UA: UKRAINE ANALYTICA

Issue 1(11), 2018

- DISINFORMATION CAMPAIGNS
- FAKE NEWS
- INFLUENCE OPERATIONS

UA: UKRAINE ANALYTICA

Issue 1 (11), 2018

Propaganda

Editors
Dr. Hanna Shelest
Dr. Mykola Kapitonenko

Publisher:
Published by NGO "Promotion of Intercultural Cooperation" (Ukraine), Centre of International Studies (Ukraine), with the financial support of the Representation of the Friedrich Ebert Foundation in Ukraine, and the Black Sea Trust.

UA: Ukraine Analytica is the first Ukrainian analytical journal in English on International Relations, Politics and Economics. The journal is aimed for experts, diplomats, academics, students interested in the international relations and Ukraine in particular.

Contacts:
website: http://ukraine-analytica.org/
e-mail: Ukraine_analytica@ukr.net
Facebook: https://www.facebook.com/ukraineanalytica
Twitter: https://twitter.com/UA_Analytica

The views and opinions expressed in articles are those of the authors and do not necessarily reflect the position of UA: Ukraine Analytica, its editors, Board of Advisors or donors.

ISSN 2518-7481

500 copies

BOARD OF ADVISERS

TABLE OF CONTENTS

THE KREMLIN’S INFORMATION WARS IN THE 21ST CENTURY: ESTONIA, GEORGIA, UKRAINE

Maksym Kyiak, PhD
Central European Institute, Ukraine

The article deals with the use of information warfare during the so-called “Bronze Night” events in Estonia in 2007, the Russian-Georgian war in 2008, and the Russian aggression against Ukraine since 2014. The events in Estonia are described as the first large-scale usage of cyber warfare combined with disinformation against a sovereign state. The war against Georgia is presented as the very first usage of military actions together with cyber-attacks and disinformation. And the ongoing Russian aggression against Ukraine is described as an example of combining of the most effective information warfare tactics applied in Estonia and Georgia together with new information warfare tools. All three examples are presented as the cornerstones for understanding the main peculiarities of the Kremlin’s modern information warfare.

In memoriam of my father, Professor and Member of the Parliament of Ukraine Taras Kyiak.

The Military Doctrine of the Russian Federation (December 2014) stated a significant role of information, which was confirmed by the attempted annexation of Crimea, the Kremlin’s aggression in Donbas, and events in Syria. Moreover, the Kremlin views the information sphere as a key domain for modern military conflict.[1] The new version of the Doctrine of Information Security signed by the Russian president V. Putin in December 2016 addresses the important status of information technologies during conflicts between states. According to the doctrine, one of the main threats to Russia is “the scale of the use of information-psychological influences by the special services of certain states”.[2] One of the main goals of the Russian government in the new doctrine is the strengthening of the vertical management and the centralization of information security at all levels.[3]

[1] *Russia Military Power 2017*, “Defence Intelligence Agency”, 28 June 2017, [http://www.dia.mil access: 05 August 2017].

[2] *Доктрина информационной безопасности Российской Федерации (The Doctrine of Information Security of the Russian Federation)*, “RG.ru”, December 2016, [https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html access: 07 January 2017].

[3] N. Nikolaichuk, *Стратегическая информационная операция может быть скоротечной, а может длиться годами (Strategic Information Operation Can Be Fast or Can Last for Years)*, “Столетие”, 22 October 2014 [http://www.stoletie.ru/politika/igor_nikolajchuk_strategicheskaja_informacionnaja_operacija_mozhet_byt_skorotechnoj_a_mozhet_dlitsa_godami_185.htm access: 12 October 2017].

The Kremlin actively used information warfare during the events in Estonia in 2007 regarding the so-called "Bronze Soldier" monument, in the Russian-Georgian war in 2008, and also has been doing so during the Russian aggression against Ukraine since 2014. Those three cases are the cornerstones for understanding the Kremlin's modern information warfare, which has improved with every next conflict. Despite the fact that the experience of these countries is often neglected, they have become not only a testing ground but also a demonstration ground for the Kremlin's information warfare capabilities. At the same time, those states have experienced much more information warfare used against them than the majority of the Western countries have.

