PIRET PERNIK
VLADIMIR SAZONOV

PROTECTING THE EUROPEAN PARLIAMENTARY ELECTIONS:

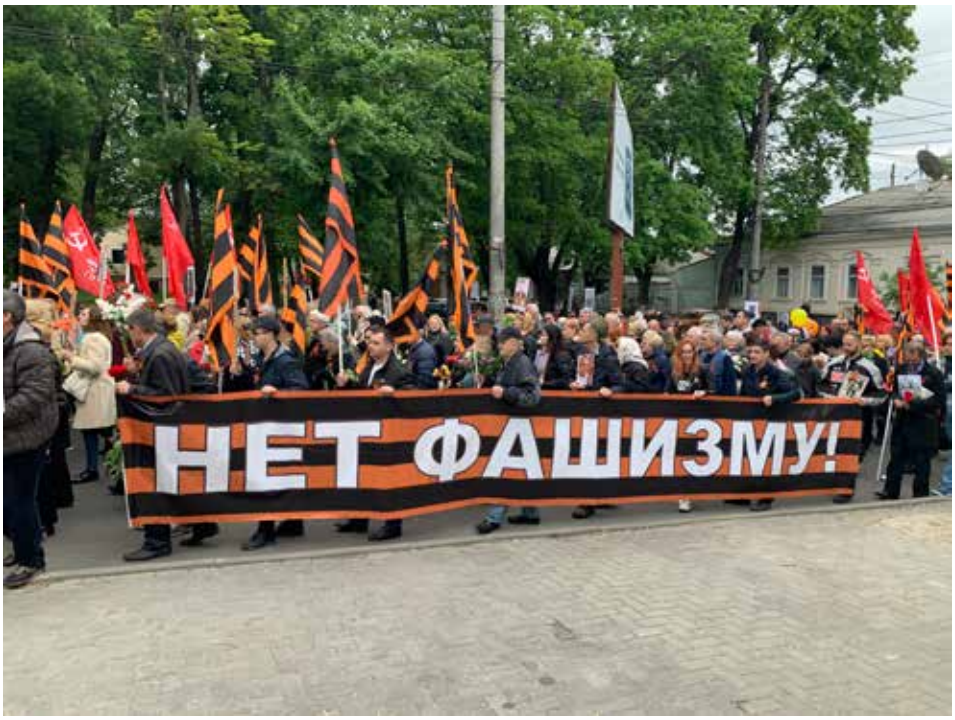
Lessons Learned From The 2019 Presidential Elections In Ukraine

sisekaitse.ee

PIRET PERNIK
VLADIMIR SAZONOV

PROTECTING THE EUROPEAN PARLIAMENTARY ELECTIONS:

Lessons Learned From The 2019 Presidential Elections In Ukraine



Demonstration in Chişinău. May 9, 2019. *Photo: Kristina Reinsalu*

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

sisekaitse.ee

www.sisekaitse.ee/kirjastus

CONTENTS

INTRODUCTION

During the present decade the foreign authoritarian influence in democratic processes – including in national elections and referendums – has become the norm. The few recent cases are Brexit, the presidential election in France, parliamentary election in Germany, presidential and mid-term congressional elections in the United States, as well as referendums in Catalonia, Spain, and the Netherlands. Europeans are increasingly concerned about the possible influence on and interference of Russia in the upcoming European Parliamentary elections that will be held on 23-26 May 2019 in the 28 EU member states.

In this broader context, we will elucidate the key hybrid tactics and tools of Russia aimed at undermining the Ukrainian state during the election period in the country; and identify key lessons that should be applied for enhancing the protection of the European Parliamentary elections.

- **First**, we will outline Russia's activities in the information sphere and cyberspace more broadly.
- **Second**, we will lay out Russia's hybrid toolbox in Ukraine in particular during the months and days preceding the 2019 election period.
- **Third**, we will briefly review the preventive and defensive actions and instruments the EU has implemented focusing on the period between 2018 and 2019. We will argue that the Europeans ought to study more thoroughly the ways and means of Russia's continuous application of the hybrid toolbox in Ukraine and elsewhere.

It is not sufficient to focus only on the short timeframe before the elections – the application of Russia's toolbox must be analysed over a longer term to fully comprehend its logic and modus operandi. Russian experts have observed that the Kremlin effectively innovates by introducing ever new instruments, which often succeed to evade the newly invented defence measures as soon as these are put in place. Offense tends to be one step ahead of defence in the field of security, and thus defenders must be agile enough to adapt the traditional defence measures and create novel ones and ideally prevent the malicious influence activities. Therefore, we suggest that the international community should meticulously gather the scattered pieces of knowledge about influence campaigns across a longer time span in many countries to compare the differences and similarities between the case studies with an aim to predict the future possible cases. Such a comprehensive knowledge-base will help to understand how the Kremlin innovates, uses various opportunities as they rise in order to attain the ultimate realization of president Vladimir Putin's worldview – that he thinks he is getting closer to – of a multipolar world. In this world Russia is a great power deciding over sovereignty of countries located at its geographic borders (her self-proclaimed "sphere of interest") and NATO does not exist. If the West fails to comprehend how this worldview is being constantly implemented, it will likely confront another strategic surprises (Bugayova, 2019).

Finally, we will recommend additional defensive measures that will complement the policy recommendations made by a large number of scholars, journalists, governments and other defenders of democratic values and freedoms.[1]

1 For example, the following report provides a set of recommendations: Conley, H. A. et al. 2019; Belfer Center for Science and International Affairs 2018; Vilmer, J.-B. et. al. 2018; and a number of reports by the British parliament.

