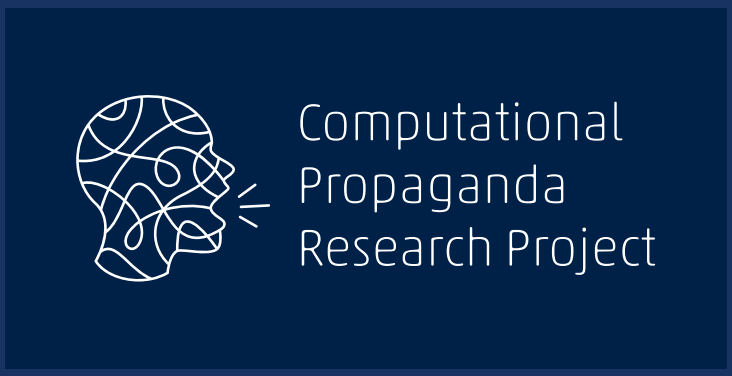


Working Paper No. 2017.9

Computational Propaganda in Ukraine: Caught Between External Threats and Internal Challenges

Mariia Zhdanova, University of Glasgow

Dariya Orlova, European Journalism Observatory

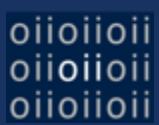


Table of Contents

Table of Figures

Abstract

This working paper examines the state of computational propaganda in Ukraine, focusing on two major dimensions, Ukraine's response to the challenges of external information attacks and the use of computational propaganda in internal political communication. Based on interviews with Ukrainian media experts, academics, industry insiders and bot developers, the working paper explores the scale of the issue and identifies the most common tactics, instruments and approaches for the deployment of political bots online. The cases described illustrate the misconceptions about fake accounts, paid online commentators and automated scripts, as well as the threats of malicious online activities. First, we explain how bots operate in the internal political and media environment of the country and provide examples of typical campaigns. Second, we analyse the case of the MH17 tragedy as an illustrative example of Russia's purposeful disinformation campaign against Ukraine, which has a distinctive social media component. Finally, responses to computational propaganda are scrutinized, including alleged governmental attacks on Ukrainian journalists, which reveal that civil society and grassroots movements have great potential to stand up to the perils of computational propaganda.

.

Introduction

Oxford Dictionaries named the term "post-truth" the word of 2016. Since then, public attention to the concept has been increasing exponentially. While the term became popular in Western public discourse just recently, the case of Ukraine, an Eastern European country in between Russia and the EU, represents a vivid example of how "post-truth" circumstances have shaped developments in an entire country for the past three years.

Since the EuroMaidan revolution and Russia's annexation of Crimea, Ukraine has turned into the frontline of numerous disinformation campaigns in Europe. Many of such campaigns have had a significant internet component, involving social media to spread and promote a certain narrative. Some of the disseminated fake stories – such as the tale of a "crucified boy" (StopFake, 2014a; Nemtsova, 2014) or the story about Ukrainian soldiers being paid with "two slaves and a piece of land" (StopFake, 2014c) – have turned into textbook examples of how propaganda works. Other stories conveying peculiar narratives such as "weakness of the EU" or "migrants destroying Europe" have been circulated all over Europe.

As one of the first countries to face a serious disinformation crisis in the present day, Ukraine represents a curious case for the study. The combination of factors for exploration is quite unique. In the course of the past three years, the country has lived through a massive uprising against the corrupt and authoritarian regime, annexation of part of its territory by a neighbouring country, eruption of armed conflict in the eastern provinces instigated by external forces, severe economic crisis, political turmoil, ongoing transition and painful reforms. All these challenges have been accompanied by the rapid development of information technologies and growing internet use, which has significantly contributed to the shaping of developments in the country.

Past Research and Previous Understandings

Given the scale of the conflict between Ukraine and Russia, and the salience of the information struggle dimension therein, the issue of propaganda and disinformation campaigns has

attracted a lot of attention from the media and scholars alike. Lucas and Nimmo (2015) explored general tactics used by the Russian state-controlled TV channel RT and the news agency Sputnik in conveying the Kremlin's narrative, while Meister (2016) analysed their influence on Western audiences. Lucas and Pomerantsev (2016) described a variety of techniques used by the Kremlin in disinformation campaigns. Hoskins and O'Loughlin (2015, p. 1320) used the case to discuss the nature of new types of present-day conflicts that are "characterized by the appropriation and control of previously chaotic dynamics by mainstream media and, at a slower pace, government and military policy-makers".

Fewer efforts, however, have been made to analyse technological tools employed to erode public discourse. Kelly et al. (2012) suggested most actors were using tactics of marketers and PR specialists online to spread their messages, while content analysis of tweets from Russian Channel One about Ukraine concluded the aim was to blur the border between lies and reality (Khaldarova & Pantti, 2016). Bērziņš et al. (2014) suggested that the Russian government's established control over media outlets has slowly turned to social media in the form of government-controlled internet "trolling", which remains a largely under-researched phenomenon.

The issue of computational propaganda in the Ukraine–Russia conflict has been predominantly addressed by journalists. Reports suggested that large troll factories have been actively used to create blogs, social media posts and comments to spread certain narratives. In September 2013, a Russian journalist from Novaya Gazeta started working at the Russian troll factory in Olgino to investigate the daily operations of the company (Garmazhapova, 2013). In October 2014, St Petersburg based online magazine Dp.ru suggested the same agency employing around 250 people was actively engaged in online discussions about the Ukraine crisis with a goal to undermine the authority of Ukrainian politicians and post hate speech and fake stories, thus shifting attention from the real events (Butsenko, 2014). Finally, in 2015, the *New York Times* proved that the Russian Internet Research Agency, the same infamous Olgino factory, was also producing fake clones of news sites, fabricating videos and attempting to influence US politics through disinformation (Chen, 2015). In March 2017, journalists from RBC company described a new phenomenon, the "Russian media factory", which combined 16 websites licensed by Roskomnadzor (the federal executive body overseeing media in Russia), with a total audience of over 36 million unique users creating stories on current events and political figures such as Trump, Putin and Poroshenko (Zakharov & Rusyaeva, 2017).

Less research has been focused on computational propaganda within Ukraine, the country's counterpropaganda attempts or the issue of internal manipulation of public opinion. Several media reports concluded that numerous political actors in Ukraine utilize different online means to attack opponents and promote their own agenda (Ivantsova, 2015; Kriukova & Pasiutina, 2016). It is noteworthy, however, that there is significant confusion in terminology around computational propaganda in Ukraine. It is quite common to see the terms bots, political bots, trolls and fake accounts used interchangeably in media reports, and even in the discourse of professionals directly engaged in providing social media management services. Thus, this working paper will start with the definition of the key terms.

Explanation of Terms and Variables

Computational propaganda is the "assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion" (Woolley and Howard, 2016, p. 4886). One example of such agents are bots – automated software operating online. Depending on their functions bots may be categorized into general, social and political. The purpose of general bots (also called "crawlers") is to gather information, while social bots operate on social media platforms and can interact with real users by sharing messages and engaging in comments, etc. Political bots, per Woolley and Howard (2016, p. 4885), are the "algorithms that operate over social media, written to learn from and mimic real people so as to manipulate public opinion across a diverse range of social media and device networks". When talking about bots this working paper will use the definition of political bots operating online (through social media, blogs, in the commentary sections of popular websites, etc.). Hiding their bot identity, automated systems promote certain ideas to create heated debates online, and according to Hegelich and Janetszko (2016) may be considered a new political actor in the Russia–Ukraine conflict. Thus, it is important to examine not only the ways bots can engage in political conversations and the scale of such activities, but the potential impact on policy making.

