economic situation are used to develop the content side of the information attack. Meanwhile, familiarity with the legal system of the target state is needed to develop the implementation strategy of the information attack. This is what makes it particularly difficult to counter information warfare activities: by using loopholes or specific advantages in the target's legal system, Russia can evade persecution for its actions.

As Ukraine began to develop a more coherent approach to combating Russian disinformation and propaganda, it quickly became clear that, to do so effectively, certain legislative amendments would be necessary. The Ukrainian parliamentary committee on freedom of expression and information policy is the main stakeholder in the process of reviewing proposals and preparing draft laws. The Ministry of

⁴² Social campaign about contract service in Ukrainian armed forces. Available at: <https://www.youtube.com/watch?v=sbeym6qz8v4> > , <https://www.youtube.com/watch?v=JmhFDxrhNCA> > , <https://www.youtube.com/watch?v=5OxrbNGTy0> >

⁴³ Giles, K. (2016). "Handbook of Russian Information Warfare". *NATO Defense College*. November 2016. Available at: https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf

Information Policy also works on reviewing the existing legal framework and trying to identify loopholes that can be used by Russia in its hostile actions against Ukraine.

A case study about amending legislation on restricting access to the Ukrainian market for foreign printed products with anti-Ukrainian content is a valuable example⁴⁴. According to details provided in the explanatory note accompanying the law, 70% of all printed production in Ukraine comes from Russia. However, due to loopholes in regulations concerning the import of published products, there was no mechanism of control about what content was imported into Ukraine. The committee on freedom of expression and information policy of the Verkhovna Rada organized a number of roundtables with representatives of the publishing business in order to prepare a set of proposals about how to effectively protect the Ukrainian market from illegally published material from Russia and stimulate the development of Ukrainian publishing.

As a result, the Ukrainian parliament adopted a law that:

- adds to the list of prohibited published production any content that popularises and praises Russia's state institutions and their decisions, creates a positive image of the aggressor, justifies or supports the occupation of Ukrainian territory, or presents a positive image of the separatists;
- gives powers to the central executive body responsible for implementing state policy in the publishing sphere to give permission to import published production from the aggressor state or temporarily occupied territories or to decide that published production is prohibited in Ukraine;
- creates an expert council at the central executive body that implements state policy in the publishing sphere and can evaluate the content of published production that is imported from the aggressor state or temporarily occupied territories and decide whether it breaks Ukrainian law;
- gives permission to the central executive body to impose fines on distributors of prohibited production with its subsequent withdrawal from the circulation.

This examples shows that in order to effectively counter disinformation and propaganda and protect national information security from Russian information warfare, it is important to assess loopholes in the legal system and create legal mechanisms to protect the domestic information space. Other important areas where the legal framework should be evaluated are those concerning ownership and financing of the media, prevention of hate speech and false alert messaging, and the financing of political parties and NGOs.

Lesson to consider

+ Comprehensive overview of the legal system is needed in order to reveal vulnerabilities or loopholes that can be used to disseminate disinformation or propaganda. While preparing draft laws or amendments to the existing legislature, it is important to have feedback from experts in the relevant field to ensure that new regulations won't create disadvantages for citizens and business.

⁴⁴ On limiting access of foreign anti-Ukrainian printed production on Ukrainian market. *The Verkhovna Rada of Ukraine*. December 2016. Available at: <<http://zakon3.rada.gov.ua/laws/card/1780-19>>

Lesson to avoid

- The process of creating new legislation is time-consuming and requires substantial political will as well as consensus among the main actors. As such, the practical implementation of the new law is often delayed. Ukraine hasn't created a task force to analyse the existing legal framework in terms of its vulnerabilities to disinformation attacks. This means that there is no clear vision of what changes should be made going forward and what specific improvements are necessary. At present, there is no systematic approach to improving Ukraine's legal system to increase the country's information security.

LESSON LEARNT #10: Stronger together: share experience, conduct workshops, and train specialists

Propaganda and disinformation have much weaker effects on societies with high levels of awareness and resilience, including specific knowledge recognising the tactics and instruments of information attacks. In Ukraine, sharing experience and increasing public awareness is conducted on different levels.

Civil society groups inform and monitor disinformation activities, analyse them, and conducting myth-busting and debunking work. They also provide individuals with instruments for fact-checking. For example, StopFake provides a list of different online tools that help reveal whether photo or video is fake or not⁴⁵. Many start-ups also fight fake content,⁴⁶ such as Check4Spam, Factmata, Grapple Media, FightHoax, Rootclaim⁴⁷, and others. Also, StopFake shares its experience and methodology with many other NGOs and journalists. The main aim of this training is to disseminate know-how and share best practices.