RUSSIA'S APPROACH TO INFORMATION WARFARE

In recent years, the Kremlin has increased aggressive rhetoric, using soft and hard power, and a range of asymmetric tools of destabilization towards the Baltic states, Ukraine and the West more generally (Winnerstig, 2014; Spriņģe, 2018; Ventsel, Sazonov, 2018). Russia is mass producing propaganda to influence different domestic and foreign target audiences (the general public, opinion leaders, businessmen, politicians, etc.), disinformation, social media trolls, informational deception, conspiracy theories, narratives of Russophobia, psychosocial operations, blackmailing, military exercises as information operations, etc (Alyukov, 2018; Yablokov, 2015, pp. 301-315; Nissen, 2015, Kowalik, Jankowski, 2017; Darczewska, Żochowski, 2015). Holger Mölder and Vladimir Sazonov (2018, p. 309) pointed out about Russian information warfare:

> *"Russia has been among the pioneers of contemporary information warfare and actively started to use different forms of information campaigns in pursuit of its political goals. However, information warfare can be used not just for promoting national interests, but for influencing the whole international system".*

Russia is waging asymmetric war against the West on different strategic levels and dimensions through the application of a broad range of hybrid tactics and tools. Additionally, to informational pressure (note: meanwhile, the effects of Russian propaganda are also visible in the West, where they are less significant than in Eastern Europe but still cannot be underestimated. The channels such as RT, Sputnik are broadcast in the whole European region, and even in the United States) Moscow is also using cyber-attacks, pressure on economic, political, social and other crucial strategical levels, etc. Moscow is trying to account for the characteristics of each country in Europe, it is trying to damage the European democratic system, targeting liberal values and European politics (Karlsen, 2019) with different types of disinformation, cyber-attacks, producing fake news, trying to intimate and bribe politicians (especially far-right forces), using "useful idiots", pro-Kremlin minded media, people etc. There are several reasons why Moscow is using hybrid threats and asymmetric tactics against Europe, one of them is creating political chaos, instability, harming democratic and liberal values and systems, damaging and weakening pan-European security architecture and cooperation in the EU (Karlsen, 2019: 1, 2, 5).

Russia is trying to reduce the sanctions from the EU, pushing the EU political elite and as Geir H. Karlsen (2019, p.5) has correctly pointed out: "In a short-term perspective, Russia aims to have the sanctions imposed since 2014 lifted".[1] Moscow's aim is to change European consistency. This is one of reason why Moscow is targeting the European parliament elections, influencing them. Ukraine is another dimension or area where Russia is conduct-

1 See also the Estonian Internal Security Service Annual Review 2018, 7: „The international measures following the annexation of Crimea have an impact on Russia's divisive policy. Among other things, the Kremlin presents Western sanctions as aggravating the situation of Russian expatriate communities".

ing hybrid war, which could provide us relevant information about the tools of destabilization and manipulative techniques of Russia's hybrid warfare arsenal. Russia is interested in the European Parliament elections.[2]

In the Ukraine for example Russia conducted a multidimensional hybrid war. It should be noted that the aggressive wave of Russian information campaigns against Ukraine (manipulative techniques, trolling, etc.) (NATO StratCom COE, 2015) began already in at least 2013 during the Maidan events, approximately a year before the annexation of Crimea in 2014 and Russian aggression in the Donbass area. Although Russian information activity in Ukraine is much older and its roots are visible already as early as the beginning of the 1990s. In the case of Ukraine, Putin's regime is also using military forces against the Ukrainian state, supporting groups of pro-Kremlin separatists in the Donbass. There are several other vulnerabilities and issues, which Russia uses or could use by implementing asymmetric threats and in Europe one of these hybrid threats is Russian intervention in democratic processes such as elections and referendums (e.g., presidential elections in the US in 2016, in France 2017, Brexit, the so-called Catalan independence referendum, etc.). Currently, Europe is preparing for European Parliament elections and there are high risks with a real possibility that Russia will try to influence it with a purpose to change and harm the security environment in Europe as well. According to some analyses (SafeGuardCyber 2019, 1) "EU personnel across administrative bodies and rank are currently vulnerable to bad actor operations, putting EU digital infrastructure at risk".

2 Stoicescu 2019: Finally, the [Estonian Foreign Intelligence Service] draws attention to Russia's interest in the May 2019 elections to the European Parliament and the growing influence of societally divisive and anti-EU parties in Europe that are overtly or covertly supported or sponsored by Moscow," (The Estonian Foreign Intelligence Service Yearbook, 2019).

RUSSIA'S INFLUENCE ON THE UKRAINIAN ELECTIONS IN 2014 AND 2019

Propaganda and Disinformation

Let's use the Ukrainian experience as an example where Russia has used analogical approaches in the spheres of information and cyber warfare around Europe and even wider. The Ukrainian case can provide some useful information which could help us to better understand the nature of Russian influence activities in the context of elections in the EU, especially related to the upcoming European Parliamentary elections.[3]

Russia's aim is to create chaos during and after the presidential elections (Müür, Mölder, Sazonov, Pruulmann-Vengerfeldt, 2016, pp. 28–71; Berzinš, 2014; Darczewska, 2014) and according to Yegor Bozhok (Head of the foreign intelligence service of Ukraine) the Russian government invested 350 million USD into its secret services for creating destabilization and chaos in Ukraine in 2019. According to Ukrainian political expert Dr. Yevhen Mahda the Russian strategic goal is to retake Ukraine into the "Russian World", there are several reasons and one of them is if Ukraine will be "taken" back under Russian influence, it will also have a demoralizing effect for several European countries. The Kremlin is trying to discredit and undermine democratic values, to destroy the democratic system (Ukrinform, 2019).

For that purpose the Kremlin activated pro-Russian and Russian media outlets in Ukraine, which tried to discredit Ukrainian politicians, who are not profitable for the Kremlin. Moscow is using trolls and bots, fake news about Ukrainian politicians, candidates in presidential elections, who are not supported by Moscow (Belikov, 2019). Russia could also use not recognizing the Ukrainian presidential elections in 2019 as a tactical step, which was even discussed in the Russian parliament (Regnum, 2019; MK.ru, 2019). Social media (e.g. Facebook, Twitter, Odnoklassniki, Vkontakte) has been seen by the Kremlin already for a number of years as a powerful tool of influence (Schwirtz & Frenkel, 2019).

According to Michael Schwirtz and Sheera Frenkel "Ukraine has long been a testing ground for all manner of so-called Russian active measures and was among the first hit with the kind of electoral manipulation later deployed against the United States, France and other countries" (Schwirtz & Frenkel, 2019).