Methodology

This working paper explores peculiarities of computational propaganda in Ukraine through interviews with experts and actors involved in the online communication industry, as well as analysis of secondary data. Examination of context and existing literature on the use of bots and other digital tools in Ukraine prompted the following research questions to be addressed by the study. Our first research question is: "How are bots and other tools used for online political communication in Ukraine?". Secondly we would like to find out how Ukraine has been dealing with Russian propaganda online against a backdrop of ongoing conflict.

In order to understand how computational propaganda works in Ukraine, face-to-face interviews with 10 experts (digital and social media specialists, academics, journalists, activists, etc.) and several informal conversations were conducted in Ukraine. Background research on the issue helped identify major platforms, tools and strategies for political communication on the web. Quantitative data was also analysed, namely a number of bots and fake accounts among the Twitter audience of popular Ukrainian news websites.

The working paper begins with an overview of the general context of the case study, explaining the major transformations in Ukrainian society and outlining key political actors, media ownership structure and the history of computational propaganda in Ukraine. The contextual part is followed by detailed analysis of distinctive examples of its use.

Case Context

Ukraine's recent history has been characterized by dramatic events, crucial challenges and dynamic changes across political and social landscapes. The EuroMaidan revolution that swept across Ukraine between November 2013 and February 2014 dramatically changed the

Ukrainian political and social landscape and triggered crucial transformations in the country. The three-month stand-off between protesters and government forces left over one hundred people dead, most of them pro-Maidan protesters. Then-president Viktor Yanukovych, whose last-moment decision to suspend signature of an association agreement with the European Union prompted initial EuroMaidan rallies, fled the country; the Ukrainian parliament created a new coalition, appointed a new government and called for presidential and parliamentary elections that eventually took place in May and October 2014, respectively.

Right after Yanukovych's escape, pro-Russian militants seized the key buildings and parliament of Crimea, a Ukrainian peninsula in the Black Sea inhabited by a Russian-speaking majority. Military personnel without insignia occupied Crimea, the dubious and internationally unrecognized public vote was held in March 2014, bringing pro-secession results, and this was followed by Russia's formal annexation of Crimea. The situation was exacerbated in other parts of the country, especially in the industrial region of Donbas, when Russia-supported militants seized government buildings in some oblasts of Donetsk and Luhansk, following the "Crimean scenario", and created the so-called Donetsk and Luhansk People's Republics in May 2014. The conflict turned into a fully fledged war involving the Ukrainian army, separatist forces and Russian troops, as numerous reports show. While ceasefire agreements were signed in Minsk in September of 2014 and February of 2015 and the situation stabilized somewhat, minor skirmishes continue in the conflict area. Part of Ukraine's territory remains under the control of pro-Russian separatist forces and Crimea has been annexed by Russia.

The conflict between Ukraine and Russia has been characterized by a fierce stand-off in the realm of information. Following EuroMaidan and throughout the conflict, Ukraine has been targeted by numerous disinformation campaigns and propaganda efforts, predominantly from Russia (Snegovaya, 2015; Khaldarova & Pantti, 2016; Nygren et al., 2016).

The post-Maidan internal transition of Ukraine has been marked by political instability, a high level of political competitiveness (Way, 2015), dynamic development of civil society (Solonenko, 2015) and "democratization" of communication between political elites, civil society and citizens. In this context, the significance of political communication online has been increasing in Ukraine, giving way to new approaches and tools (Novoye Vremya, 2016).

Political actors

The presidential and parliamentary elections that followed the victory of EuroMaidan brought a new reconfiguration of political elites in power. Petro Poroshenko, a rich Ukrainian oligarch with multiple businesses, including his most famous confectionery company Roshen, was elected as president of Ukraine. His election agenda emphasized pro-European aspirations and promises of reforms. Poroshenko's political force, Petro Poroshenko Bloc, also gained many seats in the Ukrainian parliament, 132 out of 450. The second-largest faction of parliament is represented by the Narodny Front party. The two forces made up the core of the post-Maidan parliamentary coalition and formed the government. The other parliamentary factions are represented by: the Samopomich party headed by the mayor of Lviv city, Andriy Sadovy; Opposition Bloc, a rebranded Party of Regions that had been a ruling party during the Yanukovych presidency; and Yuliya Tymoshenko's Batkivshchyna and Radical Party of Ukraine. While the political environment remains highly competitive and unstable in Ukraine,

President Poroshenko is believed to have quite strong control over the government and a parliamentary majority, although even his own faction has several informal groups with opposing standpoints on many crucial issues.

It is also important to note that the Ukrainian political landscape has long been dominated by the oligarchs and financial and industrial groups. While this pattern has been broadly criticized as being an obstacle to Ukraine's transition to democracy, free market and rule of law, it has also secured the so-called pluralism by default in Ukraine (Way, 2015). Oligarchs have largely kept their leverage in post-Maidan Ukraine, although the dynamic political situation is characterized by occasional reconfiguration of powers and loyalties in the political establishment. Consequently, major political players have been ploughing money into all sorts of self-promotion campaigns, including "black" PR campaigns against opponents in search of a stronger standing for themselves.

Media ownership and structure

Much like the political landscape, Ukraine's media market has long been dominated by the oligarchs. Over three-quarters of the television market is divided between four media groups owned by the oligarchs (KAS, 2015), a striking figure given that television remains the number one media outlet for the majority of Ukrainians (Internews, 2016). Inter Media group, which comprises the popular INTER TV channel and a number of smaller TV stations, is reportedly controlled by oligarch Dmytro Firtash and a former head of Yanukovych's presidential administration, Serhiy Lyovochkin. Another popular TV channel, 1+1, is owned by oligarch Ihor Kolomoysky, who also controls several smaller channels, UNIAN news agency and a few online outlets. Viktor Pinchuk, a businessman and son-in-law of ex-president Leonid Kuchma, owns a set of TV channels (STB, ICTV and Novyi). The country's richest man and a close ally of ex-president Yanukovych controls a bunch of national and regional media, including the popular nationwide TRK Ukrayina TV channel and a Segodnya daily. The current president himself owns a smaller TV station, 5th Channel.

The Ukrainian media market has seen a critical lack of foreign investors, especially after the financial crisis of 2008 when a number of foreign publishers left the press industry. While mainstream media remain under the control of oligarchs, smaller independent media outlets have been contributing to media pluralism in Ukraine. Some of those media have been profitable as businesses, like one of the most popular news websites, Ukrayinska Pravda; others have been relying on crowdfunding and grant support, like Hromadske TV.
Ukrainian TV and radio channels are regulated by the National Council for TV and Radio Broadcasting. In March 2014, due to the conflict with Russia, the council advised all cable operators to stop transmitting a number of Russian channels (Ennis, 2014). The number of Russian channels that have the right to broadcast in Ukraine has decreased from 72 in 2014 to 14 in 2016 (Dzerkalo Tyzhnia, 2016). Later the Ukrainian regulator issued a recommendation to ban Russian-made content that praised "special forces" and symbols of the "aggressor state", which included many films and TV series (BBC, 2016a).

Social media and internet penetration

EuroMaidan marked a milestone in the use of social media and information technologies for the purposes of political activism and contributed to the rapid rise of the significance of social network sites in the country at large, which has been examined by scholars (Bohdanova 2014; Dickinson 2014; Onuch, 2015; Gruzd & Tsyganova 2015).

According to the Factum Group Ukraine (Factum Group Ukraine, 2017), 63 percent of the adult Ukrainian population today are considered active internet users. In addition to information sharing, social networks in Ukraine are being actively used for fundraising, e-commerce and data gathering. However, social media have also become platforms for disinformation campaigns and efforts to manipulate public opinion.

The most recent survey data suggests that almost 21 percent of Ukrainians use social media as their main source of news (Detector Media, 2017). The most popular social media networks in Ukraine are VKontakte, or VK, (11.9 million users), Facebook (over 8 million users), Odnoklassniki (5.7 million users) and Twitter (2.5 million users). Since two of the networks (VK and Odnoklassniki) are owned by Russian companies, it is important to underline the Russian desire to influence and control social media in relation to the crisis in Ukraine. StratCom's March 2015 report documents vivid examples of such attempts: from blocking of pro-Ukrainian groups on social networks, requesting personal information of activists, and government-initiated internet trolling to the recruitment of the volunteer fighters for Donbass online.