> ***The Kremlin actively used information warfare during the events in Estonia in 2007 regarding the so-called "Bronze Soldier" monument, in the Russian-Georgian war in 2008, and also has been doing so during the Russian aggression against Ukraine since 2014***

The Kremlin's Information Warfare and "Bronze Night" in Estonia, 2007: The First Move

Since the collapse of the Soviet Union, the Baltic states have been perceived as a part of the Russian geopolitical interests. As a result, the Baltic countries have been portrayed by the Kremlin's media as xenophobic, hostile, and different from the rest of Europe. The best-known usage of disinformation techniques and the factor of ethnic Russians in the Baltics occurred in Estonia in 2007 during the so-called "Bronze Night" or the "Bronze Soldier" event. On 26-27 April 2007, Estonia experienced one of the most tragic days in its modern history. The trigger was the relocation of the memorial for the Soviet soldier from the center of Tallinn to the military cemetery.

The monument was erected in 1947 by the Soviet authorities, but remained in place during the collapse of the Soviet Union and no serious attempts were made to remove it until 2006. It has to be mentioned that there is a fundamentally different perception of the role of Soviet soldiers in Estonia during and after World War II. For ethnic Russian Estonian citizens, they were liberators. And for ethnic Estonians, they were unwelcome occupiers.

The debates initiated by the ethnic Estonians to remove the monument became more prominent in 2006.[4] In January 2007, the Estonian government announced that the monument would be moved from the center of Tallinn to a military cemetery on the outskirts of the city. On 26 April 2007, the monument area was fenced off and a day later, immediately after an emergency meeting of the Estonian government, the monument was relocated. It provoked riots in the center of Tallinn, accompanied by cyber-attacks against Estonian government agencies and by diplomatic pressure from the Russian Federation.[5]

[4] M. Ehala, *The Bronze Soldier: Identity, Threat and Maintenance in Estonia*, "Journal of Baltic Studies", 2009, [http://lepo.it.da.ut.ee/~ehalam/pdf/Identity%20threat.pdf access: 03 March 2017].

[5] K. Liik, *The 'Bronze Year' of Estonia-Russia Relations*, International Centre for Defence and Security, 2007, [https://www.icds.ee/fileadmin/media/icds.ee/failid/Kadri_Liik_Bronze_Year.pdf access: 10 June 2017].

[6] G. Gigitashvili, *Russia's Hybrid Warfare at Work in Estonia*, "New East Platform", 05 October 2015, [https://www.academia.edu/23006907/Russian_Hybrid_war_at_work_in_Estonia access: 09 November 2017].

The riots resulted in 153 injuries and 800 arrests.[6] Dmitri Ganin, a Russian who was killed with a knife during the protests, was portrayed by the Russian media as a victim of police actions, though this incident happened about 500 meters from the monument. The Russian media were producing fake news and spreading rumors about the number of people killed and claiming that the Estonian police were torturing ethnic Russians in "secret prisons".[7] The Kremlin's disinformation portrayed the Estonians as fascists and stated that they were discriminating against the Russians. At the same time, those protestors who took part in riots and smashed windows and stole merchandise from the shops were labeled as "peaceful demonstrators" by the Russian media.[8]

As it was already mentioned, together with disinformation and fake news, cyber warfare was used. Most of the cyber-attacks were DDoS (Distributed Denial of Service) using networks of bots or robots to send out massive numbers of signals to specific addresses to overload servers until they finally shut down.[9] The primary target of the first wave of such attacks, which was relatively simple and lasted from 27 April to 29 April, was the Estonian prime minister's website. The official website of the Estonian government was not available for eight hours in the afternoon of 28 April.[10] The Estonian news outlet "Postimees Online" also became a target of two DDoS attacks on its servers, which limited the chances for Estonia to be heard abroad.[11] Many attacks were implemented with the help of computer servers and networks located in Russia. Furthermore, instructions on Russian websites in the Russian language showed on how, when, and what to attack on websites, in forums, and in chat spaces.[12]