Ukrainian political expert Dr. Sergei Pakhomenko (Mariupol) explained the differences between Russian interventions in the Ukrainian presidential elections in 2014 and 2019. In 2014 according to Sergei Pakhomenko Russia used two main messages in information warfare: 1) Ukrainian elections are not legitimate and they were provided after the coup d'état organized in Kiev; 2) right radical Dmytro Yarosh and Ukrainian nationalists forces were leading in presidential elections, which was not true, although Russian „Pervyi kanal" on the day of the elections promoted fake news that according to preliminary data Yarosh was in the leading position in the presidential elections (Telekanal Dozhd, 2014) (Pakhomenko 2019). In 2019 the situation differed from 2014 in several ways.

3 Estonian Internal Security Service Annual Review 2018, 7: „The above scenario indicates that the Kremlin is turning to more targeted attempts to create divisions in Western societies".

Firstly, Russia didn't use the radical far-right forces this time, the main aim of the Kremlin was that Poroshenko should not be re-elected. Secondly, Russia side promoted the idea that the elections will not be legitimate.

Thirdly, several Russian politicians accentuated that they will not accept the Ukrainian elections, among them Vladimir Zhirinovski. Notable here is that both candidates Yulia Timoshenko and Volodymyr Zelenski (who got 30% of the vote in the 1st round of elections) declared that they will reach an agreement with V. Putin (Pakhomenko, 2019). It is also notable that presidential candidate Volodymyr Zelenski also shows some positive attitude towards Vladimir Putin (Youtube 2014).

Ukrainian political expert Dr. Dmitri Dubov (Kiev) claimed that in 2014 the situation was quite specific, while military Russian aggression and the question of Ukrainian existence were crucial factors during the elections. Also, for Russia, this situation was not clear and Russia used its common arsenal: economic pressure, support of pro-Russian politicians and they promoted the idea of a "Nazy junta in Kiev", used cyber-attacks during parliamentary elections, accentuated the attention of people onto "growing nationalism" and fascism forces in Ukraine, the role of the United States in Ukrainian politics, etc (Dubov, 2019). In 2019 the situation has already changed, while the impact of Russian TV channels was minimized because they were banned. Russia's aim is creating chaos around the elections and the Kremlin's aim is not to allow Poroshenko to become president for the second time. The best solution for the Kremlin will be if the elections will be won by a person who is outside of the Ukrainian political system – e.g. V. Zelenski. Moscow wants to use the „American scenario" (how it was in the case of D. Trump and the US Congress) when the Parliament of Ukraine and new President will be confronted and it could paralyze the governmental system of Ukraine. Cyber-attacks are not an important factor in that case, but cyber-attacks could be used for creating chaos – for example Russia can attack important information systems. Also, terrorist acts are not excluded (Dubov, 2019). Political expert Dr. Yevhen Mahda (Kiev) explained the situation in 2019 as follows: "In 2019 we see not only the bombing of Ukrainian information space with fakes, but we also see the presence of a pro-Russian narrative in several TV channels and their key elements – theses about direct negotiations with the "people's republic of Donbas", transition to neutral status and renouncement from aspiration to recreate the integrity of the Ukrainian state."[4]

The Kremlin massively uses fakes, disinformation and intervention in the Ukrainian political and economic spaces. Russia is actively using pro-Kremlin media channels in Ukraine, which try to discredit the presidential elections. Russia is interested in disrupting the elections in Ukraine because it will promote the narrative of "Ukraine is a failed state" (Магда, 2019). The cyber-attacks are not the main instrument of Russia in influencing the elections for many reasons, while Ukrainian governmental sites are protected by Ukrainian specialists and experts from NATO states. It seems that Russia is trying to disrupt the trust of the Ukrainian people towards elections, to show that the Ukrainian elections are illegitimate (Магда, 2019).

Dr. Yevhen Mahda states that opponents of President P. Poroshenko are active and it seems that their actions are coordinated from one centre and it seems that this centre is located outside of the Ukraine. Poroshenko is the only candidate who speaks clearly about Ukrainian membership in NATO and the EU (Магда, 2019).

According to Ukrainian expert Kostiantyn Romashko (Manager of EU-related projects, Internews Ukraine) the Kremlin's tactics have previously (in 2014) consisted in betting on a specific presidential candidate in the Ukraine. But now the strategy has changed, it is different and consists of creating chaos and disappointment in Ukraine. Additionally, there is an active dissemination of the message about the illegitimacy of the Ukrainian government. In 2014 before and during the presidential elections in Ukraine, such a message promoted the idea of "junta in Kiev". In 2019 it consists of electoral rigging and also fraud (Romashko, 2019). In the media Russia tried to influence "via dozens and hundreds of "junky" websites. We can see that from our research on the *VKontakte* social network, as well as from the study „We have bad news" conducted by Texty.org.ua. These websites often resort to exaggeration to relay aggressive messages that other media broadcast in a more "civilized" form. Their style can be characterized with aggression and hostile language" (Romashko, 2019). The Kremlin was trying to influence Ukrainian TV channels and other information channels in the Ukraine with non-transparent funding like strana.ua, *Vesti, NewsOne, 112* and others. Several pro-Russian forces and activists are also using YouTube as a channel or a tool "that drive up the

4 Interview with Y. Mahda, 29.3.2019, Facebook.

volume of their audience (including views, likes, comments), largely doing so via bots or hired users with a view to ending up in YouTube's top ranking videos, and thus being able to henceforth rely on promotion done by YouTube itself (through "recommended videos")" (Romashko, 2019).

Cyber-attacks and the Use of Technology to Spread Disinformation

During information confrontation – which is continuously occurring between the West and Russia according to Russian military thinkers – the key tools to inflict damage on an opponent are information-psychological tools – whose application was discussed in the previous sections of this article – and information-technical tools, including cyber-attacks against election infrastructure such as election servers and websites, voter registration databases, etc., as well as against the auxiliary infrastructure that the election process depends on, for example communication networks, population register, etc.

The past case studies show that cyberattacks can erode public trust in elections. For example, foreign adversaries have broadcasted stolen confidential data and falsified documents (for example, in the US, France, Ukraine, and Sweden) in order to ruin the reputation of politicians. They have used computer algorithms and inauthentic social media profiles and pages to spread and amplify disinformation and propaganda. For example, bots enable the posting of automated comments which amplify disinformation.