Bot-proof mediums?

All popular social networking sites in Ukraine can be used to deploy bots. The difference is in the cost of production and the popularity of such services. The easiest and the cheapest platform for the creation of bots is VK, since it does not have strict security measures, allowing the easy registration of mass accounts. In addition, VK is considered to be focused around groups and close communities, celebrities and entertainment, so the phenomenon of political bots on this platform in Ukraine is not that visible.

Twitter takes second place in this rating, being open for bot creation and not very effective at banning suspicious activity, according to a software developer working with the platform. Unsurprisingly, a significant amount of the overall activities on Twitter are generated by bots, with about 48 million accounts (15 percent of all users) being bots rather than people (Varol, Ferrara, Davis, Menczer, & Flammini, 2017).

Facebook, on the other hand, proves to be the most efficient in terms of protecting its API and user data, making it the most challenging environment for bot creators. Since this network is also the most popular among social and political elites in Ukraine (Orlova & Taradai, 2016), bots on Facebook are the most expensive to create, and demand for them is growing. The bot developers we talked to as part of this research managed to create a large bot farm using a script that not only registers accounts, but can automatically fill in profile information and create posts. It is easier to register female bot accounts on Facebook using pictures of models and good-looking girls from the social network VK since they will get an organic following as well. The program also allows the creation of bot accounts to like posts of certain people or

groups or on specific topics. One way to detect these bots on Facebook is to check whether they have liked or reacted to the comments left under the posts, our informant revealed.

Messengers are being called "the new social media" and their use in Ukraine is also growing. The most popular are Skype (94 percent) and Viber (84 percent), while 69 percent of all messenger users still use ICQ. Numbers for WhatsApp and Telegram are considerably lower, with 46 percent and 24 percent of users respectively (IVOX, 2016). This is an important observation since both technical and marketing specialists view them as platforms for personalized communication where the efficiency of bots would be minimal, since the architecture of the platform does not create a fruitful environment for bots to use. The only exceptions are chatbots that can simulate human conversations and are marked as robots from the beginning of their existence.

A number of companies in Ukraine provide social media monitoring services that can potentially be used for computational propaganda prevention. The market is evolving, with key players being the YouScan.io, ContextMedia, NoksFishes, SemanticForce and InfoStream agencies. They can measure the online presence of people and brands, track negative feedback and drive brand conversation online. The ability of such services to track bots and fake accounts, however, is very limited and it seems that there is currently no demand for such identification.

Bots, Trolls and Fake Accounts as Instruments of Online Manipulation of Public Opinion in Ukraine

While the information struggle has been extremely fierce externally, with numerous aggressive media campaigns generated against Ukraine (Khaldarova & Pantti, 2016), the internal information sphere has also seen the increased use of social media as a platform for attempts to manipulate public opinion.

In January 2015, the Ukrainian website dedicated to media and technology news, AIN.UA, published an interview (AIN.UA, 2015) with the so-called former "Akhmetov's bot", a young man who claimed to have worked for the company that managed the online presence for one of Ukraine's biggest oligarchs, Rinat Akhmetov. In the interview, which became one of the first stories presenting first-hand evidence on organized trolling online in Ukraine, the self-confessed "troll" told of the daily instructions he and his colleagues received on what kinds of comments to make and where they had to publish them. Although the outlet and the hero of the story himself frequently used the term "bot" to describe their activities, in reality these "bots" turned out to be fake accounts managed by paid-for people.

The experts interviewed admitted that there have been multiple such cases in Ukraine, with an entire industry of various services developed for the purposes of political communication. However, contrary to common belief, the use of bots and trolls in Ukrainian sociopolitical life is not a recent phenomenon. An industry of computational propaganda in the country emerged in the early 2000s with the rise of internet usage. Marketing and PR professionals were the first ones who started employing such services, the interviewed experts noted. As soon as Ukrainian customers turned to the internet for recommendations and product reviews, agencies

started hiring people to create fake accounts and write fake positive comments. One particularly notable segment for such campaigns, one of the interviewed experts observed, was young mothers, as they not only were interested in participating in online conversations, but also wanted to earn money while looking after their children at home.

Later on, the concept of paid comments through fake accounts was adopted by political technologists. They operated on the forums or in the comments sections of popular news websites, the most popular being Ukrainska Pravda. Similar activities have also been registered on LiveJournal – a popular blogging platform in Russia and Ukraine with a strong political content. In the popular slang those paid commentators are widely referred to as "trolls" in Ukraine. Nowadays, social media have become the primary platform for such campaigns.

Typical communication campaigns online

Interviews with experts suggest that bots and fake accounts constitute an essential element of online communication campaigns in Ukraine, but that these also involve some other crucial components. Our analysis shows that a typical campaign used for the purposes of self-promotion, discrediting of opponents and promotion of certain issues/decisions has several stages. It usually begins with the initial publication of the key message packaged into a story in some online outlet as an entrance point for the campaign. It is made possible because a large number of Ukrainian online media that deal with news and politics publish stories for money. In some cases, such initial messages are posted on social media platforms or blogs. After that, the topic is picked up by opinion leaders with a large number of followers on social media and boosted through fake manual or automated accounts. Usually, all these stages are cash-driven. Once the issue gets significant publicity online, it is very likely to be picked up by mainstream media, including major TV channels. It is thus possible to conclude that bots and fake accounts are part of a broader network of media tools employed by political actors.

Inside the industry

Stakeholders interviewed for this working paper acknowledged the large scale of employment of bots and fake accounts to manipulate public opinion online in Ukraine. The market for such services seems to be particularly driven by political actors. Interviewed experts noted that the market is diverse and horizontal in Ukraine, in contrast to the Russian one. While the market is quite big given the high demand for such services, it is also quite disguised.

As part of the project, we managed to establish contact with several market insiders, but they refused to identify their companies due to sensitivity of the issue. According to the information obtained, a large part of the market is represented by small and medium-sized companies without a public profile. Some interviewees suggested that digital agencies also provide services related to political social media management that involve paid-for commenting and audience boosting through bots, etc. However, established agencies do not openly promote their expertise in such services.

One of the interviewed stakeholders who owns a small company of his own noted he usually gets political clients from intermediaries. Typical tasks involve promotion of a politician or

political force online, distribution of certain messages, neutralization of negative information or an attack on clients' rivals. Many projects are related to election campaigns; sometimes the company provides a "package" of services, or deals only with specific cases, for example a scandal. Once there is a project, the owner of the company hires a team, usually targeting students. The team receives guidelines on what they are supposed to do, for example boost certain posts by reposting with the help of the established database of fake accounts. If needed, they also get engaged in commenting (spreading certain messages or neutralizing others). Such commentators are usually expected to post up to 200 comments each day, the informant said. During the 2012 parliamentary election campaign they received about US$100 per week. All the discussed activities are conducted with the help of fake accounts that are manually maintained. According to the owner of this small company, his database of fake accounts, which includes several hundred "advanced" accounts on Facebook and VKontakte (meaning accounts that have up to 5,000 friends), is an asset in its own right and can be sold any time.

Conducted interviews, as well as media reports, suggest that major political parties have created internal divisions within their offices/headquarters that deal directly with social media (Ivantsova, 2015). Such divisions are led by political consultants/advisors who develop key messages and a plan for their distribution across different communication channels. Sometimes in-house SMM departments also outsource some of their projects to independent companies, like the one described earlier. This happens, for instance, if they need some extra capacity in times of crisis.