The intensity and sophistication of cyber-attacks increased during the second wave (30 April-18 May 2007). They became more complex, varied, and focused on different targets. Between 3 May and 17 May, there were 128 separate DDoS attacks on Estonian websites. Out of these, 106 attacks were concentrated on three websites – the Ministry of Finance, the Police and Border Guard, and the websites of the Estonian government and prime minister.[13] Among other targets were the websites of the Estonian presidency and parliament, almost all government ministries, political parties, three of the country's biggest news organizations, two of the biggest banks, and also firms specializing in communications. The Estonian minister of defense stated that the cyber-attacks on the state servers were a military aggression and some of the attacks originated in Russian state institutions. Moreover, the leader of the pro-Kremlin youth movement "Nashi" admitted launching some of the cyber-attacks.[14]

[7] *Таллинский расчет (Tallinn's Reckoning)*, "НТВ (NTV)", 2011, [https://www.youtube.com/watch?v=m8cpFAMoJGQ access: April 2017].

[8] M. Kyiak, *Countering Kremlin's Disinformation in Baltic and Eastern Europe*, "Baltic Worlds", 01 December 2016, [http://balticworlds.com/countering-kremlins-disinformation-in-baltic-and-eastern-europe access: December 2017].

[9] *Prepared Testimony and Statement for Record of Toomas Hendrik Ilves*, 09 March 2017, [http://docs.house.gov access: 10 March 2017].

[10] A. Schmidt, *The Estonian Cyberattacks*, 2013, [http://www.researchgate.net access: 09 April 2017].

[11] A. Schmidt, *The Estonian Cyberattacks*, 2013, [http://www.researchgate.net access: 09 April 2017].

[12] A. Schmidt, *The Estonian Cyberattacks*, 2013, [http://www.researchgate.net access: 09 April 2017].

[13] A. Radin, *Hybrid Warfare in the Baltics*, "RAND", 2017, [https://www.rand.org/pubs/research_reports/RR1577.html access: July 2017].

[14] D. Denning, *Tracing the Sources of Today's Russian Cyber Threat*, "Scientific American", 18 August 2017, [https://www.scientificamerican.com/article/tracing-the-sources-of-today-rsquo-s-russian-cyberthreat access: 25 August 2017].

War against Georgia, 2008: Kremlin Steps out of the Shadow

The war against Georgia lasted for only five days, but the implications of what had happened were far more enduring.[15] It was caused by many complex factors: geopolitical, legal, cultural, and economic. The 1992 South Ossetia War and the 1993 Abkhazian War led to Georgia's loss of these regions to unrecognized pro-Russian local governments. In 2003-2004, a pro-Western government came to power in Georgia following the Rose Revolution. In 2006, four employees of the Russian GRU (Chief Intelligence Service) were accused of spying and were arrested in Georgia. The Kremlin's reaction was the deportation of three thousand Georgians from the Russian Federation. Then the banning of Georgian wine and mineral water followed. During 2007-2008, several articles about the necessity of a military operation against Georgia appeared.[16] Moreover, in June-July 2008, Russian railroad troops made repairs of 54 kilometers of the railroad track in Abkhazia. Those railway links were important to the deployment of mechanized Russian units. In July 2008, the military exercise "Caucasus 2008" took place. Some of the units involved in this exercise later took part in the military operation against Georgia.

> ***One of the Kremlin's main goals during this war was to discredit and isolate the Georgian government inside Georgia and in front of foreign countries***

Although Georgia lost this short war, it still managed not to lose the information front. Almost immediately after the start of the war, the Georgian government stopped broadcasting Russian TV channels and blocked access to Russian websites. In August 2008, there was a vacuum of information in the media while many foreign reporters were on holiday.[17] Consequently, Georgia was successful in convincing the international community that the big Russia was attacking a small state.