Social media has also been successfully used for organizing real-world protests by foreign government affiliated actors (for example, in the US and Ukraine). Thus, the computer technology is a perfect technical tool in order to covertly activate societal groups and possibly change their behaviour. According to Russian thinkers this can be achieved by altering the picture of reality and consciousness of target groups (this activity is dubbed also as "reflective control"). In 2017, a Russian military theorist, Colonel V. A. Kiselyov opined that in the future information and cyberwarfare will "in their dialectic progress [...] merge into a single whole." (Kiselyov, 2017). Russia's influence activities over the recent years prove that he was right.

Put into expert jargon, cyber-attacks target confidentiality, availability and the integrity of information and information systems.[5] Various types of cyber-attacks can be used against elections. One of the most popular low-cost high-effect threat vector is disrupting the availability of information or services which are related to the elections process. Denial of Service (DoS) attacks against election committees' websites that may disrupt the timely provision of information for the voters belong to this category. Another option is defacing websites that provide information for citizens regarding the elections. These types of relatively unsophisticated cyber-attacks do not require specialist technical knowledge or much financial resources. One of the recent examples from this category were DoS attacks against the Finnish Central Election Commission a few days prior to the parliamentary elections that were held in March 2019 (Pohjapalo, 2019).

Another possibility to erode trust in the democratic election process is to target auxiliary infrastructure that it depends on – for example, online voter registers or online transmission of election results from local polling stations to the central location where the votes will be counted. According to the Ukrainian police this type of cyber-attack against the local mobile operators communications networks was planned by Russian agents in March – a Russian resident collected intelligence on the Ukrainian mobile operators networks of which the functioning of Ukrainian election infrastructure depended on (The Security Service of Ukraine, 2019).

A more severe cyber-attack can be launched against the integrity of data or computer systems. For example, in May 2014 a pro-Russia hacker group CyberBerkut – believed to be affiliated to the Russian security services – infected the Ukrainian Election Commission computer systems with malware which was meant to display on the commission's website falsified election results. The falsified results were broadcasted by the Russian TV channel on

5 Information security ensures the availability, confidentiality and integrity of information. In addition it can involve other properties such as authenticity, accountability, non-repudiation and reliability (International Organisation for Standardisation, 2018).

the same day.[6] More advanced techniques of information manipulation are the so-called deep fakes which consist of synthetic video and audio materials.

In addition, computer systems and communication networks can be compromised in order to collect intelligence, which facilitates the launching of further cyber-attacks. Also open-source personal data as part of social engineering tactics can be collected for the purpose of harvesting email log-in credentials or installing malware to a victims computer through spear-phishing emails and malicious websites. If hackers are able to obtain confidential or sensitive information about election candidates these individuals can become victims of blackmailing.

Another option for hackers is to take over social media accounts of election candidates in order to spread disinformation or ruin their reputation by posting on their behalf.

Since the mid-2000s Russia has used most of these opportunities. According to technology companies who have investigated cyber-attacks, Russia has developed an impressive set of malware. For example, NotPetya ransomware attacks that incorporated zero-day vulnerabilities were attributed to Russian military intelligence by several Western governments. Russia has sophisticated social engineering tactics thanks to which Russian hackers have successfully stolen email credentials. It has also conducted false flag operations – for example, TV5/Monde cyber-attacks in April 2015 (Greenberg, 2018).

Turning back to Ukraine, the country has been the primary target of Russia's information and psychological operations at least since the 2000s. In the months before the Euromaidan protests began in December 2013 low-level cyber-attacks against many Ukrainian websites intensified (Koval, 2015). Both Ukrainian and American intelligence services predicted that Russia will use cyber techniques to influence the elections in Ukraine in 2019, and as of March the Ukrainian police had registered over 220 cases of election interference attempts, attributed by Ukrainian authorities to Russian security services and individuals working for them.

In January 2019, Dan Coats, the US Director of National Intelligence, predicted that foreign actors will "refine their capabilities and add new tactics as they learn from each other's experiences and efforts in previous elections." (Coats, 2019). Russia has certainly learned from its own mistakes and from its success stories, and refined their tactics accordingly. For example, a few weeks before the Ukrainian presidential elections that were held on the 31st of March, Facebook shut down nearly 2000 Russia-linked profiles and pages (Schwirtz & Frenke, 2019). Instead of creating new fake social media pages and profiles (this has been Russia's key tactics to influence voters in many countries) the Russian masterminds chose to co-opt local Ukrainians and pay them for spreading disinformation through authentic pages that had large auditorium and accounts.

In this way, the Russian actors successfully evaded the stronger security measures put in place by Facebook. In some cases Russian special operations officers who resided in Kiev were organizing these influence campaigns. The Ukrainians who received payments from Russian agents had in addition to using their own pages and accounts also register new webpages, news platforms and create additional social media profiles for spreading disinformation. Russian security services also paid for hackers who were supposed to disseminate malware and infect state computer systems. Ukrainian police arrested an individual residing in Ukraine who was posting propaganda on social media who received instructions from authorities of the Donetsk People's Republic (The Security Service of Ukraine, 2019). Fake domain servers – resembling authentic news sites – were registered for social engineering purposes, and at the closed hackers forums orders were placed for buying personal data of Ukrainian election officials, as well as of state internal databases such as voter registration lists (Zn.ua, 2019) .

These examples demonstrate close cooperation between Russia's state authorities, security services, hackers and even ordinary individuals who may not hold any political convictions, but are simply trying to earn extra money for renting out their social media accounts.

Similar innovative thinking regarding spreading disinformation on social media has been used in the past in the Baltic countries. For example, in Estonia, during the seven months prior to the 2019 March parliamentary elections, pro-Russian actors created hundreds of fake accounts that appeared legitimate – it took diligent effort from investigative journalists to prove that the accounts were managed by individuals residing in Russia (Propastop, 2019).

6 The APT28 that is affiliated to the Russian military intelligence service was also found on the commission's systems (Koval, 2015).

In mid-March doxing (which means hacking into internal databases and broadcasting the stolen data such as emails publicly on the Internet) was used against Petro Poroshenko, the incumbent president of the country who also ran as a candidate in the March elections. A large dossier of stolen emails was published with an aim to show that the president and his associates hid money made in Russia offshore (Stack, 2019). The Ukrainian authorities did not attribute these cyber-attacks, but it is safe to assume that the purpose of the hacking was to impact the opinion and behavior of voters in the March elections.