Analysis shows that manually maintained fake accounts are one of the most popular instruments for online campaigns due to their relatively small cost and flexibility, since they can be used for boosting pages/posts/links through likes and rigorous commenting. Automated bots seem to be less widespread in Ukraine, although our study identified several market players who developed technological solutions for bots. An informant asserted that there is a leading company in Ukraine that creates bots and sells them across the world, but did not specify which one.

Popular myths

As mentioned earlier, despite there being quite a developed market, there is significant confusion regarding bots, trolls and other instruments of computational propaganda in public discourse, as well as myths about the industry. Firstly, the terms are often confused, which reveals a lack of understanding. Many people believe computational propaganda is either fully manual or completely automated, while in reality it can be a mixture of both. The second myth suggests that bots used for political purposes are cheap, while PR services are more expensive. In fact, correct and effective automation is time- and resource-consuming, and hiring a software developer is much pricier than using paid-for commentators. The final popular assumption among the public concerns the inability of bots to influence public opinion. While there may not be direct impact, bots constitute a big threat to those working with big data (Hegelich, 2016). Since most PR, marketing and political campaigns rely on primary research and market data, it is often hard to assess quality, as analysis of social media narratives, audience reach of certain pages and people becomes inaccurate due to the increased volumes of fake and automated accounts.

Fake accounts

Out of the variety of tools, manually maintained fake accounts seem to be the most widely used in Ukraine. Fake accounts play a critical part in the chain of tools used to boost attention to certain topics or messages in social media. Hundreds of such accounts are easily bought online. The price of Facebook accounts in Ukraine varies from US$0.90 to US$200 depending on the year of registration, previous activities and level of profile completeness (bio, pictures, friends, etc.). Twitter accounts cost US$0.40 to $90, and VK accounts are the lowest at US$0.40 to US$1.50. Popular websites for such services are https://buyaccs.com/, http://darkstore.biz/ and others. However, these services do not provide a guarantee and purchased accounts can be easily blocked by the social media platforms themselves due to suspicious behavior, for example an account on Facebook registered in the US and reactivated in Ukraine will require a security check that can only be tricked with certain computer expertise, which buyers of such fake accounts do not always have. In addition, fake accounts are most often used for manual commenting and are not likely to be turned into automated bots. Therefore, it is plausible to conclude that fake accounts are predominantly used to promote certain messages or trivialize or hijack the debate online.

Bots

Automation of media, political communication and propaganda also takes place in Ukraine. However, this tool is rather under-researched compared with paid commentators and fake accounts. Interviews and secondary data suggest the following types of bots can be distinguished:

Impact bots – used to create a mass following for certain pages or persons and to establish a bigger presence online. Most popular on Twitter. Usually inactive and easily detained by programs such as BotOrNot, StatusPeople, TwitterAudit, etc. We have analysed five of the most popular accounts on Ukrainian Twitter according to SocialBakers stats. The percentage of bot accounts in their audience varies from 1 percent to 14 percent according to StatusPeople, and up to 72 percent of the audience consists of inactive accounts, and thus it is difficult to determine their bot identity. The high percentage of bots can be explained by the periods of active bot registration on Twitter after the start of the EuroMaidan protests in 2013 and the armed conflict in eastern Ukraine in early spring 2014 (Alexander, 2015b).

Amplifiers – used for liking, sharing and promoting certain content. These operate on all social platforms in Ukraine. Journalists from the online outlet Texty.org.ua conducted an investigation and uncovered an organized network of bots on Facebook operated from Russia that pretended to be Ukrainian patriots and spread information calling for the third Maidan, an uprising against the government (Romanenko, Mykhaylyshyn, Solodko, & Zog, 2016). Examples of automated accounts for promotional and quite probably propaganda purposes on Twitter include @schancellery, @laraz1377 and @IvanPetrov_34.

Complainers – some clients of Ukrainian bot developers also request blocking of certain accounts with the help of complaints lodged by bots. Even though Facebook itself does not allow banning of a user without giving reasons, complainers may monitor the posts of other accounts for certain terms that do not comply with Facebook policy and send ban requests.Trackers – used for detection and driving attention towards certain behaviours online.

As an example, in July 2014 Twitter bots were launched to track anonymous edits in Wikipedia from Russian (@RuGovEdits) and Ukrainian (@UAGovEdits) government IP addresses. Among others, the bots helped track attempts to rewrite an article on MH17 in the German version of Wikipedia (Rothrock, 2014).

Service bots – often defined as software or scripts that can help automate the process of bot account registration. For instance, they can automatically generate names or email addresses or read CAPTCHAs. Together with external services for obtaining virtual cell phone numbers in order to receive an SMS for account creation, service bots may help create a bot account on Facebook within four minutes, our informant revealed. More advanced versions of such software may even automate creation of fake photos of ID documents that can be sent to Facebook as proof of user authenticity if the bot user is blocked.

The use of amplifier bots for content promotion purposes creates a misleading narrative for the users, who will only see a certain part of the story or a particular angle. For instance, the message "I think big war is coming" was widely shared at the time of active military action by Russian-backed rebels in the cities of Schastya and Artemivsk in eastern Ukraine (Alexander, 2015c).

A study by Alexander (2015a) revealed an average retweet rate for Russian media by bot accounts on Twitter is 20 percent. Some commentators claim impact bots are used for search engine optimization (SEO) purposes only. This claim is debatable because tweets produced/retweeted by bots do not always contain links to any articles (which would be necessary for SEO). It is more likely that they are used to abuse the trending topics section on Twitter. The official policy of the social network does not allow this: "Repeatedly Tweeting the same topic or hashtag without adding value to the conversation in an attempt to get the topic trending or trending higher; Tweeting about each trend in order to drive traffic to your profile or website, especially when mixed with advertising".

Impact and amplifier bots on Facebook are much more difficult to create, and therefore they are more valuable. According to one of our informants, Facebook bots are in large demand for the purposes of PR and political communication in Ukraine. One automated account can reach a target of gaining the maximum 5,000 friends limit within a three-month period. Facebook itself promotes such accounts through its "You may also know" section. Therefore, 100 bots in the audience of a certain person can achieve access to hundreds of thousands of new users. When bots suggest liking this or that page to their "friends", conversion is quite high, which makes the use efficient. Most pages of Ukrainian politicians on Facebook have seen a suspicious boost in the audience numbers, according to the Ukrainian monitoring resource Zmiya. However, it remains unclear whether the politicians themselves are ordering such boosts, or whether it is an initiative of their advisors, digital agencies providing social media management services or external forces such as opponents trying to manipulate the numbers of real followers.

One industry insider provided an interesting scenario of how Ukrainian PR consultants would use the information conflict with Russia to pursue their own agendas. For instance, if there is an unpopular decision that needs to be made by an MP or a new bill, they could use paid

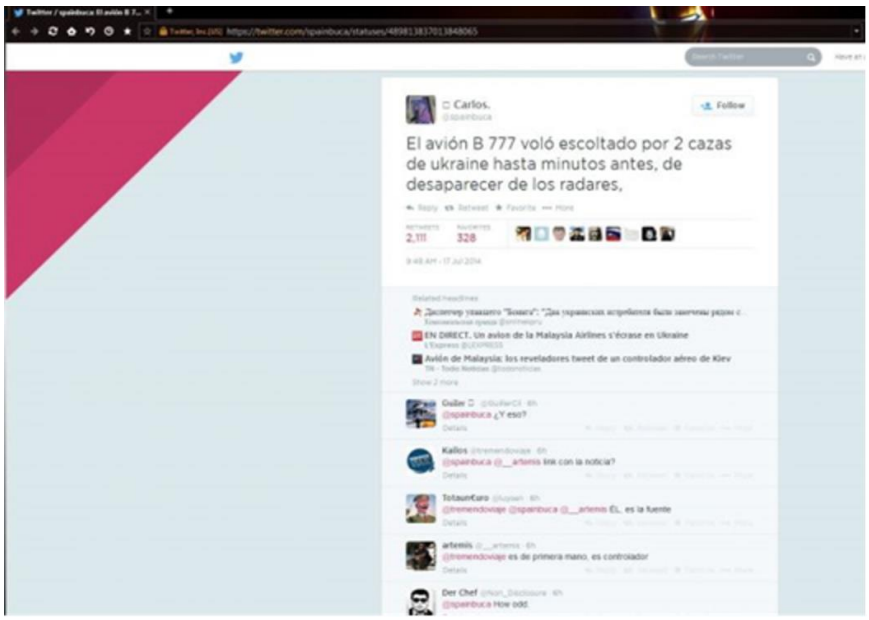
commentators or automated bots to spread negative messages about this MP and the project. Screenshots with often identical messages would then be sent to the press saying this MP is a target of Russian propaganda and the infamous Olgino trolls. Such publicity would thus work in favour of a "victim of Russian disinformation games" and his or her ideas, according to the industry insider.