The Georgian government set up a media center in a hotel lobby in central Tbilisi. Journalists had access to updated military maps posted with troop movements. Foreign journalists in Tbilisi were briefed several times a day. Within hours after the beginning of the war, the Georgian government began issuing hourly e-mail updates for foreign journalists.[18] Government officials conducted international telephone conferences with reporters who were outside Georgia.[19] Georgia had a media staff of 60 volunteers, who were organized into teams. All information collected during

[15] A. Jugaste, *Communicating Georgia: Georgia's Information Campaign in the 2008 War with Russia*, Tartu University, 2011, [http://ut.ee access: April 2017].

[16] O. Panfilov, *Как Россия не смогла захватить Грузию в 2008 (How Russia Couldn't Conquer Georgia in 2008)*, "Inforesist", 03 January 2017, [https://inforesist.org/kak-rossiya-tak-i-ne-smogla-zahvatit-gruziyu-v-2008-godu access: 04 May 2017].

[17] A. Jugaste, *Communicating Georgia: Georgia's Information Campaign in the 2008 War with Russia*, Tartu University, 2011, [http://ut.ee access: April 2017].

[18] C. King, *The Five-Day War: Managing Moscow after the Georgia Crisis, "Foreign Affairs"*, 01 January 2008, [http://foreignaffairs.com access: 10 March 2017].

[19] A. Jugaste, *Communicating Georgia: Georgia's Information Campaign in the 2008 War with Russia*, Tartu University, 2011, [http://ut.ee access: April 2017].

the day was distributed the next day in the form of Georgia Update, the government's newsletter that existed before the war. Georgia Update also included international media coverage of the war to show the Western support.

One of the Kremlin's main goals during this war was to discredit and isolate the Georgian government inside Georgia and in front of foreign countries. Georgia was presented as a puppet aggressor, which had violated both international law and human rights.[20] Another target of the Kremlin's information war was the Georgian army. The Kremlin hoped to induce panic and demoralization among inexperienced Georgian soldiers.

According to the Kremlin's frame, the reason behind "Georgia's aggression" was its nationalist and violent government. This message appeared in 41% of the statements issued by the Russian Ministry of Foreign Affairs. Moscow explained its presence on the territory of Georgia as "a peacekeeping mission" and as historical guarantees for the "people of Caucasus".[21] Russian senior officials used such international legal and emotional terms as "genocide", "ethnic cleansing in South Ossetia", and "humanitarian catastrophe in Ossetia". The Kremlin argued that Russia was forced to use its military because of the sudden actions of the Georgian army. The Russian media even attempted to prove the existence of US citizens in the Georgian army to discredit it.[22]

Unlike the cyber-attacks against Estonia in 2007, cyber-attacks against Georgia were accompanied by military combat. When tanks, airplanes, and troops were crossing the border, Georgian citizens were not able to access websites for information and instructions. Cyber-attacks also degraded the ability of the Georgian government to communicate, both internally and with the outside world. News and local government websites became targets for cyber warfare exactly in the areas the Russian military was going to attack. Consequently, the federal and local Georgian governments, military, local news agencies were not able to communicate with Georgian citizens.[23]

Moreover, Georgian authorities were temporarily unable to communicate their story to the rest of the world. Once Russia successfully moved troops into Georgia, the second phase of cyber-attacks began. The target list expanded to include financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website. Hackers were mobilizing themselves through various websites such as StopGeorgia.ru, which went online on 9 August 2008.[24] However, when Georgian websites were disabled, they were moved to the blogosphere under the Google.com shield and the website of the president of

[20] J. Rogoza, A. Dubas, *Russian Propaganda War: Media as a Long- and Short-range Weapon*, Centre for Eastern Studies, September 2008, [https://www.files.ethz.ch/isn/91705/commentary_09.pdf access: 07 June 2017].

[21] A. Jugaste, *Communicating Georgia: Georgia's Information Campaign in the 2008 War with Russia*, Tartu University, 2011, [http://ut.ee access: April 2017].