In October 2018, researchers at the Atlantic Council anticipated that Russian-sponsored "cyber operations will likely compromise networks that deal directly with vote tallying and result presentation, exploit civil and financial-sector institutions, and technically manipulate media outlets and campaigns' digital efforts" (The Atlantic Council, 2018). While some of these tactics were used, fortunately there were no successful cyber-attacks against the election systems on the day of the election. However, DoS attacks against the Central Election Commission's website and many state institutions were reported by the authorities; and there were attempts to intrude the Central Election Commission's networks (The Security Service of Ukraine, 2019).[7]

To conclude, the Ukrainians were able to halt many hacking attempts and identify social media influence campaigns in the months prior to the elections. Even though social media companies were late to stop the spread of Russia's propaganda (fake accounts were taken down just a few weeks before the elections), the Ukrainians were prepared and had relatively good early warning and monitoring of their information and cyberspace.

7 Further information of these cases is available at the news section on the website of the Security Service of Ukraine.

SUPPORT TO UKRAINE FROM THE INTERNATIONAL COMMUNITY

One reason for this success was that Ukraine was actively cooperating with strategic partners before the elections: a cyber dialogue with the United States where cyber threats and cooperation including the security of election systems and critical infrastructure were discussed in November 2018. Ukraine has also received financial assistance from the US to foster election security (Ministry of Foreign Affairs of Ukraine, 2018). In cooperation with domestic and American think tanks Kiev has set up a rapid reaction team – dubbed a Ukrainian Election Task Force – whose objective is to monitor, evaluate, and disclose the full range of foreign subversive activities in the country as well as to propose suitable responses to them (The Atlantic Council, 2018).

According to the previous president Poroshenko, the US, but also Germany and France sent their cyber experts to the Ukraine to assist in the protection of election infrastructure (Ukrinform, 2018).

In addition to these large NATO allies, NATO provides a cyber security capacity building in Ukraine. The assistance includes discussions among subject matter experts, and support to the development of a cyber security strategy and cybersecurity curriculum (NATO, 2018).

The EU organized a table-top exercise for Ukrainian election staff and other domestic stakeholders where responses to cyber-attacks against the election process were rehearsed (The Security Service of Ukraine). The EU also has longer-term assistance projects supporting cyber security in Ukraine, such as the European Union Advisory Mission which provides training and other assistance in the aera of election security and countering cybercrime. (EUAM Ukraine, 2019).

AN EXAMPLE OF RUSSIA'S ATTEMPT TO INFLUENCE THE EUROPEAN PARLIAMENT ELECTIONS IN GERMANY

Naja Bentzen (2018, p. 10) claims: „In a January 2018 debate on the influence of Russian propaganda on EU countries, Members of the European Parliament warned that the upcoming EU elections in May 2019 are likely to be the next big target for Russian disinformation". For that reason the Ukrainian experience from the 2014 and 2019 elections and also the experiences of other countries (US presidential elections 2016, presidential elections in France 2017 etc.) should be taken in to consideration during the European Parliament elections. One Russian tool to influence the European Parliament elections is using politicians, who get financial support from Moscow like in the case of Markus Frohnmaier from die Alternative für Deutschland, who is also a member of Deutsche Bundestag. It is suspected that Markus Frohnmaier is a Russian marionette (Focus, 2019). It is known that the Kremlin provides support to right radical parities, groups and movements in Europe, supporting populism, left radicals. One of the Russian tools of influence is destabilization, organizing chaos in the political landscape of Europe prior to elections. Ukrainian expert Yevhen Mahda accentuated that Russia is considering a scenario of destabilization in the Ukraine as an element of destabilizing Europe prior to the forthcoming elections to the European Parliament. By destabilizing Ukraine, Moscow's aim is to create fear and discomfort in Europe, in the European political circle, Moscow's purpose is to create political chaos and destabilization in the European Parliament by influencing elections (Магда, 2019).

THE EU'S RESPONSE TO DISINFORMATION AND CYBER-ATTACKS

According to Julian King, the European Commissioner for Security, the European Parliament elections "present a tempting target for malicious actors." The elections last for several days in 28 countries, which have different electoral systems and diverse electronic means for communicating the results, as well as different maturity levels of cyber security and awareness of the public about hybrid threats. As discussed earlier, successful cyber-attacks have been launched against the election processes in many European countries (for example, Poland, Bulgaria, Germany, Czech Republic, and Finland) and there is no reason to expect that the European Parliamentary elections will be an exception (Cerulus, 2019).

Since mid-2018 the EU has adopted a broad set of measures to increase election security (European Commission, 2019).[8] In July 2018 the EU published the Compendium on Cyber Security of Election Technology gathering best practices and providing guidelines on improving the protection of the election processes, including the European Parliament elections. The authors warn that a successful campaign against one member state could compromise the entirety of the election processes and affect the very functioning of the EU. They pinpoint that while each country has a different electoral system there is common shared vulnerability at the union level which is "the communication of the results from capitals to Brussels and the display of the results." While national level elections (local, municipal, parliamentary, presidential) take place every couple of years, the elections to the European Parliament are held only once in five years imposing additional security risks due to the lack of regularity and the changed security environment.[9] The EU's election package from September 2018 (Communication and Recommendation) called the member states to cooperate with media, online platforms, technology companies, and other stakeholders in conducting awareness raising campaigns. It was anticipated that these campaigns would increase trust and transparency of the election processes (Joint Communication, 2018).

The EU has also launched national and European election cooperation networks to discuss among other issues cyber threats to the European Parliament elections and share best practices. The European election cooperation network has met in 2019 three times (European Commission, 2019). In April, the European Parliament, the Commission, the EU Agency for Cybersecurity (ENISA) together with member states organized an exercise to test the response to and crisis plans for potential cyber security incidents against the European Parliament elections (European Commission, 2019).

The EU Action Plan against Disinformation from December 2018 sets up a variety of approaches and countermeasures against disinformation (European Commission, 2019). Technology and social media companies Google, Facebook, Twitter, and Mozilla signed in October 2018 a Code of Practice on Disinformation and provided implementation reports in January 2019 to the EU (European Commission, 2019). In March 2019 the EU launched a digital platform to share information in real-time about disinformation campaigns. The Rapid Alert System provides tools for coordinating responses to disinformation (European Union External Action Service, 2019).

8 These include the Communication, Recommendation, Guidance Document of the European Commission from September 2018.
9 The Document provides practical and workable measures to secure the technology involved in elections.