Complexity of the issue: the case of MH17

A remarkable example of computational propaganda operations is the notorious case of the MH17 tragedy. On 17 July 2014, a Malaysian Airlines Boeing 777 crashed into fields in Donbas in an area not under the control of the Ukrainian government, causing the death of all 298 people on board (BBC, 2016b). In September 2016, a joint investigation team presented the first results of its investigation, concluding the MH17 was shot down by a BUK surface-to-air missile fired from Russian-backed, separatist-controlled territory in eastern Ukraine (JIT, 2016). Prior to release of the official version, the case was subject to many conspiracy theories (Shandra, 2015), such as one claiming a military jet downed the passenger Boeing (Higgins, 2015).

This theory was initiated by tweets of an alleged Spanish air traffic controller named Carlos (@spainbuca) working in the Kyiv Boryspil Airport, who claimed to have seen a military aircraft in the area of the catastrophe.

Figure 1: Tweet from Fake @spainbuca Account

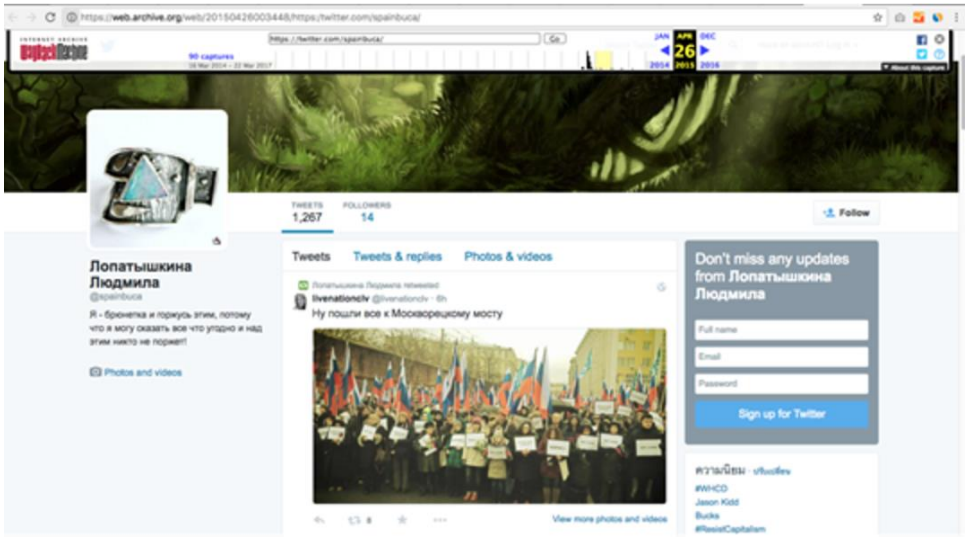


Source: author's screenshot, 16 June 2017.

The story was quickly picked up by the Russian channel RT as well as many other news outlets, such as RIA Novosti, Tass and others. On 21 July 2014, Russia's Ministry of Defence held a press conference presenting a statement (Ministry of Defence, 2014) and a fake satellite image suggesting an Su-25 fighter jet had been spotted near the Boeing (Kivimäki, 2014). Later on an investigation conducted by the fact-checking website StopFake proved that the account of the so-called Carlos was fake, because non-Ukrainian citizens are not allowed to work as flight operations officers in Ukraine (StopFake, 2014b). Soon the @spainbuca

account was blocked, but it reappeared in late 2014 under the name of Lyudmila Lopatyshkina (The Insider, 2016).

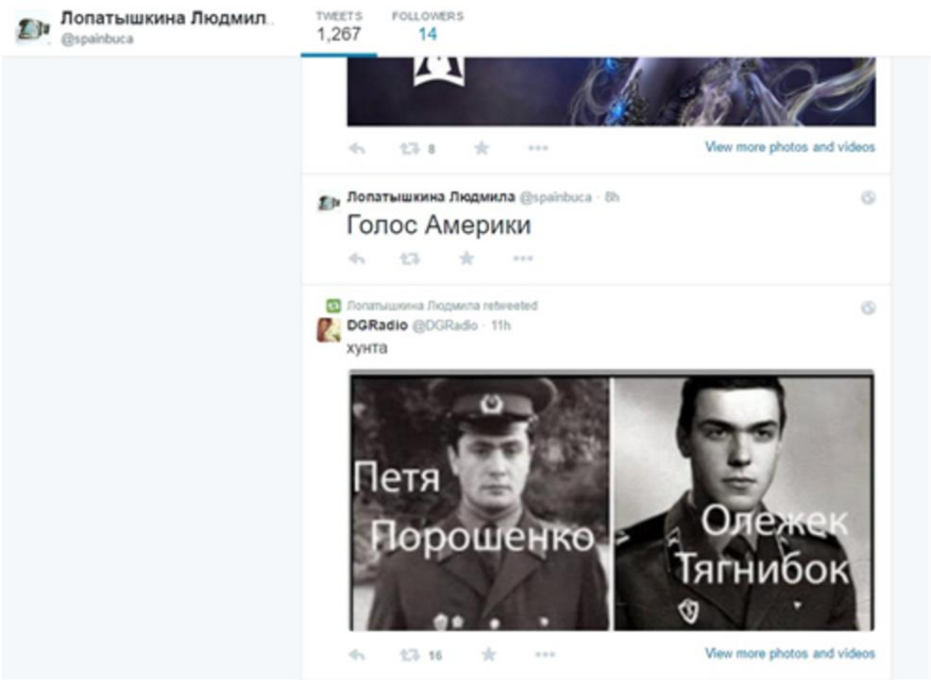
Figure 2: The Lyudmila Lopatyshkina Account



Source: author's screenshot, 16 June 2017.

Many assumed this account to be a bot tweeting out anti-Ukrainian messages and images, which caused its complete suspension later on.

Figure 3: Tweets from the Lyudmila Lopatyshkina Account



Source: author's screenshot, 16 June 2017.

Research by the Ukrainian deputy minister of information policy shows an account of the so-called Carlos was registered during the active phase of the EuroMaidan revolution in February 2014 and actively retweeted pro-Russian messages. This was most active on 2 May 2014, almost two months in advance of the MH17 case. On 8 May 2014, a person calling himself Carlos gave an interview to the Spanish version of RT, accusing Ukraine of aggression and hatred, but his face was covered up and no proof of the existence of such a person has been found (RT, 2014). This fake account became active once again in July 2014 to produce one of the strongest fake theories of what had happened to the MH17 flight.

Bots were also actively used to help block Facebook accounts of journalists posting about the MH17 case. One such incident happened with a journalist called Sergey Parkhomenko, whose account was temporarily suspended. Comments from the experts suggest bots have been used to send thousands of complaints to Facebook's abuse team to cause blocking of certain opinions online (Novaya Gazeta, 2015).