Another example of information sharing concerning media literacy is a project of the Academy of Ukrainian Press and Deutsche Welle Akademie⁴⁸. The project involved workshops based on the logic of "training the trainers". The workshops took place in four different towns around Ukraine to ensure national coverage. Participants were trained how to distinguish fake news from real news, the basics of information security, and how to share knowledge of these topics in interactive and engaging ways. Overall, there is a high level of awareness among Ukrainian NGOs that deal with information security that their experience and knowledge must be disseminated to as many journalists, experts, and individuals as possible.

The Doctrine of Information Security also envisages initiatives to increase media literacy and facilitate professional training in the media sphere. According to the Doctrine, this task should be implemented by the Ministry of Information Policy, the Ministry of Education and Science, and the Ministry of Defence. For instance, the Ministry of Defence has organized several rounds of capacity building courses for its staff. The Ministry of Information Policy runs an Open Intelligence Investigation (OSINT) project and organizes OSINT training around Ukraine. Additionally, the MIP has prepared the introduction of new

⁴⁵Instruments. Available at: < <https://www.stopfake.org/category/instrumenty/> >

⁴⁶ Doing it together: overview of the startups that help fighting fake content. (2017, November 10). *Stop Fake*. Available at: < <https://www.stopfake.org/obshhimi-usiliyami-obzor-startapov-kotorye-boryutsya-s-fejkovym-kontentom/> >

⁴⁷ Startups against fakes. (2017, July, 20). *Stop Fake*. Available at: < <https://www.stopfake.org/startapy-protiv-fejkov-novyj-vzglyad-na-borbu-s-internet-lozhyu/> >

⁴⁸ Guza, Y. (2017, March 15). Trainings on media literacy available in Ukrainian cities. *Gurt*. Available at: < <https://gurt.org.ua/news/trainings/37380/> >

qualifications that can be taught at universities, e.g., communicative science (komunikatyvistyka) and media communications. The goal is to professionalise understanding of these topics within academia, as well as produce more specialists on media literacy and information security.

The plans of the Ministry of Education and Sciences regarding the implementation of this task are still unknown, but it would make sense to have media and literacy classes at schools to share knowledge with young people (the most active users of the internet). Also, experts suggest that it would be useful to amend existing university programs for future journalists to include fact-checking and media literacy in their courses.

However, what is strongly missing in these activities is a television component. As mentioned previously, the majority of Ukrainians still obtain most of their information from TV stations. So far, all fact-checking and experience sharing events are conducted online or during workshops with limited participants. Having TV programs or public awareness campaigns to share the basics of media literacy will reach wider audiences and could thus have a bigger effect than online initiatives alone.

Moreover, knowledge and experience sharing is important not only domestically but internationally as well. In this regard, the civic sector is again more dynamic than state structures. For example, StopFake and the recently founded Hybrid Warfare Analytical Centre produce analyses and investigations that are translated into foreign languages and disseminated across international networks. However, it is important to note that there remains a lack of analytical material about Russia's disinformation activities in Ukraine. Ukraine was the first target of Russia's full-scale information war and a testing ground for the techniques later used in Western states. As such, comprehensive analysis of the Ukrainian situation is invaluable for Western states that are now also combatting Russian disinformation and influence operations.

Lesson to consider

+ There should be various programs for increasing media literacy and experience sharing about countering disinformation available to journalists, civil servants, and individuals.

Lesson to avoid

- Apart from organizing its own initiatives, states should provide more support for civic projects aiming to increase media literacy, fact-checking, and experience sharing in combating disinformation. A lack of coordination leads to decentralization of activities and duplication of efforts.

Like what we do? Support us!

Use the form at: <http://www.europeanvalues.net/o-nas/support-us/>

Or send your donation directly to our transparent account: 2300405420/2010.

© Evropské hodnoty z.s. 2017

The European Values Think-Tank is a non-governmental policy institute defending liberal democracy.

Our vision is that of a free, safe and prosperous Czech Republic within Central Europe that is an integral part of the West.

We help to face aggressive regimes, radicalisation within the society, the spread of authoritarian tendencies and extremist ideologies including Islamism.

We provide decision-makers with expert recommendations and we systematically watch and evaluate their performance. We consider active citizens, accountable politicians, political parties that fulfil their role, as well as cohesive society that shares the values of individual freedom, human dignity and equal rights to be the principle elements of a functioning liberal democracy.

Since 2005, as a non-governmental and a non-profitable organisation which is not linked to any political party, we have pursued research and educational activities. In addition to publishing analytical papers and commentaries for the media, we organise conferences, seminars and training sessions for both experts and the wider public. Our events provide a platform for dialogue amongst politicians, experts, journalists, businesspeople and students.

EUROPEAN VALUES THINK-TANK

Na baště sv. Jiří 260/11, CZ-160 00 Praha 6 – Hradčany

info@evropskehodnoty.cz

www.europeanvalues.net

facebook.com/Evropskehodnoty