In addition, in March the European Commission called national political parties to implement a set of measures aimed at reducing the risks to European Parliament elections (European Commission, 2019). The EU's framework of Horizon 2020 includes several actions aimed at developing technological tools for online content verification. Finally, in June 2019 the Romanian Presidency, the European Commission and the High Representative will present to the European Council a report about lessons learnt on fighting disinformation.

RECOMMENDATIONS

In addition to the EU's broad range of protective activities against cyber-attacks and disinformation the EU should consider taking the following steps.

First, research community and technology companies should analyze the specific ways and means on how Russia has attempted to influence elections in the past. The most obvious case studies are Ukraine, France, Germany, Montenegro and the US. The case studies should elucidate counter-measures implemented by the target countries, and give recommendations on best practices to be replicated in the future.

Second, while the cooperation between member states and at the EU level should be improved. More financial support should be made available from the European Commission especially for non-governmental organisations and research institutions.

Third, EU member states should work with other stakeholders (online platforms, technology companies, internet service providers, researchers and computers scientists, civil society organizations, etc.) to continuously develop innovative approaches to counter psychological and technological attacks against democratic processes. More support from the governments is needed to speed up the development of new technological tools (algorithms, applications to identify deep fakes and disinformation, machine learning, deep learning, etc.). For example, in a few years the Transatlantic Commission on Election Integrity will make available an application that scans videos on popular social media channels such as Youtube, WhatsApp, etc. and filters deep fakes. Similar applications should be made available to European citizens in their languages.

Forth, more should be done to increase awareness of the Russophone community in members states, especially in the Baltic states and Germany about the harmful influences of Russian disinformation and cyber activities (Saunders, 2014).

REFERENCES

Alyukov, Maxim 2018. Conspiracy theory has gone mainstream in Russia. But how does it work? *Open Democracy*. 7 September 2018, https://www.opendemocracy.net/od-russia/maxim-alyukov/conspiracy-theory-has-gone-mainstream-in-russia (accessed: 22.2.2019).

Belfer Center for Science and International Affairs, Harvard Kennedy School, 2018. The State and Local Election Cybersecurity Playbook. https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook. (accessed: 15.4.2019).

Bentzen, Naja 2018. Foreign influence operations in the E, p.10, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf?fbclid=IwAR2e_lo75tqC92ZTChcjh8LD7tPsbXd408JDFZrBXB-JZUYn-A5umtI9A4z0 (accessed: 8.4.2019).

Berzinš, Janis 2014. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy". Policy Paper No. 2 (April 2014). National Defence Academy of Latvia, Center for Security and Strategic Research.

Bugayova, Nataliya 2019. How we got here with Russia: The Kremlin's worldview. March 2019, http://www.understandingwar.org/sites/default/files/ISW%20Report_The%20Kremlin%27s%20Worldview_March%202019.pdf (accessed: 15.4.2019).

Cerulus, 2019. Europe's most hackable election. Politico. 24 January 2019, https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/ (accessed: 15.4.2019).

Coats, Dan 2019. Remarks as prepared for delivery by The Honorable Dan Coats Director of National Intelligence Annual Threat Assessment Opening Statement Tuesday. 29 January 2019. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf (accessed: 15.4.2019).

Conley, Heather A., Ruy, Donatienne; Stefanov, Ruslan & Vladimirov, Martin 2019. The Kremlin Palybook 2. The Enablers. CSIS. Washington: Roman & Littlefield. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190326_KP2.pdf. (accessed: 15.4.2019).

International Organisation for Standardization, 2018. ISO/IEC 27000:2018 (E). https://www.iso.org/standard/73906.html (accessed: 15.4.2019).

Darczewska, Jolanta, 2014. The Anatomy of Russian Information Warfare: The Crimean operation, a case study. Point of View 42 (May 2014). Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia (Centre for Eastern Studies).

Darczewska, Jolanta & Żochowski, Piotr, 2015. Russophobia in the Kremlin's Strategy. A Weapon of Mass Destruction. – Point of View, No. 56, October. Warsaw: Centre of Eastern Studies (OSW), https://www.osw.waw.pl/en/publikacje/point-view/2015-11-02/russophobiakremlins-strategy-a-weapon-mass-destruction>. (accessed: 28.2.2019).

Estonian Internal Security Service Annual Review 2018. Compiled by: Harrys Puusepp.

EUAM Ukraine, 2019. EUAM brings together police, civil society and state authorities in Odesa ahead of elections. 19 February 2019, http://www.euam-ukraine.eu/news/euam-brings-together-police-civil-society-and-state-authorities-in-odesa-ahead-of-elections/ (accessed: 15.4.2019).

EUAM Ukraine, 2019. EUAM donation supports intelligence-led policing and fight against cyber crime. 15 February, http://www.euam-ukraine.eu/news/euam-donation-supports-intelligence-led-policing-and-fight-against-cyber-crime/ (accessed: 15.4.2019).

EUAM Ukraine, 2019. EUAM launches first series of training for investigators of the State Bureau of Investigations. 14 March 2019, http://www.euam-ukraine.eu/news/euam-launches-first-series-of-training-for-investigators-of-the-state-bureau-of-investigations/ (accessed: 15.4.2019).

European Commission, 2018. Code of Practice on Disinformation. 26 September 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (accessed: 15.4.2019).

European Commission, 2019. Action Plan on disinformation: Commission contribution to the European Council (13-14 December 2018), https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en (accessed: 15.4.2019).

European Commission, 2019. Code of Practice on Disinformation. 29 January 2019. Code of Practice on Disinformation. https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en (accessed: 15.4.2019).

European Commission, 2019. Electoral rights. European Parliament elections. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights_en#electionsnetwork (accessed: 15.4.2019).

European Commission, 2019. Electoral rights. European Parliament elections. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights_en#electionsnetwork (accessed: 15.4.2019).

European Commission, 2019. EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections. 5 April 2019, http://europa.eu/rapid/press-release_IP-19-2011_en.htm (accessed: 15.4.2019).

European Commission, 2019. European Commission calls on national political parties to join efforts to ensure free and fair elections in Europe. 15 March 2019, http://europa.eu/rapid/press-release_IP-19-1672_en.htm (accessed: 15.4.2019).