In September 2016, when the official results of the MH17 investigation were presented, a Twitter user named @TimurKhorev spotted a second increase in bot activity. He noticed a certain pattern: each time somebody used the #MH17 hashtag in tweets in Russian, a bot would join the conversation and reply with a link to a fake article questioning the results of the investigation. A number of users have proved the theory to be correct and demonstrated how the bot reacted to messages that had nothing to do with the context but simply contained the #MH17 tag (Online.ua, 2016). Automated accounts were also actively promoting certain messages related to the story (such as this one). Media expert and director of Mohyla School of Journalism Yevhen Fedchenko suggests the case of MH17 illustrates how tools of computational propaganda become powerful and effective when supported by other actors – journalists and government officials.

Ukraine's Response to Computational Propaganda

External responses

Analysis suggests that the Ukrainian government's response to the external threats of propaganda within the context of the Ukraine–Russia conflict has been quite sporadic and weak. Representatives of and advisors to the Ukrainian government claim they do not have the necessary funds to conduct comprehensive monitoring of the online sphere, develop appropriate software or create and manage accounts that would "fight" with Russian bots online. In January 2015, the Ukrainian Ministry of Information announced its "Internet Army" project – a voluntary initiative aimed at "fighting back Russian occupants in the information war" (Yarovaya, 2015). Media reports suggested that almost 40,000 people registered as "information soldiers" with the ministry. However, our interviewees indicated the "Army" did not exist in the first place, since the volunteers did not receive any particular tasks. Therefore, effectiveness of the project is quite dubious.

Response from media and civil society

More rigorous attempts to respond to Russian computational propaganda have been undertaken by civil society and media initiatives. For instance, the StopFake.org project – a

website launched by students, professors and alumni of the Kyiv-Mohyla School of Journalism in March 2014 – has debunked over 1,000 fake stories produced mainly by the Russian media. Activists of the project have been relying on fact-checking and news verification to deal with news content in mainstream media, but they have also tackled disinformation in social media.

The issue of Russia's disinformation campaigns against Ukraine has received significant public attention in Ukraine, even resulting in private initiatives aimed at fighting propaganda. For instance, a Ukrainian software developer nicknamed Alex Novodvorski developed an extension for the Chrome browser that allowed automatic blocking of thousands of Russian websites (Forpost, 2017).

Ukrainian media have also been trying to investigate computational propaganda, with Texty.org.ua producing the most impressive example. This analysed the network of accounts that purposefully disseminated messages to instigate public unrest, the so-called third Maidan.

All in all, Ukraine's response to Russian computational propaganda has been decentralized and largely driven by civil society, whereas investigations from St Petersburg's troll HQ suggest a high level of organization and vertical structures.

It is not only external threats of computational propaganda that have attracted the attention of Ukrainian civil society and media. Increasing attempts to manipulate and erode public discourse online through organized communication campaigns have not gone unnoticed. Ukrainian journalists and experts have been acknowledging the toxic influence of paid commentators from fake accounts on public discourse. Thus, a recent survey of media professionals showed that 56 percent of respondents believe in pro-government manipulation in online debate (Internews, 2017).

One of the most notorious cases occurred in July 2016. It began with a post on the Facebook page of the press service of Ukraine's anti-terror operation, which accused journalists from Hromadske TV of smuggling a Russian journalist to the frontline in eastern Ukraine and exposing the position of Ukraine's troops. The journalists denied both claims and provided evidence of their innocence. However, they faced an avalanche of attacks from Facebook users. In her op-ed piece published in *The Guardian*, Katya Gorchinskaya (2016), an executive director of Hromadske TV, noted that, "As soon as the statement on their Facebook page appeared, something strange started to happen. In the first five minutes, the statement was shared more than 360 times. Within an hour, it became the most popular post on the joint staff's press page", adding that a typical post on the page received a few dozen likes and shares, whereas that post "spread like a forest fire". "Reposts trashed our journalists, attacking their reputations and slamming their work", Gorchinskaya wrote, suggesting that Hromadske TV was hit by pro-government commentators due to the independence of the medium and its frequent criticism of the government.

Even though this story was much discussed in the media, there was no factual evidence of the involvement of bots and no particular countermeasures have been taken. However, a number of Ukrainian journalists have experienced attacks via comments, especially under posts

criticizing various political actors. One of the interviewed experts, the former deputy minister of information policy, Tetyana Popova, also said she was targeted by pro-Russian bots and even received death threats on Facebook. She reported the incident to cyberpolice, but they do not deal with such complaints.

The most recent counter-measure taken by the Ukrainian government involved a ban on Russian web services and social media networks in Ukraine, for example VK, Odnoklassniki, mail.ru and Yandex (BBC, 2017c). Similar to the blocking of Russian TV channels in the country, the legislation comes as part of Ukraine's sanctions against Russia. President Poroshenko admitted the government's attempt to use social networks to fight Russia's 'hybrid war', but "the time has come to act differently and more decisively" (Luhn, 2017).

Conclusion

Analysis of Ukrainian cases revealed a number of curious trends in the use of computational propaganda. Given a complex political context, both external and internal, the study focused on two major dimensions: the use of bots in political communication inside the country and Ukraine's response to the challenges of computational propaganda caused by the Ukraine–Russia conflict.

Our findings suggest the internal market of online political communication in Ukraine is quite diverse and horizontal, with many players, but mostly hidden. Evidence of the variety of tools used for online information campaigns has been obtained. The main purposes of the utilization of computational propaganda tools include not only manipulation of public opinion, but often discrediting opponents and defending the interests of different business and political groups. Many still rely on manually maintained fake accounts due to their relatively cheap cost and flexibility. Automated political bots are gaining popularity as more technological solutions appear.

Our study suggests the following classification of bots: impact bots, amplifiers, service bots, trackers and complainers depending on their functions. The technical capacity of Ukrainian software developers is quite significant, but most innovative tools seem to be developed for foreign countries and out of commercial interest. The effectiveness of tools such as bots and fake accounts remains to be explored, but the widespread use that we witnessed in Ukraine definitely undermines credibility of public debate and requires a more rigorous reaction.

Analysis of the external dimension of computational propaganda disclosed the complexity of challenges it brings for countries engaged in the information stand-off, especially under conditions of unequal resources. Past research, as well as a variety of media reports, show the Russian government has created a strong network of online actors and tools such as bloggers, trolls and automated bots in order to spread misinformation online, promote official narrative and attack opponents.

One of the strong examples of such disinformation attacks is the case of MH17. It illustrates the complexity of the computational propaganda phenomenon and suggests it can have a visible influence on the international political domain. Russia actively used the Twitter accounts

of mass media and bots to disseminate fake information about the tragedy. The followers of these accounts, including mass media, used this information in further references. Moreover, this fake evidence was used by the Russian Ministry of Defence and other officials to build a case against Ukraine, blaming it for the catastrophe and complicating the official investigations. Our findings suggest that the response of the Ukrainian government to these challenges has been rather weak and sporadic. It has been lacking a comprehensive strategy and responsiveness to the immediate challenges created by the growing social media influence. Nevertheless, a lot of efforts to tackle computational propaganda have been made by activists and volunteers. This indicates the potential of civil society to address the challenges of computational propaganda in the digitalized world.

About the Authors

Mariia Zhadanova is a member of the Ukrainian fact checking organization Stop Fake, a project launched by the Kyiv Mohyla Journalism School and Digital Future of Journalism Project. Stop Fake's goal is to verify and refute disinformation and propaganda while also acting as an information hub for examining and analyzing Kremlin propaganda. She is also Head of Digital at Vogue Ukraine.

Dariya Orlova is also a member of Stop Fake. She is a Senior Lecturer and media researcher at the Mohyla School of Journalism and a former visiting professor at Stanford's Center for Russian, East European and Eurasian Studies. She received her PhD in Mass Communication from the Autonomous University of Barcelona.