[22] *U.S. Citizen Was among Georgian Commandos - Russian Military*, "RT.com", 28 August 2008, [https://www.rt.com/news/us-citizen-was-among-georgian-commandos-russian-military access: 01 February 2017].

[23] D. Hollis, *Cyberwar Case Study: Georgia 2008*, "Small Wars Journal", 2011 [http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 access: 10 March 2017].

[24] *Kremlin's Information War: Why Georgia Should Develop State Policy in Countering Propaganda*, Institute for for Development of Freedom of Information, 01 September 2016, [https://idfi.ge/en/informational-war-of-kremlin-against-georgia-the-necessity-of-having-state-policy-against-propaganda access: 23 March 2017].

Poland, which allowed Georgia to continue operating their websites and helped their communications with the world. Georgians transferred cyber assets and websites to servers in countries such as the United States, Estonia, and Poland.[25] The Georgian government also contacted Estonian officials to share their knowledge after the 2007 cyber-attacks in Estonia.

> ***Same as with the Georgian army, one of the most important targets for the Kremlin were Ukrainian soldiers. Mobile operators were used as tools for spreading panic and fear among the Ukrainian soldiers, especially during significant battles***

The war against Georgia in 2008 revealed weaknesses in the Kremlin's information warfare, which made the Kremlin rethink and improve its information capabilities. Some experts (including Russian) are convinced that Russia lost the information war against Georgia and was not prepared to fight it.[26] Shortly after the war ended, at that time the Russian prime minister V. Putin "congratulated" the organizers of what he called "the Western propaganda machine".[27] The war against Georgia became a significant trigger for the Kremlin's information warfare upgrade.[28]

The Kremlin's Aggression against Ukraine, 2014-Current Days: A Lethal Medley

Unlike Estonia in 2007 and Georgia in 2008, where the events lasted for a much shorter period, an active use of information warfare by the Kremlin against Ukraine has been already ongoing for four years. Here we describe just a few examples of the disinformation and fake news around the Ukrainian events.

The Kremlin's information war against Ukraine began at least in 2005, after the so-called Orange Revolution, when Russian politicians used such words as a "failed state" towards Ukraine. Symbolism played a significant role in the Russian disinformation campaigns and creation of perceptions for both Russian citizens and outsiders. Consequently, during and after the Revolution of Dignity (2013-2014), the Kremlin has vividly used World War II terminology such as "fascists", "Nazi", "banderovtsi" against the Ukrainian authorities, so as to create a specific image. For instance, on 28 April 2014, the Russian Ministry of Foreign Affairs referred to rumors of a construction of "fascist concentration camps" in Ukraine.[29] The representatives of the Ukrainian Armed Forces were often labeled as "punishers", "fascists", and "execution squads under the command of the Kyiv junta".

Same as with the Georgian army, one of the most important targets for the Kremlin

[25] D. Barker, *The Russo-Georgia War of 2008: Information Operations Case Study Analysis*, "Information Operations", 24 February 2013, [https://www.academia.edu/11903525/The_Russia-Georgia_War_of_2008_Information_Operations_Case_Study_Analysis access: 15 March 2017].

[26] N. Nikolaichuk, *Стратегическая информационная операция может быть скоротечной, а может длиться годами (Strategic Information Operation Can Be Fast or Can Last for Years)*, "Столетие", 2014 [http://www.stoletie.ru/politika/igor_nikolajchuk_strategicheskaja_informacionnaja_operacija_mozhet_byt_skorotechnoj_a_mozhet_dlitsa_godami_185.htm access: 12 October 2017].

[27] A. Jugaste, *Communicating Georgia: Georgia's Information Campaign in the 2008 War with Russia*, Tartu University, 2011, [http://ut.ee access: April 2017].

[28] M. Kyiak, *Countering Kremlin's Disinformation in Baltic and Eastern Europe*, "Baltic Worlds", 01 December 2016, [http://balticworlds.com/countering-kremlins-disinformation-in-baltic-and-eastern-europe access: December 2016].

were Ukrainian soldiers. Mobile operators were used as tools for spreading panic and fear among the Ukrainian soldiers, especially during significant battles such as the one near Debaltseve (January 2015).