European Union External Action Service, 2019. Factsheet: Rapid Alert System. 15 March 2019, https://eeas.europa.eu/headquarters/headquarters-homepage_en/59644/Factsheet:%20Rapid%20Alert%20System (accessed: 15.4.2019).

Focus, 2019. Wie Putin einen „unter absoluter Kontrolle stehenden“AfD-Abgeordneten installierte, Focus, 5. April 2019, https://www.focus.de/politik/deutschland/russische-marionette-im-bundestag-afd-frohnmaier-russland_id_10555974.html (accessed: 15.4.2019).

Graham Stack, 2019. “Ukrainian Papers” - massive business data leak embroils Poroshenko in a new corruption scandal. bne IntelliNews. 14 March 2019, http://www.intellinews.com/ukrainian-papers-massive-business-data-leak-embroils-poroshenko-in-a-new-corruption-scandal-157953/. (accessed: 15.4.2019).

Greenberg, Andy 2018. The untold story of NotPetya, the most devastating Cyber-attacks in the history. *Wired.* 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed: 15.4.2019).

Karlsen, Geir Hågen 2019. Divide and rule: ten lessons about Russian political influence activities in Europe. Palgrave Communications 5: 19, pp. 1-14.

Kiselyov, V.A., 2017. What Kind of Warfare Should the Russian Armed Forces Be Prepared for? *Military Thought* 26(2) (2017).

Koval, Nickolai, 2015. Revolution Hacking. In Kenneth Geers (Ed.). Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications.

Kowalik, Tomasz K. & Jankowski, Dominik P. 2017. The Dangerous Tool of Russian Military Exercises. Center for European Policy, 09.05.2017, http://cepa.org/EuropesEdge/The-dangerous-tool-of-Russian-militaryexercises (accessed: 28.2.2019).

Ministry of Foreign Affairs of Ukraine, 2018. Second Ukraine – U.S. Cybersecurity Dialogue takes place at Ukraine’s Foreign Ministry. https://mfa.gov.ua/en/press-center/news/68316-mzs-ukrajini-vidbuvsya-drugij-raund-mizhvidomchih-ukrajinsyko-amerikansykih-konsulytacij-u-sferi-zabezpechennya-kiberbezpeki (accessed: 15.4.2019).

Mölder, Holger & Sazonov, Vladimir 2018. Information Warfare as the Hobbesian concept of Modern Times – Principles, Techniques and Tools of Russian Information Operations in Donbass, Journal of Slavic Military Studies, 31 (3), 2018, pp. 308–328.

Müür, Kristiina, Mölder, Holger; Sazonov, Vladimir & Pruulmann-Vengerfeldt, Pille 2016. Russian Information Operations against the Ukrainian State and Defence Forces: April-December 2014 in Online News. Journal on Baltic Security 2 (1), pp. 28–71.

NATO StratCom COE 2015. The Manipulative Techniques of the Russian Information Campaign Against Ukraine. http://www.stratcomcoe.org/manipulative-techniques-russian-information-campaign-against-ukraine (accessed: 12.3.2018).

NATO, 2018. Enhancing cybersecurity in Ukraine. 29 October 2018, https://www.nato.int/cps/en/natohq/news_159840.htm?selectedLocale=en

NATO, 2018. Relations with Ukraine. 14 June 2018, https://www.nato.int/cps/en/natohq/topics_37750.htm (accessed: 15.4.2019).

NIS Cooperation Group, 2018. Compendium on Cyber Security of Election Technology. July 2018.

Nissen, Thomas Elkjer, 2015. The weaponization of social media. Royal Danish Defence College, Copenhagen, 2015, http://www.fak.dk/publikationer/Documents/The%20Weaponization%20of%20Social%20Media.pdf?pdfdl=theweaponizationofsocialmedia?pdfdl=TheWeaponizationOfSocialMedia (accessed: 28.2.2019).

Pohjapalo, Kati 2019. Finland Detects Cyber Attack on Online Election-Results Service. Bloomberg. 10 April 2019, https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service (accessed: 15.4.2019).

Propastop, 2019. Over one hundred fake accounts are connected with #ESTexitEU. 8 January 2019, https://www.propastop.org/eng/2019/01/08/over-one-hundred-fake-accounts-are-connected-with-estexiteu/ (accessed: 15.4.2019).

SafeGuardCyber 2019. Contacless Actions Against the Enemy: How Russia Is Deploying Misinformation on Social Media to Influence European Parliamentary Elections

https://cdn2.hubspot.net/hubfs/3918364/SafeGuardCyber_November2017/New%20White%20Papers/SafeGuardCyber_Contactless%20Actions%20Against%20the%20Enemy%20-%20EU%20Elections_May2019%20(1).pdf (accessed: 8 May 2019)

Saunders, Robert A. 2014. The Geopolitics of Russophonia: The Problems and Prospects of Post-Soviet "Global Russian. – Globality Studies Journal 40, 15 July, https://gsj.stonybrook.edu/article/the-geopolitics-of-russophonia-the-problems-and-prospects-of-post-soviet-global-russian/ (accessed: 2 May 2019)

Spriņģe, Inga, 2018. How Russian Propaganda Becomes Even Nastier in Baltic News. – Re:Baltica, 29.03.2018, https://en.rebaltica.lv/2017/03/how-russian-propaganda-becomes-even-nastierin- baltic-news/ (14. 03.2019) (accessed: 15.4.2019).

Schwirtz, Michael & Sheera, Frenkel, 2019. In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering. The New York Times, 29 March 2019, https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html (accessed: 15.4.2019).

Stoicescu, Kalev 2009. Estonian Foreign Intelligence Service Yearbook 2019, ICDS, blog, 13 March 2019, https://icds.ee/estonian-foreign-intelligence-service-yearbook-2019/ (accessed: 4.5.2019).

The Atlantic Council, 2018. Ukrainian Election Task Force—Exposing Foreign Interference in Ukraine's Democracy. Issue Brief. https://www.atlanticcouncil.org/images/publications/Ukrainian-Election-Task-Force-Exposing-Interference-in-Ukraines-Democracy1.pdf (accessed: 15.4.2019).

The Security Service of Ukraine, 2019. News. https://ssu.gov.ua/en/search?search_request=cyber&news=1 (accessed: 15.4.2019).