References

AIN.UA. (31 January 2015). Kak rabotayut internet-trolli i kak ikh raspoznat: intervyu s byvshim “akhmetovskim botom” (How Internet trolls work and how one can recognize them: an interview with a former “Akhmetov’s bot”). AIN.UA. Retrieved from https://ain.ua/2015/01/31/kak-rabotayut-internet-trolli-i-kak-ix-raspoznat-intervyu-s-byvshim-axmetovskim-botom

Alexander, L. (2015a). Are Russian news media getting a boost from retweet bots on Twitter? Global Voices. Retrieved from https://globalvoices.org/2015/11/27/are-russian-news-media-getting-a-boost-from-retweet-bots-on-twitter/

Alexander, L. (2015b). The curious chronology of Russian Twitter bots. Global Voices. Retrieved from https://globalvoices.org/2015/04/27/the-curious-chronology-of-russian-twitter-bots/

Alexander, L. (2015c). Social network analysis reveals full scale of Kremlin’s Twitter bot campaign. Global Voices. Retrieved from https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

BBC. (21 April 2016a). Ukraine bans Russian films in media war. BBC News. Retrieved from http://www.bbc.com/news/world-europe-36099885

BBC. (28 September 2016b). MH17 Ukraine plane crash: What we know. BBC News. Retrieved from http://www.bbc.com/news/world-europe-28357880

BBC. (16 May 2017c). Ukraine's Poroshenko to block Russian social networks. Retrieved from http://www.bbc.com/news/world-europe-39934666

Bērziņš, J., Jaeski, A., Laity, M., Maliukevicius, N., Navys, A., Osborne, G., … Tatham, S. (2014). Analysis of Russia’s information campaign against Ukraine. NATO StratCom Report.

Bohdanova, T. (2014). Unexpected revolution: The role of social media in Ukraine’s Euromaidan uprising. *European View*, *13*(1), 133–142.

Butsenko, A. (28 October 2014). Trolli iz Olgino pereehali v novyy chetyrekhetazhnyy ofis na Savushkina (Trolls from Olgino moved into a new four-storey office on Savushkina). Dp.ru. Retrieved from https://www.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo/

Chen, A. (2 June 2015). The Agency. *The New York Times*. Retrieved from https://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=1

Detector Media. (2017). Yak rosiyska propaganda vplyvae na suspilnu dumku v Ukrayini (doslidzhennia) (How Russian propaganda influences public opinion in Ukraine (research findings)). Retrieved from http://osvita.mediasapiens.ua/mediaprosvita/research/yak_rosiyska_propaganda_vplivae_na_suspilnu_dumku_v_ukraini_doslidzhennya/

Dickinson, J. (2014). Prosymo maksymal’nyi perepost! Tactical and discursive uses of social media in Ukraine’s EuroMaidan. *Ab Imperio*, *2014*(3), 75–93.

Dzerkalo Tyzhnia. (20 September 2016). Ukrayina zaminyt rosiyski telekanaly na koreyski (Ukraine will substitute Russian TV channels with Korean ones). Dzerkalo Tyzhnia. Retrieved from http://dt.ua/UKRAINE/ukrayina-zaminit-rosiyski-telekanali-na-koreyski-219354_.html

Ennis, S. (12 March 2014). Ukraine hits back at Russian TV onslaught. BBC Monitoring. Retrieved from http://www.bbc.com/news/world-europe-26546083

Factum Group Ukraine (2017). Proniknovenie Interneta v Ukraine (Internet penetration in Ukraine). Internet Association of Ukraine. Retrieved from http://inau.ua/sites/default/files/file/1701/iv_kvartal_2016.pptx

Forpost. (18 April 2017). Stop propaganda: Ukrayintsi mozhut vstanovyty sobi dodatok, yakyi blokuye rosiysku propagandu (Stop propaganda: Ukrainians can install an extension that allows blocking Russian propaganda). Forpost. Retrieved from http://forpost.lviv.ua/novyny/2815-stop-propaganda-ukraintsi-mozhut-vstanovyty-sobi-dodatok-iakyi-blokuie-rosiisku-propahandu

Garmazhapova, A. (9 September 2013). Gde zhivut trolli. I kto ikh kormit (Where do trolls live. And who feeds them). *Novaya Gazeta*. Retrieved from https://www.novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

Gorchinskaya, K. (27 July 2016). The rise of Kremlin-style trolling in Ukraine must end. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/jul/27/kremlin-style-troll-attacks-are-on-the-rise-in-ukraine-hromadske

Gruzd, A., & Tsyganova, K. (2015). Information wars and online activism during the 2013/2014 crisis in Ukraine: Examining the social structures of pro- and anti- Maidan groups. *Policy & Internet*, *7*(2), 121-158.

Hegelich, S. (2016). Invasion of the social bots. Policy Paper. Konrad Adenauer Stiftung. Retrieved from http://www.kas.de/wf/doc/kas_46486-544-2-30.pdf?161007093837 September, no.221

Hegelich, S., & Janetszko, D. (2016). Are social bots on Twitter political actors? Empirical evidence from a Ukrainian social botnet. International AAAI Conference on Web and Social Media. Retrieved from http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13015/12793

Higgins, E. (10 January 2015). SU-25, MH17 and the problems with keeping a story straight. Bellingcat. Retrieved from https://www.bellingcat.com/news/uk-and-europe/2015/01/10/su-25-mh17-and-the-problems-with-keeping-a-story-straight/

Hoskins, A., & O'Loughlin, B. (2015). Arrested war: The third phase of mediatization. *Information, Communication & Society*, *18*(11), 1320–1338.

Internews. (2016). Media consumption survey—Ukraine 2016. Internews Network. Retrieved from https://www.internews.org/sites/default/files/resources/Media_Consumption_Survey_2016-09_Eng_Internews.pdf

Internews. (2017). Results of the survey about the risks of Internet freedom in Ukraine. Internews Ukraine. Retrieved from http://internews.ua/2017/01/netfreedom-survey/

Ivantsova, A. (29 May 2015). Internet-troli na sluzhbi v oligarkhiv i politykiv (Internet trolls servicing oligarchs and politicians). Radio Free Europe/Radio Liberty. Retrieved from http://www.radiosvoboda.org/a/27042051.html

IVOX. (20 January 2016). Samye populiarnye messendzhery v Ukraine i Rossii—infografika (The most popular messengers in Ukraine and Russia—infographics). Tehnot. Retrieved from http://tehnot.com/samye-populyarnye-messendzhery-v-ukraine-i-rossii-infografika/

JIT. (2016). Criminal investigation MH17. Joint Investigation Team. Retrieved from https://www.om.nl/onderwerpen/mh17-crash/

KAS. (2015). Ukrainian media landscape—2015. Policy Paper. Konrad Adenauer Stiftung. Retrieved from http://www.kas.de/wf/doc/kas_43639-1522-13-30.pdf?151209161127 27 March 2016

Kelly, J., Barash, V., Alexanyan, K., Etling, B., Faris, R., Gasser, U., & Palfrey, J.G. (2012). *Mapping Russian Twitter*. The Berkman Center for Internet & Society.

Khaldarova, I., & Pantti, M. (2016). Fake news: The narrative battle over the Ukrainian conflict. *Journalism Practice*, *10*(7), 891–901.