The Russian state media produced plenty of fake news. The most profound example here is the downing of Malaysia Airlines Flight MH17 on July 2014. The main idea was to confuse the public with as many different rumors and fake news as possible, even contradicting one another, so as to obfuscate this tragic event. There were several statements from Russia about the plane, for example, that the plane was loaded with dead bodies and purposely flown overhead.[30] Other versions were that the Ukrainian air defense hit the MH17, or a Ukrainian ground attack airplane SU-25 brought down the Boeing. To "prove" the version of the SU-25 airplane, a "quote" from the Twitter account of an "air controller" at the Ukrainian international Boryspil airport named "Carlos" was provided. This was contravened by the fact that this person has never worked there and that foreign citizens are not allowed to work as air controllers in Ukraine.[31] A Joint Investigation Team composed of representatives of the Netherlands, Ukraine, Belgium, Malaysia, and Australia was set up to investigate the incident. The Kremlin-controlled media have offered at least nine different versions of what happened to MH17 and none of those versions correspond to the conclusion reached by the Joint Investigation Team in 2016.[32]

It may seem that the Kremlin was not using cyber warfare against Ukraine, but concentrated more on disinformation, diplomatic tools, and military actions.[33] No doubt if cyber-attacks were raised to the effectiveness of the attacks against Estonia in 2007 and Georgia in 2008, the consequences of this could be more severe.[34] Nevertheless, in 2014-2017, the Kremlin made more than 7,000 different cyber-attacks against Ukraine, according to the minister of defense of Ukraine S. Poltorak.[35] For example, just several minutes before the polls were closed during the May 2014 presidential election, the pro-Kremlin "hacktivist" group "Cyberberkut" posted false election results on the election commission's website, and Russia's TV "Channel One" aired those results. In December 2015, a huge cyber-attack was launched against Western Ukrainian energy provider

[29] K. Pynnoeniemmi, A. Racz, *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, Finnish Institute for International Affairs Report, May 2016, p. 79.

[30] A. Polunin, *Мертвый самолет или самолет мертвых? (A Dead Plane or a Plane with the Dead?)*, "Свободная Пресса", 03 August 2014, [http://svpressa.ru/war21/article/94297/ access: February 2017].

[31] T. Nazarchuk, *Збитий Боїнг Malaysia Airlines: що придумала російська пропаганда (The Downed Boeing of Malaysia Airlines: What Has Russian Propaganda Invented)*, "Mediasapiens", 18 July 2014, [http://osvita.mediasapiens.ua/ethics/manipulation/zbitiy_boing_malaysia_airlines_scho_pridumala_rosiyska_propaganda access: 10 June 2017].

[32] F. Hensen, *Russian Hybrid Warfare: A Study of Disinformation*, Center for Security Studies, 08 September 2017, [http://www.css.ethz.ch/en/services/digital-library/publications/publication.html/330e6a04-b2d4-4946-b296-5f39dae3044a access: 10 October 2017].

[33] J. Hsu, *Why There's No Real Cyberwar in Ukraine Conflict*, "IEEE Spectrum", 14 March 2014, [https://www.spectrum.ieee.org/tech-talk/computing/networks/why-theres-no-real-cyberwar-in-the-ukraine-conflict access: 02 May 2017].

[34] P. Pernik, *Is All Quiet on the Cyber Front in the Ukrainian Crisis?* International Centre for Defence and Security, 07 March 2014, [https://www.icds.ee/et/blogi/artikkel/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis access: 07 April 2017].

[35] *Росія здійснила понад 7 тисяч кібератак проти України – Полторак (Russia Has Made More Than 7 Thousand Cyberattacks against Ukraine – Poltorak)*, "Українська Правда", 05 April 2017, [https://www.pravda.com.ua/news/2017/04/5/7140280 access: 06 April 2017].