The Security Service of Ukraine, 2019. News. https://ssu.gov.ua/en/search?search_request=cyber&news=1 (accessed: 15.4.2019).

The Security Service of Ukraine, 2019. SBU exposes Internet propagandist on discrediting electoral process, tasked by Russian Special Services (video). 11 April 2019, https://ssu.gov.ua/en/news/1/category/21/view/5964#.53KDswqg.dpbs (accessed: 15.4.2019).

The Security Service of Ukraine, 2019. SBU hosts international training on cyber-security for CEC systems. 6 March 2019, https://ssu.gov.ua/en/news/1/category/1/view/5806#.OGkRmHfC.dpbs (accessed: 15.4.2019).

Ukrinform, 2018. Poroshenko: International experts already enhancing cyber security on eve of election. 17 October 2018, https://www.ukrinform.net/rubric-polytics/2560392-poroshenko-international-experts-already-enhancing-cyber-security-on-eve-of-election.html (accessed: 15.4.2019).

Välisluureamet 2019 = Eesti rahvusvahelises julgeolekukeskonnas 2019, Välisluureamet, https://www.valisluureamet.ee/pdf/raport-2019-EST-web.pdf (accessed: 4.5.2019).

Ventsel, Andreas & Sazonov, Vladimir, 2018. Russofoobia mobiliseeriv jõud. – Postimees, 26.06.2018, https://arvamus.postimees.ee/4509822/andreas-ventsel-ja-vladimir-sazonovrussofoobia- mobiliseeriv-joud (14. 03.2019) (accessed: 15.4.2019).

Vilmer, Jean-Baptiste Jeangène; Escorcia, Alexandre; Guillaume, Marine & Herrera, Janaina 2018. Information Manipulation: A Challenge for Our Democracies. The Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. Paris. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (accessed: 15.4.2019).

Winnerstig, Mike (ed.) 2014. Tools of Destabilization. Russian Soft Power and Non-military Influence in the Baltic States. Report FOI-R-3990-SE. Stockholm: FOI (Swedish Defence Research Agency)

Yablokov, Ilya 2015, Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT), Politics 35 (3-4), 2015, 301-315.

In Ukrainian and Russian

Belikov = Беликов, Олег 2019. Как Россия будет влиять на выборы в Украине и как противодействовать этому влиянию. 24канал. 4.2.2019, https://24tv.ua/ru/kak_rossija_budet_vlijat_na_vybory_v_ukraine_i_kak_protivodejstvovat_jetomu_vlijaniju_n1106782?fbclid=IwAR1qKb6dcsaUOXvsndqGbFv_5YSNYN6SMIw92Zd-5YLJH-rfYmiGvg8RUu0 (accessed: 8.4.2019).

Внешнее давление на выборы 2019: на какие манипуляции и вмешательства следует ожидать? Ukrininform. 20.3.2019, https://www.ukrinform.ru/rubric-presshall/2660507-vnesnee-davlenie-na-vybory-2019-na-kakie-manipulacii-i-vmesatelstva-sleduet-ozidat.html?fbclid=IwAR3koseWBQDxbF-RtmHGvZqOCWGRVPfNBgerGCSbU_-SQP1itqQE6RC0ELU (accessed: 8.4.2019).

Магда, Евгений, 2019. Украинские выборы и интересы Кремля. International Centre for Defence and Security, Estonia. 25 March 2019, https://icds.ee/ru/ukrainskie-vybory-i-interesy-kremlja/ (accessed: 15.4.2019).

MK.ru, 2019. В Госдуму внесен проект заявления о непризнании итогов украинских выборов. MK.ru, 27.03.2019, https://www.mk.ru/politics/2019/03/27/v-gosdumu-vnesen-proekt-zayavleniya-o-nepriznanii-itogov-ukrainskikh-vyborov.html?fbclid=IwAR3Sbz0_XTd0iZJUEghQFE-uw4XTQDhw2VuoBFas1wovMMinlZwdGdk_lS4 (accessed: 8.4.2019).

Regnum, 2019 = «Не признавать и точка»: Как отреагирует Россия на выборы на Украине? Regnum, 6.2.2019, https://regnum.ru/news/2566873.html?fbclid=IwAR2Lj0Mnn0cBV1xzOoyc5aOyJt0DNrptI3WmHBlKZMssh6feWYVJFe4OzAQ (accessed: 8.4.2019).

Telekanal Dozhd, 2014 = Первый канал показал «фейковые» данные о победе Яроша на президентских выборах. Телеканал Дождь, 27.5.2014, https://www.youtube.com/watch?v=qRUEBsig4JY (accessed: 8.4.2019).

Штогрін, Ірина, 2019. «Привид громадянської війни». Росія використовує вибори, щоб «хаотизувати» Україну, Radio Svoboda, 29 March 2019, https://www.radiosvoboda.org/a/vybory-rosija-xaos/29849885.html?fbclid=IwAR0-wEv4vaN_CykX0ALDGZ-_Dv8u3XWmfUXL9qYPVQljCfNjpq59PqAt2bE (accessed: 8.4.2019).

Youtube, 2014. ОБРАЩЕНИЕ ВЛАДИМИРА ЗЕЛЕНСКОГО К ЯНУКОВИЧУ И ПУТИНУ, 2014, https://www.youtube.com/watch?v=KZteEACYdgE (accessed: 8.4.2019).

Zn.ua, 2019, Российские хакеры пытаются получить доступ к сетям государственных органов Украины — глава Киберполиции, 17 March 2019, https://zn.ua/POLITICS/rossiyskie-hakery-pytayutsya-poluchit-dostup-k-setyam-gosudarstvennyh-organov-ukrainy-glava-kiberpolicii-312012_.html?fbclid=IwAR2cWVZqLk5C696e5gbuU5SkYN0nNmeYQ749HexPqSyouiELDVEH5LNZwrY

Interviewed

Interview with Dr. Seregi Pakhomenko, Political expert 29.3.2019, Facebook.

Interview with Dr. Dmitry Dubov, Political expert 29.3.2019, Facebook.

Interview with Dr. Yevgen Mahda, Political expert, 29.3.2019, Facebook.

Interview with Kostiantyn Romashko, Manager of EU-related projects, Internews Ukraine, 2.4.2019, gmail.com.