Kivimäki, V-P. (14 November 2014). Russian state television shares fake images of MH17 being attacked. Bellingcat. Retrieved from https://www.bellingcat.com/news/2014/11/14/russian-state-television-shares-fake-images-of-mh17-being-attacked/

Kriukova, S., & Pasiutina, A. (2 June 2016). Territoriya botov. Kto i kak sozdaet parallelnuyu realnost v ukrainskikh socsetiakh (Bots' territory. Who and who creates a parallel reality in Ukrainian social networks). Strana.ua. Retrieved from http://longread.strana.ua/territoriya_botov

Lucas, E., & Nimmo, B. (2015). Information warfare: What is it and how to win it? Policy Paper. CEPA Infowar Paper No.1. Retrieved from http://cepa.org/files/?id_plik=1896

Lucas, E., & Pomerantsev, P. (2016). Winning the information war: Techniques and counter-strategies to Russian propaganda in central and eastern Europe. CEPA Report. Legatum Institute. Retrieved from http://cepa.org/reports/winning-the-Information-War

Luhn, A. (2017). Ukraine blocks popular social networks as part of sanctions on Russia. *The Guardian*. Retrieved from https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war

Meister, S. (2016). Isolation and Propaganda. The Roots and Instruments of Russia's Disinformation Campaign. Transatlantic Academy Paper Series. April 2016. Retrieved from https://dgap.org/en/article/getFullPDF/28043

Ministry of Defence. (21 July 2014). Materialy Ministerstva oborony Rossiyskoy Federatsii k brifingu po obstoyatelstva katastrofy samoleta "Boing-*777*" aviakompanii "Malaziyskie avialinii" (Materials of the Ministry of Defence of Russian Federation for the briefing on the circumstances of Boeing-*777* crash of Malaysian Airlines). Ministry of Defence of Russian Federation. Retrieved from http://function.mil.ru/news_page/country/more.htm?id=11970771@egNews

Nemtsova, A. (15 July 2014). There's no evidence the Ukrainian army crucified a child in Slovyansk. The Daily Beast. Retrieved from http://www.thedailybeast.com/articles/2014/07/15/there-s-no-evidence-the-ukrainian-army-crucified-a-child-in-slovyansk

Novaya Gazeta. (*7* May 2015). Facebook zablokiroval Sergeya Parkhomenko za kommentariy doklada o sbitom "Boinge" (Facebook blocked Sergey Parkhomenko for a commentary on report about shutdown Boeing). Novaya gazeta. Retrieved from https://www.novayagazeta.ru/news/2015/05/07/112052-facebook-zablokiroval-sergeya-parhomenko-za-kommentariy-doklada-o-sbitom-171-boinge-187

Novoye Vremya. (2016). Geroi Feisbuka: Novoye Vremya predstavliaet ezhegodnyi reyting liderov mneniy v socsetiakh (Facebook heroes: Novoye Vremya presents the annual ranking of opinion leaders in social networks). Novoye Vremya. Retrieved from

http://nv.ua/ukraine/events/geroi-fejsbuka-novoe-vremja-predstavljaet-ezhegodnyj-rejting-liderov-mnenij-v-sotssetjah-276466.html
Nygren, G., Glowacki, M., Hök, J., Kiria, I., Orlova, D., & Taradai, D. (2016). Journalism in the Crossfire: Media coverage of the war in Ukraine in 2014. *Journalism Studies*, 1–20.
Online.ua. (24 September 2016). V socsetiakh na paltsakh pokazali, kak rabotayut boty Kremlia: opublikovany foto (Social media users showed how Kremlin's bots work: photo published). Online.ua. Retrieved from https://news.online.ua/754036/v-sotssetyah-na-paltsah-pokazali-kak-rabotayut-boty-kremlya-opublikovany-foto/
Onuch, O. (2015). EuroMaidan protests in Ukraine: Social media versus social networks. *Problems of Post-Communism*, *62*(4), 217–235.
Orlova, D., & Taradai, D. (2016). Facebook as an alternative public space: The use of Facebook by Ukrainian journalists during the 2012 parliamentary election. *Central European Journal of Communication*, *9*(16), 37–56.
Romanenko, N., Mykhaylyshyn, Y., Solodko, P., & Zog, O. (4 October 2016). Trolesfera (Trolls sphere). Texty.org.ua. Retrieved from http://texty.org.ua/d/fb-trolls/
Rothrock, K., (20 July 2014). The Russian Government's 7,000 Wikipedia Edits. Global Voices. Retrieved from http://www.globalvoicesonline.org/2014/07/20/the-russian-governments-7000-wikipedia-edits/
RT. (9 May 2014). Ispanskiy bloger o situatsii na Ukraine: liudi perepolneny nenavistiu (Spanish blogger about situation in Ukraine: people are overwhelmed with hatred). RT. Retrieved from https://russian.rt.com/article/31215
Shandra, A. (2015). The most comprehensive guide ever to MH17 conspiracies. Euromaidan Press. Retrieved from http://euromaidanpress.com/2015/10/14/confuse-and-obfuscate-the-most-comprehensive-guide-ever-to-mh17-conspiracies/#arvlbdata
Snegovaya, M. (2015). Putin's information warfare in Ukraine. Soviet origins of Russia's hybrid warfare. Russia Report, 1. Institute of the Study of War. Retrieved from http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf
Solonenko, I. (2015). Ukrainian civil society from the orange revolution to Euromaidan: Striving for a new social contract. In *OSCE Yearbook 2014*, 219–236. Nomos Verlagsgesellschaft mbH & Co. KG, 2015. doi: 10.5771/9783845260945-219.
StopFake. (15 July 2014a). Fake: Crucifixion in Slovyansk. StopFake. Retrieved from http://www.stopfake.org/en/lies-crucifixion-on-channel-one/
StopFake. (18 July 2014b). Lies: Spanish flight operations officer from Kiev informed about Ukrainian planes involved in Boeing tragedy. StopFake. Retrieved from http://www.stopfake.org/en/lies-spanish-flight-operations-officer-from-kiev-informed-about-ukrainian-planes-involved-in-boeing-tragedy/
StopFake. (3 November 2014c). Fake: Ukrainian militaries are promised "a parcel of land and two slaves". StopFake. Retrieved from http://www.stopfake.org/en/fake-ukrainian-militaries-are-promised-a-parcel-of-land-and-two-slaves/
The Insider. (4 August 2016). Ispanskiy dispetcher, videvshiy kak ukraintsy sbili MH17, prevratilsia v Liudmilu Lopatyshkinu (Spanish flight operations officer who saw how Ukrainians shut down MH17 turned into Liudmila Lopatyshkina). The Insider. Retrieved from http://theins.ru/antifake/27246

Varol, O., Ferrara, E., Davis, C.A., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. arXiv preprint arXiv:1703.03107. https://arxiv.org/pdf/1703.03107.pdf

Way, L. (2015). *Pluralism by default: Weak autocrats and the rise of competitive politics*. JHU Press.

Woolley, S., & Howard, P.H. (2016). Political communication, computational propaganda, and autonomous agents. *International Journal of Communication, 10*, 4882–4890.

Yarovaya, M. (23 February 2015). "Minstets" zapustil i-army.org i ischet dobrovoltsev "Internet-voiska Ukrainy" ("Minstets" launched i-army.org and looks for volunteers to join "Ukraine's internet army") AIN. Retrieved from https://ain.ua/2015/02/23/minstec-zapustil-i-army-org-i-ishhet-dobrovolcev-v-internet-vojska-ukrainy

Zakharov, A., & Rusyaeva, P. (23 March 2017). V nedrakh "fabriki trollei" vyros krupneishiy v Rossii mediaholdin (The biggest media holding in Russia grew out of "troll factory"). RBC. Retrieved from http://www.rbc.ru/technology_and_media/23/03/2017/58d2c2df9a7947273ccb28e5?from=main

Citation

Mariia Zhdanova & Dariya Orlova, "Computational Propaganda in Ukraine: Caught between external threats and internal challenges." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.9. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk<http://comprop.oii.ox.ac.uk/>. 25 pp.

Series Acknowledgements

The authors gratefully acknowledge the support of the European Research Council, Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe," Proposal 648311, 2015-2020, Philip N. Howard, Principal Investigator. Additional support has been provided by the Ford Foundation and Google-Jigsaw. Project activities were approved by the University of Oxford's Research Ethics Committee. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders or the University.