“Prykarpattiaoblenergo”, which caused problems with energy delivery throughout the whole region. It led to a blackout that affected 200,000 consumers.[36] In June 2017, the computer virus “NotPetya” in a single day attacked about 2,000 organizations and two thirds of them were located in Ukraine.[37]

During the Kremlin’s information war against Ukraine not only cyber warfare, but first and foremost, media and social networks were used. Almost immediately after the attempted annexation of Crimea and aggression in Donbas region in 2014, Ukrainian authorities stopped the transmission of the main Russian TV channels[38] in Ukraine. Later, on 25 February 2017, President of Ukraine P. Poroshenko signed the Doctrine of Information Security of Ukraine. According to the recent decision of the National Security and Defense Council signed by the president, any access to the Russian social networks such as Odnoklassniki.ru and Vkontakte.ru as well as Internet services Mail.ru and Yandex.ru was prohibited for a period of three years.

Conclusion

The so-called “Bronze Soldier” events in Estonia in 2007 were the first examples of a large-scale usage of cyber warfare against a sovereign country and a NATO member. During the Russian-Georgian war in August 2008, a combination of military actions, disinformation, and cyber warfare were used together. The ongoing aggression against Ukraine combines both strategies used in a much improved way. These three cases provide the possibility for positing conclusions that will go beyond this article:

- The Kremlin is skillful in understanding foreign audiences, as well as in using and increasing ethnic, linguistic, and ideological differences within other states. Both in Georgia and in Ukraine, one of the Kremlin’s main information warfare goals has been to separate governments and citizens of these countries. The Kremlin is also applying and monopolizing World War II narratives, which have been widely used against Estonia, Georgia, and Ukraine.

- Usually, the information warfare of the Kremlin is not applied separately, but in combination with other tools (diplomatic, kinetic, economic, intelligence, political, etc.). Still, the Kremlin never repeats the same consequence and same proportions of those tools while exercising aggression against another state. Its information warfare is vertically constructed, very centralized, and most likely has one core decision center.

- Estonia was the first case of cyber warfare used by Russia against another country’s infrastructure. Cyber-attacks have been used against Ukraine on a lesser scale than in Georgia, which could be explained by different goals of the Kremlin in those two states and by the peculiarities of the undeclared war against Ukraine. Most likely, the Kremlin has not used all of its cyber warfare potential yet.

[36] Y. Lapayev, A. Holub, *The Other Front*, “The Ukrainian Week: Cyber Insecurity”, January 2017, N1 (107), p. 37.

[37] A. Soshnikov, *Он вам не Petya: был ли доказан российский след вируса (He Is not Petya for You: Was Russian Trace of the Virus Proved)*, “Русская Служба BBC”, 17 July 2017, [http://www.bbc.com/russian/features-40525776 access: 07 Bebruary 2018].

[38] V. Sazonov, K. Muur, H. Moelder, *Russian Information Campaign against Ukrainian State and Defence Forces*, 08 February 2017, [http://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf access: 03 March 2017].

- The Russian aggression against Ukraine has demonstrated that information attacks are most effective in their early phases, when an emotional reaction is needed. The Ukrainian case has shown that the Kremlin is much weaker in keeping up and managing a long-term strategic information war. In this sense, the Russian information warfare looks more like a sum of wavelike information attacks than a complete strategy. Nevertheless, for now the Kremlin has all the needed capabilities to apply efficiently against any other Western state.

Maksym Kyiak *is a Doctor of Philosophy, the Deputy Director in the Central European Institute, and a co-founder of "Global Ukrainians", a worldwide network of public diplomats. He worked at various academic and governmental institutions in Ukraine and abroad. He has represented Ukraine at the CAHROM Committee in the Council of Europe and was one of the co-authors of the research of the NATO StratCom COE on the role of humor in strategic communications, "StratCom Laughs: In Search of an Analytical Framework". Maksym is also working on his postdoctoral research on information society and its influence on religious processes. Research interests: disinformation, information warfare, public policy, foreign policy, sociology of religion, ethnic policy.*